
DEEPSTRAT
STRATEGY . POLICY . ACTION
THEMES FOR
DIGITAL
INDIA BILL
AN ANALYSIS

DEEPSTRAT FOUNDERS

Yashovardhan Azad, IPS (Retd) Chaiman

Amb Pinak R Chakravarty, IFS (Retd)

Saikat Datta CEO

Amitabh Mathur, IPS (Retd)

Nandkumar Saravade, IPS (Retd)

Saurabh Chandra, IAS (Retd)

Vice Admiral Shekhar Sinha (Retd)

Amb Amar Sinha, IFS (Retd)

Anand Venkatanarayanan CTO

DeepStrat was founded by a group of experienced professionals who served in the top echelons of the Indian government in fields as diverse as administration, intelligence, policing, military, international relations, media, law and public policy.

CONTRIBUTORS

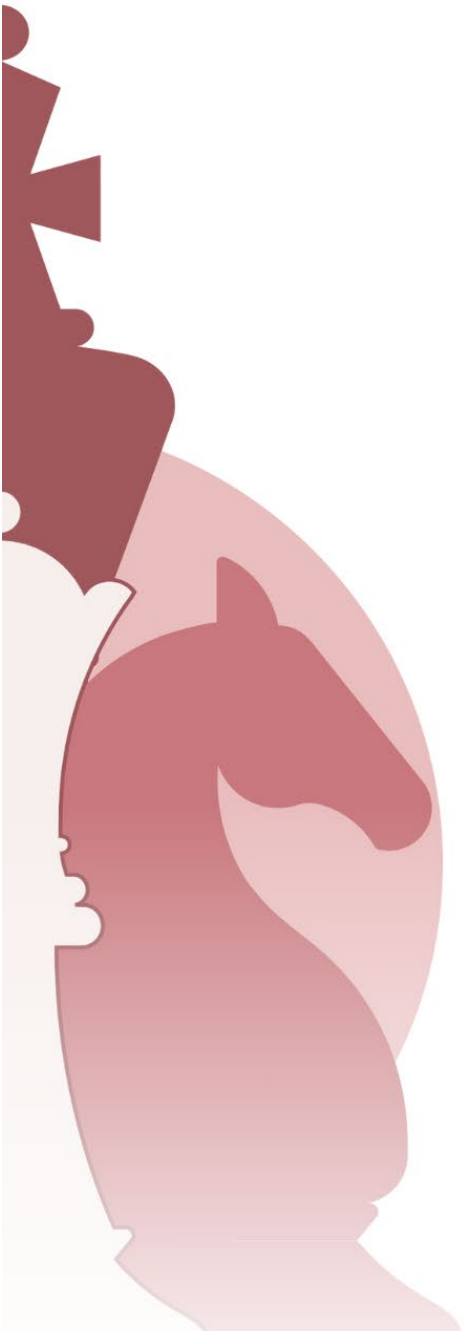
Shachi Solanki
Deputy Chief of Operations

Oleina Bhattacharya
Programme Associate

Nandkumar Saravade, IPS (Retd)
Co-Founder

Saikat Datta
Co-Founder and CEO

Shriya Bhatia
Lead Graphic Designer



About Us

DeepStrat is a New Delhi-based Strategic Consultancy and Think Tank specialising in Risk Management and integrated solutions to business continuity threats across sectors.

It was founded with the vision to combine rich experience in government with the best talent available in the private sector to produce sustainable solutions. At DeepStrat we focus on a broad spectrum of issues – Risk Assessment & Mitigation, Cybersecurity, Technology, Sustainability, Governance, Capacity Building, Foreign Policy, Defence and Public Policy.

DeepStrat is incorporated under India's Ministry of Corporate Affairs.

DEEPSTRAT
STRATEGY . POLICY . ACTION

Table of Contents

Foreword

Nearly 23 years after India passed the Information Technology (IT) Act 2000, we are again looking at passing an ambitious Digital India Act. Much has changed in the intervening years since the last Act and technology as well as services have undergone a paradigm shift. In 2000, the IT Act was passed to cater to the newly emerging IT and IT Enabled Services (ITES), which has now become a significant contributor to India's GDP.

India is poised to continue its journey as a major contributor to the global technology pool and its Digital India program is an ambitious push towards this goal. The proposed DIA is an opportunity to repeat the success of the IT Act, keeping in mind new and emerging technologies, services and India's potential to dominate digital markets globally.

DeepStrat has begun a series of position papers that draws on experiences from India and abroad on laws, regulatory frameworks, academia and start-ups to look at issues that are pertinent to the DIA. This is the first of the series where it looks at elements such as; Intermediary classification and liability, online harms, cybersecurity and innovation in fair markets.

Chapter 1: Intermediary Classification and Liability

1.1. Research analysis – 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 be the first level of classification.

2. Classification based on the nature of services

    - Helps tackle issues that arise from different types of online services.

- From the prism of user harm, 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, of 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 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

[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

[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

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,

[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

"intermediaries with respect to any particular electronic records, means any 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

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

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.

Classification Models

We recommend a combination of 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]

[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.

The Open System Interconnection model (OSI Model), developed by the 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].

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

[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/21/21-1333/252467/20230118141433052_2023%2001%2018%20i2C%20Amicus%20Brief%20-%20Bridges.pdf

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 service 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'.

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

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 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

[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
[19] OECD, Rethinking Antitrust Tools for Multi-Sided Platforms, 2018, www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.html
[20] ibid

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. However 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 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 the value of a platform and the number of its users.[22] A key driver of value-creation, and therefore the impact of online platforms is the strength of their user-base.

[21] Australia's Online Safety Act 2021, https://www.legislation.gov.au/Details/C2021A00076
[22] Stobierski Tim, *What are Network Effects?,* https://online.hbs.edu/blog/post/what-are-network-effects, November 12, 2020.

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

[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.

now scraping the web and developing the AI engine that 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

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.

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

[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

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 mitigation4. 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?

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

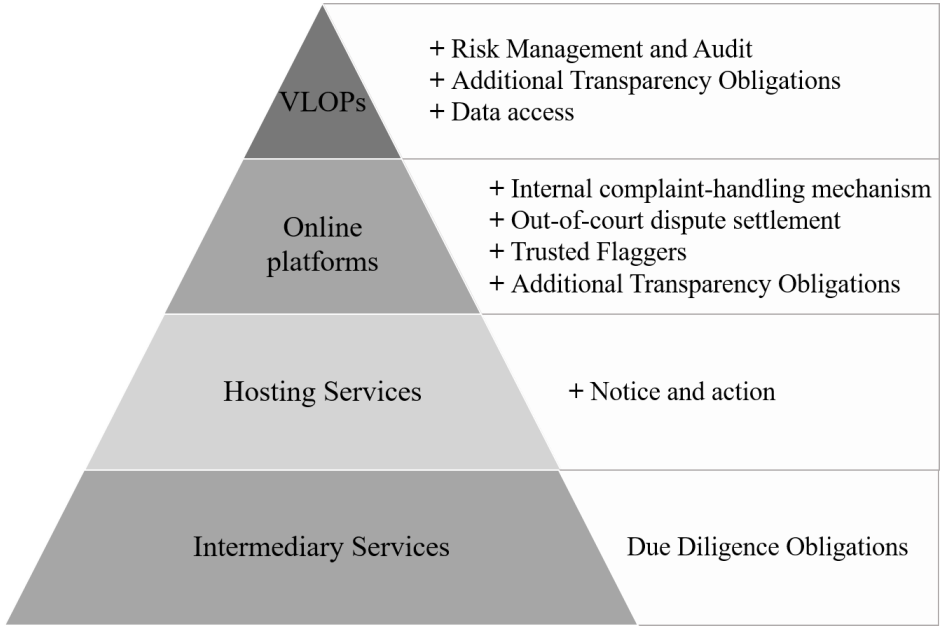
[27]Devadasan, V., 2023. Report on Intermediary Liability in India (December 2022). *Centre for Communication Governance*.
[28] Woods, L. 2022. The UK Online Safety Bill: an outline. https://blogs.lse.ac.uk/medialse/2022/03/25/the-uk- online-safety-bill-an-outline/

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.

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,

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

[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.

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- 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

[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

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?

[34] Jeff Koseff, *The twenty six words that created the Internet,* Cornell University Press, 2018 https://www.cato.org/events/twenty-six-words-created-internet

[35] Avnish Bajaj Redux? Supreme Court Of India Denies Relief To Google In Criminal Defamation Proceedings. https://www.medianama.com/2019/12/223-avnish-bajaj-redux-supreme-court-of-india-denies-relief-to- google-in-criminal-defamation-proceedings/

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.

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.

[36] Ganesan, A. (2023). Breaking: Karnataka HC Dismisses Twitter's Petition Challenging Government's Content Blocking Orders. https://www.medianama.com/2023/06/223-karnataka-hc-dismisses-twitters-petition/

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.

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

[37] Lefouili, Y. and Madio, L. (2022) The economics of platform liability. European Journal of Law and Economics. Available from : https://doi.org/10.1007/s10657-022-09728-7.

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] Dual-use regulation: Managing hate and terrorism online before and after Section 230 reform | Brookings. (2023) https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism-online-before-and- after-section-230-reform/

[39] Baghdasaryan, M. (2022) New Amendments to Intermediary Rules threaten Free Speech in India. Electronic Frontier Foundation. 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.

[40] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

[41] Online Safety Bill. United Kingdom. https://publications.parliament.uk/pa/bills/cbill/58-03/0209/220209.pdf

[42] Santa Clara Principles. https://santaclaraprinciples.org/

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 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.

[43] United Nations Human Rights. Guiding Principles on Business and Human Rights. 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

1.4. Principles for Intermediary classification and liability

1. **<u>Necessary, proportionate and differential obligations</u>**

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.

1.5. Definitions - Intermediary liability and classification

Definitions,- In this Act, unless the context otherwise requires,

a) **'Advertisement'** means information designed to promote the message of individuals or entities, irrespective of whether to achieve commercial or non-commercial purposes, and displayed by an online platform on its online interface against remuneration specifically for promoting that information;
b) '**AdTech'** means the software and tools that help agencies and brands target, deliver, and analyse their digital advertising efforts; (US Securities and Exchange Commission)
c) **'Content'** means the electronic record defined in clause(t) of Section 2 of the Act and includes anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description;
d) **'Content moderation'** means the activities undertaken by providers of intermediary services aimed at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of a recipient's account;
e) **'Cloud service provider'**[44] means a person who makes cloud services available;
For the purposes of this provision:
'Cloud service'[45] means one or more capabilities offered via cloud computing;

[44] 3.2.15 ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en
[45] 3.2.8 ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

'Cloud computing'[46] means the paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

f) **'Grievance'** includes any complaint, whether regarding any content, any duties of an intermediary or publisher under the Act, or other matters pertaining to the computer resource of an intermediary or publisher, as the case may be;

g) '**Grievance Officer'** means an officer appointed by the intermediary or the publisher, as the case may be, for the purposes of these rules;

h) **'Grievance Appellate Committee'** means a grievance appellate committee constituted under rule 3A;

i) **'Internet intermediaries'**[47] means those persons that bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties. Internet intermediaries will fall under three categories[48]:

i) a '**conduit**' means service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;
Explanation: For the purposes of this Act, Internet Service Providers will be included under this category.

ii) a '**caching**' means a service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

iii) a '**hosting**' means a service that consists of the storage of information provided by, and at the request of, a recipient of the service;
Explanation: For the purposes of this Act, Online Platforms will be included under this category.

j) **'Internet service provider'**[49] – means a person who provides end-users with a data connection allowing access to the internet and associated services;

[46] 3.2.5 ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en. ITU, Cloud computing – Overview and high-level requirements of distributed cloud, 2019. https://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00001C0043PDFE.pdf

[47] OECD, The Economic and Social Role of Internet Intermediaries, 2010. https://www.oecd.org/digital/ieconomy/44949023.pdf

[48] Article 2(f) EU's Digital Services Act, 2022. https://digitalservicesact.cc/dsa/art2.html

[49] OECD, Report on Access Pricing, 2004. https://www.oecd.org/regreform/sectors/18645197.pdf

k) **'news and current affairs content'** includes newly received or noteworthy content, including analysis, especially about recent events primarily of socio-political, economic or cultural nature, made available over the internet or computer networks, and any digital media shall be news and current affairs content where the context, substance, purpose, import and meaning of such information is in the nature of news and current affairs content;

l) **'online gaming intermediary'**[50] means any intermediary that enables the users of its computer resource to access one or more online games;

For the purposes of this provision –

'online game'[51] means a game that is offered on the Internet and is accessible by a user through a computer resource or an intermediary;

Explanation.—In this clause, 'Internet' means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that transmits information based on a protocol for controlling such transmission.

'online real money game'[52] means an online game where a user pays the service fee charged by the online gaming intermediary and makes a deposit towards the prize pool with the expectation of earning winnings on that deposit;

Explanation.—In this clause, 'winnings' means any prize, in cash or kind, which is distributed or intended to be distributed to a user of an online game based on the performance of the user and in accordance with the rules of such online game.

[50] S. 2(qb) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf

[51] S. 2(qa) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf

[52] S. 2(qd) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf

'prize pool' means the total prizes or rewards, in the form of money or money's worth, that is deposited by users participating in an online game, excluding the service fee charged by the online gaming intermediary, which is to be distributed to winners in such online game and that such total prizes or rewards are made known to all participating users in advance of the online game;

'service/platform fee' means the commission or entry amount, in the form of money or money's worth, charged by the online gaming intermediary for provisioning or facilitating or organising the online gaming service to the users, but excludes the deposit or prize pool;

m) 'Online platform'[53] - means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation;

n) 'Prominently publish' shall mean publishing in a clearly visible manner on the home page of the website or the home screen of the mobile based application, or both, as the case may be, or on a web page or an app screen directly accessible from the home page or home screen;

o) 'Publish', when in relation to intermediaries, means to make content available in electronic form to a potentially unlimited number of third parties, either on demand of the user or by means of a partially or fully automated system(s) that suggest(s) specific information to users in an intermediary's online interface;

Explanation.-- in this clause, "suggests specific information" means suggestions that are a result of a search initiated by a user and includes determining the relative order or prominence of information displayed.

p) 'social media intermediary'[54] means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;

[53] Article 2(h), European Union's Digital Services Act, 2022. https://digitalservicesact.cc/dsa/art2.html

[54] S. 2(w) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

q) 'Significant social media intermediary'[55] - means a social media intermediary having number of registered users in India above such threshold[56] as notified by the Central Government;

r) 'search engine'[57] means a service which (a) includes a service or functionality which enables a person to search some websites or databases (as well as a service or functionality which enables a person to search (in principle) all websites or databases); (b) does not include a service which enables a person to search just one website or database;

s) 'Taking action', when in relation to content, means taking down content, restricting users' access to content, or taking other action in relation to content (for example, adding warning labels to content);

t) 'Taking down (content)' means any action that results in content being removed from a user-to-user service or being permanently hidden so users of the service cannot encounter it (and related expressions are to be read accordingly);

u) 'Taking action against a person' means giving a warning to a person, or suspending or banning a person from using a service, or in any way restricting a person's ability to use a service;

v) **'user account'** means the account registration of a user with an intermediary or publisher and includes profiles, accounts, pages, handles and other similar presences by means of which a user is able to access the services offered by the intermediary or publisher;

****Refer to Appendix 1 for a comparative analysis of definitions in model laws from other jurisdictions***

[55] S. 2(v) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[56] Ministry Of Electronics And Information Technology Notification New Delhi, the 25th February, 2021 https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf

[57] S. 230, UK Online Safety Bill, 2021. https://bills.parliament.uk/publications/52368/documents/3841

Chapter 2: New and Emerging Technology

2.1. Research analysis - Emerging Technologies

Summary of Recommendations

1. Establish a regulatory sandbox model imbibing principles of an;
- Adaptive-outcome based approach,
- Risk-weighted approach
- Collaborative approach.
2. Utilise the sandbox framework to establish liability standards for emerging technologies.

Background

Emerging technologies are new technological innovations that break new ground in a particular field. They can revolutionise how we live and work, create new markets, and displace existing ones. Over centuries, innovative technologies have been developed and have opened new avenues for lifestyle and market transformation. Emerging technologies have already had an impact on our everyday lives by providing opportunities to ease the quality of our everyday life. Digital trade and finance are opening **economic opportunities.** Digital health and education are providing cost-effective solutions from a **social perspective**. In smart cities, EVs are posing as alternative models for protecting **the environment** and enhancing sustainability.

These new technological capabilities are evolving faster than the law's ability to keep up. As a result, new and rapidly evolving technologies and sectors will present formidable challenges to traditional regulatory regimes and will necessitate the formulation of new governance processes.[58]

Importance of Emerging Technologies

New technologies hold the potential to fundamentally transform the way the economy and society function. **Emerging technologies are disruptive** because they can change the way we live and work in fundamental ways. **They have also created new markets and displaced existing ones, by making significant impacts in various industries.** For example, the invention of the printing press led to the spread of knowledge, while the development of the internet has revolutionised the way we communicate and do business.

Emerging technologies are the drivers of economic growth. **India is a prime example of this, as its economy has grown rapidly in recent years due to its embrace of new technologies.** These technologies have helped businesses to become more productive and efficient, which has led to higher profits and more jobs. In addition, new technologies have also created new industries and markets, which has further boosted economic growth. India is now prepping for cutting-edge technologies including 5G, AI, blockchain, augmented reality & virtual reality, machine learning & deep learning, robots, natural language processing, etc as per MeiTY.[59] The Digital India Act (DIA) aims to foster this by supporting the development of these new products and services.

Incorporating Emerging Technologies

The Internet is the essential infrastructure that connects various devices like smartphones, tablets, game consoles, PCs, and servers. These devices collect and transmit large volumes of data for storage, processing, decision-making, monitoring, and management

[58] AI & Emerging Technologies Division | Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/emerging-technologies-division

[59] Ibid

purposes. The backbone of this connection is broadband Internet along with other connectivity tools. The demand from consumers for these devices and services leads to investments in broadband, which in turn spurs innovation in infrastructure technologies like 4G, 5G, fiber optics, and satellite communication.

In the healthcare industry, India's growth has been fueled by Emerging Technologies. The importance of this was also highlighted by the MoS Mr. Rajeev Chandrashekhar in the Digital Bharat Summit, on digital infrastructure.[60] Importance of leveraging digital public infrastructure in a significant manner, to attain Sustainable Development Goals (SDGs) was highlighted. Most countries are also trying to harness emerging technologies, examples include;
The European union in its European Innovation Council WORKING PAPER 1/2022[61] identified the use of emerging technologies and breakthrough innovations in the field of digital **technologies, healthcare and climate neutrality.** The identified areas underwent a validation process by cross- referencing with other reports and methodologies, including the "100 Radical Innovation Breakthroughs[62]" report. In 2023, the Infocomm Media Development Authority (IMDA) Singapore, established that it aims to foster both the business and research communities to continually push the frontiers of technology, driving digital transformation and enabling innovations within its digital economy. Focusing on supporting three key emerging technology domains – **AI, Communications and Connectivity, and Trust.[63]**

The United States and India announced the launch of the **Initiative on Critical and Emerging Technology (iCET)**, which will focus on cooperation in areas of Emerging Technologies such as quantum computing, artificial intelligence, and biotechnology.[64] Under iCET a

[60] Sanzgiri, V. (2023) Global DPI Summit: Experts discuss the role of digitization in healthcare and education sector. MediaNama https://www.medianama.com/2023/06/223-global-dpi-summit-digitization-healthcare-education/

[61] IDENTIFICATION OF EMERGING TECHNOLOGIES AND BREAKTHROUGH INNOVATIONS https://eic.ec.europa.eu/system/files/2022-02/EIC-Emerging-Tech-and-Breakthrough-Innov-report-2022-1502- final.pdf

[62] Visualization RIBRI. https://ribri.isi-project.eu/index.html

[63] Emerging Technologies - Infocomm Media Development Authority. https://www.imda.gov.sg/about-imda/emerging-technologies-and-research

[64] FACT SHEET: Republic of India Official State Visit to the United States. The White House 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/22/fact-sheet-republic-of-india- official-state-visit-to-the-united-states/

technology partnership and defence cooperation between governments, businesses and academic institutions was committed. Ensuring that an open accessible and secure technology ecosystem on mutual trust and confidence is to be fostered.

This clearly portrays the idea that innovation is at the center of incorporating emerging technologies, but these idea incubation tools make us realise that there is no model method to regulate such emerging technologies.

Who does the liability fall on?

Because of the nature of disruptive models that emerging technologies create, it can be difficult to assign liability for the harm caused.

For instance, 3D printing is a new technology that is changing the way we build things. Certain challenges posed are that traditional liability laws are not always clear-cut when it comes to 3D printed products. For example, if a 3D printed house collapses, who is to blame? Is it the supplier who provided the design, the manufacturer who 3D printed the house parts, or the manufacturer of the 3D printer?

Similarly, in the case of blockchains, since it is a decentralised model and there is no central authority that executes this model, it is difficult to determine who is liable in case of a breach, because of the very importance of anonymity that it revolves around.

With the growth of Artificial Intelligence, these systems have the ability to act autonomously. Although the set of objectives of the AI models are set by humans. Which gives rise to questions of risks imposed by an AI model, for instance if a healthcare worker follows the recommendation of an AI-based tool to treat a patient, who would bear liability for any treatment injury?

Tools such as ChatGPT and Bard are being used extensively by employees of various companies to tackle redundancy in work. In April 2023 a report was released, that Samsung employees accidentally leaked confidential data into ChatGPT[65]. Would this constitute a breach on the employees' part or negligence of duty on the company's part?

Incorporating Emerging technologies make it challenging for regulators to keep up and assess the risks associated with these new technologies. Additionally, regulators may lack the necessary expertise to effectively regulate them.

Regulatory sandboxes for Emerging Technologies

To address these issues, a regulatory sandbox offers a secure space for businesses to test and evaluate new technologies, identifying and mitigating risks in the process. Enacting a regulatory sandbox model can both help to answer the "**what to regulate**", "**when to regulate**" and "**how to regulate**" by encompassing principles of adaptive and outcome based, risk-weighted, and collaborative regulations. It can be adaptive by allowing rule adjustments based on new information. It can be outcome-based, focusing on results rather than specific methods. It can be risk-weighted, tailoring regulations to technology-specific risks. Additionally, it can be collaborative, involving businesses, regulators, and academics to discuss technology risks and benefits for fair and accountable regulation development. Emerging technology has the potential to transcend regulatory and national boundaries. It is not feasible to confine different technological platforms within the jurisdiction of a single regulator or nation.

[65] Mack DeGeurin. Samsung Employees Leaked Confidential Data to ChatGPT. Gizmodo. April 6, 2023. https://gizmodo.com/chatgpt-ai-samsung-employees-leak-data-1850307376

- **Adaptive and Outcome-based regulation** Unlike traditional regulations that can quickly become outdated, this approach suggests a shift towards a responsive approach instead of a static one, focusing on desired outcomes rather than specific methods, of achieving this change. This can help businesses to identify and mitigate risks, and to develop new products and services that can benefit society. emphasises focusing on results and performance rather than rigid forms. Additionally, it enables a proportionate response to risk. A regulatory sandbox will help recognise how a desired adaptive outcome of an emerging technology can be recognised identifying it's potential risks in a controlled environment by regulators.
- **Risk-weighted regulation** advocates for a segmented approach tailored to different risks posed by different emerging technologies. This approach ensures proportionate allocation of regulatory resources by matching them to the risks associated with different emerging technologies. It offers flexibility, enabling regulators to adapt their approach based on the specific risks posed by each technology. This balance between effective regulation and flexibility encourages innovation while still providing protection against high-risk activities. Liability rules create incentives to reduce risk and avoid engaging in risky activities.

This was addressed in Germany[66], where the Federal Government proposed rules for decision- making to promote ethical behaviour by systems guiding crash scenarios for driverless cars. These rules prioritise human life above property damage and do not discriminate between human lives. Ensuring fairness and prioritising the risks associated with such technology.

- **Collaborative Regulation** aims to align regulations nationally by involving a wider range of stakeholders. This approach would allow different levels of legislation to collaborate on the same level rather than being addressed by different jurisdictions in their own capacity. Furthermore, it builds trust and cooperation among regulators, businesses, and stakeholders, facilitating responsible and beneficial development and adoption of emerging technologies.

Similarly, the Regulatory sandbox approach has been implemented within the Indian ambit at various stages of regulatory bodies including the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI), Securities and Exchange Board of India (SEBI) and the Telecommunication Regulatory Authority of India (TRAI). As per the RBI, the first and foremost benefit

[66] Ethics commission; Automated and connected Driving Report 2017. Federal Ministry of Transport and Digital Infrastructure. https://bmdv.bund.de/SharedDocs/EN/publications/report-ethics-commission-automated-and-connected- driving.pdf? blob=publicationFile

of the regulatory sandbox is that it fosters 'learning by doing' on all sides.[67] The central bank has identified four areas of monitoring financial related activities – Retail payments, cross-border payments, MSME lending and mitigation of financial fraud. This was an outcome-based approach. The question of "what" is being addressed by identifying the goal it aims to achieve and the "how" will be answered by the practice conducted within the regulatory sandbox. It also fosters a sense of collaboration within this framework, where fintech's are to comply with various regulatory requirements regulated under one body (RBI).

From a DIA perspective the sandbox model must be inclusive, catering to businesses of all sizes. It should offer clear regulatory guidance tailored to each product or service, and not exclude small emerging tech businesses. Stakeholder feedback, including from consumers, regulators, and industry experts, should be gathered. Additionally, the sandbox should undergo monitoring and evaluation to ensure its effectiveness in fostering innovation and managing risks.

Sandboxing Process

The need to identify the sectors in which emerging technologies are utilised is important to establish to what extent experimentation within the framework would be allowed. Focusing on the objective this regulatory sandbox model aims to foster is necessary. Once a sector specific threshold is in place, the sandbox model would focus on what must be exempted from being regulated in a clause-by-clause nature. [68]

[67] Shreesh Kapoor. Regulatory Sandbox Explained: How RBI is moderating Fintechs' disruption in BFSI. 2021 https://bfsi.economictimes.indiatimes.com/news/policy/regulatory-sandbox-explained-how-rbi-is-moderating- fintechs-disruption-in-bfsi/87098591

[68] Jeník, Ivo, and Schan Duff. 2020. "How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers." Technical Guide. Washington, D.C.: CGAP.

A recent sandbox test by the Consumer Financial Protection Bureau (CFPB) in the US, found that this technology resulted in: Approval of 27% more applicants, 16% lower average annual percentage rates (APRs) overall, substantially higher approval rates for applicants under age 25 and consumers with incomes under $50,000, No discrimination in approvals.[69]

In order to be future ready, a regulatory sandbox approach must conduct a **feasibility assessment:**

The assessment should be linked to the overall objectives of the program and help identify the eligibility criteria of business, wherein it would define who can participate in the sandbox. Eligibility should be articulated clearly to ensure a level playing field across all market participants. Post which a regulatory sandbox unit must be put in place, with key roles and responsibilities, and key operational processes, coordinating sandbox inquiries with other units of the regulator. A threshold must be put in place, assessing the duration of the test. Followed by tests restrictions in order to gauge to the scope, scale, and/or conduct of the sandbox test to minimise potential harm. The Assessment would also include an exit strategy for businesses, which would incorporate individual test outcomes and the integration of insights and lessons learned to inform the broader regulatory agenda.

Conclusion

Emerging Technologies have the potential to fundamentally affect our day-to-day lives. They offer economic growth opportunities and have already made significant impacts in various sectors such as trade, finance, healthcare, education, and sustainability. However, the rapid pace of technological advancements often surpasses the ability of existing regulations to keep up. Assigning liability for harm caused by emerging technologies can be challenging due to the disruptive nature of these innovations. Traditional liability laws may not provide clear answers, especially in cases where multiple parties are involved or where decentralised models like blockchain are used. As technologies like AI become more autonomous, questions arise regarding who bears responsibility for any negative outcomes, or rather what do negative outcomes construe?

[69] https://files.consumerfinance.gov/f/documents/cfpb_statement-on-competition-innovation_2022-09.pdf

To address these challenges, regulatory sandboxes can emerge as a potential solution. These sandboxes provide a controlled environment for businesses to test and evaluate new technologies, identifying and mitigating risks while fostering innovation. Adaptive and outcome- based regulations focus on desired results rather than rigid methods, allowing for responsiveness to changing circumstances. Risk-weighted regulations tailor the approach to the specific risks associated with different emerging technologies, striking a balance between innovation and protection. Collaborative regulation involves stakeholders from various levels, promoting alignment and cooperation to effectively govern emerging technologies.

Examples from around the world, such as Germany's ethical rules for driverless cars and India's regulatory sandboxes for financial technology, showcase the benefits of these approaches. However, it is crucial to ensure that regulatory sandboxes are inclusive, providing guidance for businesses of all sizes and involving stakeholder feedback. Monitoring and evaluation are also essential to assess the effectiveness of the sandbox model in managing risks and fostering innovation. By striking a balance between innovation and protection, we can foster the responsible and sustainable development of these technologies while addressing societal concerns and upholding ethical standards.

2.2. Principles for Emerging Technology

Principles for Emerging Technology

1. **Principle of Solidarity** – Benefits and burdens of Emerging technologies must be shared across stakeholders.

    1.1 Deploy emerging technologies after its potential implications have been assessed by an empowered committee

    1.2. Implement mechanisms of redressing the risks of AI to curb inequality.

2. **Principle of Proportionality -** Emerging technology should be regulated in a proportionate manner to promote innovation and establish relevant guardrails.

2.3. Definitions – Emerging technology

a. **'Emerging Technology'** (For the purpose of this Act) means digitally enabled tools representing new and significant developments, as notified by the Emerging Technology Committee;
b. **'Non-Fungible Tokens**' means a programmable blockchain-based digital item that publicly proves ownership of digital assets or physical assets that are tokenised;
c. **'Regulatory Sandbox'** means a controlled environment to test innovative technologies for a limited time on the basis of a testing plan agreed with the competent authorities, ensuring overarching regulatory objectives;

Chapter 3: Fair markets and Digital Competition

3.1. Research analysis – Digital competition

Key Recommendations:

1. Emphasise certain principles such as non-discrimination and non-exclusivity in the Digital India Act (DIA) to govern competition regulations in digital markets.
2. Adopt an *ex-ante* framework to pre-empt certain anti-competitive practices and clarify them to all market players before harm occurs.
3. Ensure that regulations on digital competition do not impose undue compliance burdens for new and emerging technologies.
4. Create a mechanism for identifying dominant players in the market that can negatively influence competitive conduct.
5. Ensure a level playing field by providing small market players essential resources that allow them to participate in the market.
6. Specify a harmonised set of rules for regulating designated gatekeepers to prevent barriers to entry, facilitate fair competition, and promote innovation.

Introduction

An open and reliable marketplace is crucial to foster competition, fuel innovation and expand consumer choices. Innovation depends on fair play by market players and a level playing field. However, recent developments have demonstrated that big market players can and do engage in anti-competitive behaviour that skews the market. This prevents newer entrants from establishing a footing. As

conversations about the ambitious Digital India Act gain traction, it is becoming increasingly clear that safeguarding competition within digital markets will play a crucial role.

The commitment to fair competition exists in the backdrop of Prime Minister Narendra Modi announcing India's goal of becoming a trillion-dollar digital economy by 2026. This is best realised by an overarching framework for online intermediaries that includes principles for identifying anti-competitive practices without stifling innovation or depriving consumer choices. Ex-ante mechanisms like regulatory sandboxes are also proposed as a valuable tool for Indian regulators since it allows market players to innovate freely, unhindered by the fear of regulatory and compliance costs.

The DIA will be an omnibus legislation. It will not only replace the Information Technology Act, 2000 but also establish the principles for digital competition for the next "techade", a decade powered by the impact of technology. Any principles that it may evolve must remain aligned with its aim of creating an internet that is open, safe, trustworthy, transparent, and accountable.

The proposed law also aims to foster innovation, which enhances choices available to users. Users benefit when businesses have the freedom to design, create and introduce new technologies or services. While innovation can create a spurt of new companies, the network effects enable companies to scale and operate more efficiently by attracting a larger user base. Network effects are a type of economic interaction in which the value of a good or service increases with the number of users. *For example*, the value of a social media platform increases with the number of users on the platform. Network effects can often lead to concentration because the more users a platform has, the more valuable it becomes. This makes it difficult for new competitors to enter the market because they need to attract users away from the dominant platforms. This is known as the chicken-and-egg problem because new platforms need users to be valuable, but users need a valuable platform to join. As a result of network effects, a few dominant players can emerge in a market. These dominant players can benefit from economies of scale, which are cost advantages that come from producing a large quantity of goods or services. These cost advantages can make it even more difficult for crucial competitors to enter and diversify the market.

India has witnessed a rise in competition concerns, such as abuse of dominant position and predatory pricing. This has led India's competition regulator, the Competition Commission of India (CCI) to intervene and penalise anti-competitive behavior from dominant players. This kind of ex-post approach, where the harm is addressed after it has occurred, may not be able to predict and prevent anti-competitive behaviour till it is brought to the regulator's attention. There is also undue pressure on the CCI to process all competition concerns in India's economy across different sectors. Therefore, it might be useful to flag certain practices that are anti-competitive in advance so that harm can be prevented and not just adjudicated after the event has occurred.

Competition in Digital Markets: Current Scenario

In India, the Competition Act, 2002 governs all competition in the Indian economy but has not been able to adequately address concerns in the digital context. This is because traditional competition law concepts like 'relevant market', 'market power', 'abuse of dominant position', or 'predatory pricing' gain a new meaning in a digital context. Furthermore, under the current framework anti-competitive behavior is not processed in a timely manner.[70] As a result, irreparable and far-reaching harm can be caused by the time an investigation is concluded or an order is issued to large platforms.[71] For instance, by using predatory pricing or exclusive agreements, a dominant platform can benefit from such practices if investigation of such anti-competitive practice is delayed. This could lead to the exclusion of new entrants from the market.

[70] https://www.cci.gov.in/public/images/annualreport/en/20-211665122051.pdf

[71] For example in the case of the *United States v. Microsoft Corp,* which spanned from 1998 to 2001. The U.S. Department of Justice accused Microsoft of engaging in anti-competitive practices by tying its internet browser, Internet Explorer, to the Windows operating system. This behaviour limited the market opportunities for competing browsers, such as Netscape Navigator, and hindered innovation in the browser market.
https://www.justice.gov/atr/us-v-microsoft-courts-findings-fact

This has been observed and addressed by a Parliamentary Committee Report, by the CCI and also by the Indian government's amendment of the Competition Act in 2023[72]. Notably, the Parliamentary Committee Report puts forth the argument that the ineffectiveness of the current framework can be overcome if India adopts *ex-ante* measures to regulate digital competition.[73]

Principles for Digital Competition

The jurisprudence of CCI's orders indicates certain principles that can be adopted by the DIA in developing an *ex-ante* framework for the digital economy. The **principle of non-discrimination** that was adopted in the order against Google in 2018[74] set an important precedent for digital anti-trust regulation. The CCI also addressed **exclusivity practices** in the Flipkart order,[75] in which it examined allegations of exclusivity and preferential treatment by the e-commerce platform, towards certain sellers. The CCI ordered a detailed investigation into the matter to assess potential anti-competitive practices. Similarly, there are other principles that can form the basis of regulating digital competition:

[72] Finance Standing committee 53rd Report, 2023. https://loksabhadocs.nic.in/lsscommittee/Finance/17_Finance_53.pdf

[73] In India, the Parliament's Standing Committee on Finance identified ten anti-competitive practices in digital markets in India. These were:

1. Anti – steering
2. Self preferencing
3. Bundling
4. Use of non-public data
5. Deep discounting
6. Exclusive tie ups
7. Search and ranking preferences
8. Restricting 3rd party applications
9. Advertising policies

[74] Case No. 39 of 2018. https://www.cci.gov.in/images/antitrustorder/en/07-and-3020121652434133.pdf

[75] Case No. 20 of 2018, https://www.cci.gov.in/images/antitrustorder/en/2020181652328846.pdf

1. Balancing anti-competition regulation with innovation

Competition in the digital economy has to be regulated, but not at the cost of innovation and economic advancement. Efficiency of digital market places can be achieved by pre-empting certain anti-competitive practices and behaviours, known as an '*ex ante*' approach.

Ex-ante measures are proactive regulatory actions taken before any potential harm or anti-competitive behaviour occurs. Such an approach is different from the ex-post approach currently followed in India wherein abusive practices are addressed only once the damage has occurred. In Australia, for instance, an *ex-ante* measure taken by the Australian Competition and Consumer Commission (ACCC) was implementing mandatory 'service-specific' codes that follow the principles of competition on merits, informed consumer choice, and fair-trade practices for users on digital platforms. [76]

However, an '*ex-ante*' framework needs to be balanced with India's goal to foster innovation in new and emerging technologies. Since technologies like AI, Non-fungible tokens (NFT) and cryptocurrency are still evolving, these are early days to impose regulations. Overregulation can also impede growth by imposing compliance burdens on nascent technologies. Instead, as some regulators such as the RBI have shown, a regulatory sandbox for new and emerging technologies ensures innovation to evolve.

[76] The ACCC suggests that implementing a service specific code approach protects and promotes competition not only among providers of digital platform services but also among providers of goods and services in related markets. This approach allows for strategic prioritization of specific digital platform services, addressing urgent and significant harms effectively. It provides the flexibility to develop targeted obligations through codes of conduct, ensuring clarity about the scope and obligations of future codes.

Regulatory sandboxes ensure a safe space for businesses venturing into developing new technologies. These allow for businesses to invest in innovation without having to bear the burden of complex regulatory requirements governing digital markets.

2. Transparency in Digital Markets

User trust and safety can only be established when there is transparency in digital markets. Digital markets become more transparent when key stakeholders are identified and there is a robust redressal mechanism. This allows informants to report and be compensated for the anti-competitive practices of large/dominant market players. Thus, identification of dominant players in a digital market becomes a crucial starting point in this regard. This is mentioned in the 53rd Standing Committee on Finance Report which recommended that India identify leading players in digital markets that can negatively influence competitive conduct and categorise them as Systemically Important Digital Intermediaries (SIDIs). Identifying them as gatekeepers aids transparency, by allowing targeted regulatory interventions, including the enforcement of anti-trust laws, to ensure fair competition and prevent abuse of market power. Such classification can be addressed by the DIA, which is already seeking to develop a framework for classifying intermediaries.

A leading market player becomes a gatekeeper when they hold enough power to restrict access to resources crucial for the growth of a business. Gatekeepers can unilaterally change the terms and conditions of access to their services without providing users advance notice or an option to remain under the existing terms and conditions. This may be restrictive for internet users as well as small market players, disincentivising them from investing or innovating. Fair competition can be ensured by providing users the choice to consent to services provided by large platforms, instead of being automatically signed to the services provided by the platform.

In the EU, gatekeepers are defined as "large online platforms" under the Digital Markets Act (DMA).[77] Similarly, Indian competition regulations should also deliberate upon the thresholds that would qualify a subset of intermediaries as SIDIs, or even "Gatekeepers". By identifying them, their roles and responsibilities can be established to ensure that the rights of the users as well as new entrants are protected. These rights must be addressed under the DIA by ensuring stricter guidelines for data collection, usage and control. The DIA must also foster mechanisms for consumer redressal, non-compliance and harm caused by the actions of SIDIs.

3. User Empowerment

Promoting a fair marketplace for businesses alone would not ensure a holistic development of the digital economy. It is also important to provide users with quality products and services. This is only possible when digital markets are accessible to large and small market players equally. This ensures users have a choice to choose between different players in the digital market. Therefore, it is imperative that there is a level playing field for all businesses so that the quality of digital products and services to users can be assured. Monopolies and oligopolies need to be carefully regulated as they are a major threat to perfect competition, which is ideal for ensuring consumer welfare. A legal principle that addresses the regulation of such monopolies is the essential facilities doctrine. This doctrine entails providing certain basic infrastructure (which may include connectivity, cloud computing, security, storage, SaaS and PaaS applications) to all competitors, big or small, so that they may participate in the marketplace on fairer terms.

4. Harmonised Laws

Consistent enforcement of competition and anti-trust policies relies on cooperation between regulators.[78] A fragmented regulatory landscape undermines the functioning of a single market, which is characterised by the free movement of goods and services and can enhance the power of monopolistic or oligopolistic market players. Since gatekeepers in digital markets also facilitate a flow of services

[77] Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force. Press release 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423
[78] https://www.e-ir.info/2020/10/27/tech-giants-and-competition-a-political-economy-perspective/

and goods across borders, a harmonised framework would allow for uniform enforcement of policies across jurisdictions. The need for this has also been highlighted in Recital 31 of the Digital Markets Act (DMA) which recognises that a harmonised set of rules for gatekeepers and their services can prevent barriers to entry, facilitate fair competition, and promote innovation by ensuring a level playing field.[79] The Digital India Authority (DIA) should consider adopting a framework for regulating digital competition that is aligned with national and international laws and emerging jurisprudence. India must ensure that the principles underlying its framework reflect its unique goals, while also being compatible with the global effort to create a unified market. This can be done by harmonising India's digital competition framework with those of other jurisdictions and ensuring that the underlying principles are congruent.

Conclusion

A key goal of the proposed DIA is to address challenges in the digital economy by promoting fair competition by ensuring a level playing field among market players. This can be achieved through a framework that balances the need to regulate competition with the need to foster innovation. Hence, to develop a framework that balances fair competition with innovation, it will help if:

3.2. Principles for Digital Competition

1. Principle of Transparency

1.1. Accountability in regulating platforms and allowing them a choice to moderate content in a transparent manner. Identifying intermediaries as large platforms aids transparency, by allowing targeted regulatory interventions, including the enforcement of anti-trust laws, to ensure fair competition.

1.2. Data controller must be obliged to inform data users.

[79] European Competition Journal Volume 19, 2023 - Issue 1

1.2.1. Scope of processing of personal data.

1.2.2. Potential consequences of the processing.

1.3. Ensure user trust and safety through transparency.

1.3.1 Identify key stakeholders.

1.3.2. Establish a grievance redressal mechanism.

2. **Principle of Accountability -** *Prescribing performance reporting mechanisms ensures accountability.*

2.1. Accountability of regulators.

2.2. Accountability of Intermediaries (Platforms).

2.2. Accountability towards end-users.

3. **Principle of User Empowerment and Autonomy**- *Users' best interests should be catered by platforms, through*

3.1. Provide technical measures enabling users to manage their safety.

3.2. Establish light-touch protocols for service violations.

3.3. Leverage the use of technical measures to mitigate risks and harms, which can be flagged to users timely.

This is possible when digital markets are accessible to large and small market players equally. This ensures users have a choice to choose between different players in the digital market.

3.3. Definitions - Digital Competition

a. **'AI systems'** A system created to function with a certain level of autonomy, utilising machine and/or human-provided data and inputs to infer how to achieve specific human-defined objectives, accomplished through machine learning, generating outputs, such as content, predictions, recommendations, or decisions, which in turn influence the environment it interacts with;

b. **'Blockchain'**[80] means an electronic record created by the use of a decentralised consensus ledger or consensus database maintained via Internet or peer-to-peer network, by multiple parties to verify and store a digital record of transactions which is secured by a cryptographic hash of previous transaction information;[4]

c. '**Digital Internal (Domestic) Market'**[81] - means virtual spaces within the territorial jurisdiction of India, where the buying, selling, and exchanging of digital goods, services, and rights take place involving Digital Platforms;

d. '**Digital Markets'**[82] means virtual spaces including Digital Platforms where buying, selling, and exchanging of digital goods, services, and rights take place;

e. '**Digital Platforms'**[83] means any digital services operating in two (or multi) sided markets, enabling interactions between two or more distinct but interdependent groups of users, who interact via the Internet;

[80] Illinois Government - 205 ILCS 730/) Blockchain Technology Act.
[81] https://www.government.nl/topics/european-union/the-netherlands-and-the-eu-internal-market
[82] https://joernlengsfeld.com/en/definition/digital-market/
[83] OECD defines an online platform as "a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet." https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en

f. '**Emerging Technology Committee'** means the Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Emerging Technology Committee;

f.i. Shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit;

j. '**Systemically Important Digital Intermediaries'** means dominant entities performing in digital markets, identified by their significant control over user data, high network effects, and substantial influence on user behaviour, based on evidence of control as notified by the Central Government;

k. '**User'** means any person(s) or entity that access or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and includes addressee and originator;

**** Refer to Appendix 2 for a comparative analysis of definitions in model laws from other jurisdictions***

Chapter 4: Online Harms and Rights

4.1. Research analysis – Tackling online harms

Summary of Recommendations:

1. Identify user harm for artificial and natural persons, vulnerable groups and map proportionate response and redressal mechanisms.

2. Identify scope of online harms not covered under existing legal provisions such as IPC and Competition Act. This would include damage to computer systems, tampering with computer source documents, etc.

4. Map out categories of actual and perceived harms to different age groups and across intermediaries. This should be done on the basis of evidence gathered on effects of online harms by Self-Regulatory Bodies (SRBs).

5. Platforms can develop mechanisms for users to control content they want to see and who they engage with.

6. Platforms can develop mechanisms to enforce age limits and age-checking measures for children.

7. Platforms can perform transparent risk assessment on measures taken to protect children from harm and also allow parents to monitor their online activities.

8. Platforms should publish annual accountability reports on the effectiveness of safety measures including metrics on prevalence

of harmful content on platforms and user reports resolved.

9. SROs should be tasked with:
   - Identifying relevant user harms for intermediaries
   - Reviewing third-party audits of online safety measures taken by platforms.

Background

The Internet space has a lot of potential for driving India's economic development, but it is also fraught with challenges for user safety in terms of both psychological and financial harms. In order to create a safe and trusted space for an Internet user, the upcoming Digital India Act needs to address these user harms in a way that does not stifle innovation. Numerous international legislations contain provisions for regulation of online harms. Some of these provisions could be useful in the Indian context as well. This article provides recommendations on how the Digital India Act can tackle online harm in a way that boosts the digital economy and provides a trusted space for Internet users.

Introduction

Decades after the Internet came into existence, there is global recognition of the harms it poses to users. While the internet and internet-enabled technologies grew at a scorching pace, there has been a proportional rise in all kinds of harms that affect a multitude of users, thus posing complex challenges for regulators and policy makers. Policy makers have to balance protecting users, without stifling innovation and the digital economy.

For some, it is as simple as providing a safe space for users, while for others it could be an issue of national security. The very existence of the internet and its growth is predicated on the premise that it is a safe and trusted space. This is also the bedrock of a growing digital economy and for India's proposed Digital India Act (DIA), a key requirement to achieve a trillion-dollar digital economy by 2026.

While India's laws have recognised user harm in 2021, the DIA offers scope for a more nuanced and effective mechanism to address it. The Information Technology (IT) Act, 2000 does provide us a definition of "user" which is more precise in terms of information technology than the one provided by UK legislations, there are several key concepts that are still missing from the current regulatory landscape in India. The IT Rules 2021 imply "user harm" to mean any effect which is detrimental to a user or a child. This definition is very broad and fails to recognise the degrees of harm that need proportionate protections for users.

Most jurisdictions have special provisions for dealing with harms affecting children and minors. However, there is no definitional clarity in Indian law of the age groups that might be more susceptible to certain kinds of online harm. The definition of a "child" in current Indian legislation is a person under 18 years of age. For instance, the UK legislation aims to protect minors from being exposed to harmful content by restricting minors from using social media, but the age limits have not been defined. This will not only help platforms to define their users better, while also creating specific protections commensurate with the kind of harms minors could face.

Types of harmful content

Some jurisdictions have provided for a certain kind of classification for what it considers harmful content. These classifications may be based on the size of the platforms, the levels of harm caused by different types of platforms, and so on.

A lot of the jurisdictions require platforms to take steps in relation to illegal content, regarding radicalization or child sexual abuse material (CSAM). Some jurisdictions go beyond this and aim to regulate content that is "lawful but harmful", such as disinformation (EU, Singapore and the UK) or the promotion of eating disorders (Singapore, Ireland and the UK). Due to concerns about restricting free speech, obligations in respect of "legal but harmful" content for adults have been removed from UK's Online Safety Bill. Even so, the UK and Irish proposals and the Singaporean regime seek to cover the broadest category of harms.

What falls within the purview of illegal content and legal but harmful content varies significantly from jurisdiction to jurisdiction. This is largely decided on the basis of local cultural, social and political considerations. Therefore, an emerging economy such as

India has to carefully curate its list of harmful content particular to its aspirations and socio-cultural considerations.

The UK's Online Safety Bill, requires platforms to remove content relating to: CSAM, controlling or coercive behavior, cyber bullying, extreme sexual violence, extreme violence against animals or people, fraud, hate crime and speech, inciting violence, illegal immigration and people smuggling, promoting or facilitating suicide, promoting self-harm, revenge porn, selling illegal drugs or weapons, sexual exploitation, and terrorism. This Bill goes a long way in outlining different categories of content that are harmful to children and adults. It provides definitions for:

- illegal content
- primary and priority content harmful to children and adults
- pornographic content, among others

Although this classification might be useful in understanding varying levels of harm associated with different types of content, it might also be difficult to implement. This is so because the categorisation is complex and arbitrary. Instead of following this approach, a better method would be to categorise content into two or three categories based on the grievousness of harm caused, such as illegal content, legal but harmful content, and so on.
In Singapore, for instance, the Code of Practice for Online Safety and the Content Code for Social Media Services implements safety standards for six types of content: sexual content, violent content, self-harm content, cyber-bullying content, content that endangers public health and content that facilitates vice and organised crime. The Online Safety Bill in Singapore has also defined certain categories of content as "Egregious content". This includes content that advocates suicide or self-harm, violence or cruelty to human beings, content that exploits the nudity of a child, and content that advocates engaging in conduct that obstructs any public health measure carried out in Singapore.

By providing broad categories of content that are considered harmful and providing a clear definition of "Egregious content", Singapore's legislation makes it easier for platforms to create tools that enable them to comply with these directives better.

Similarly, the proposed DIA can consider defining different categories of illegal and harmful content to better equip platforms to

monitor them. India's digital landscape has to be cognizant of an emerging category of harms such as addictive tech and content that leads to promotion of suicide or self-harm, among others. Different categories of harms require different sets of responses, and the same regulatory body cannot form mechanisms to address all the harms.

In February 2021, the Indian government introduced new rules under the existing framework of the IT Act, called the "I**ntermediary Guidelines and Digital Media Ethics Code.**" Under these rules, the kind of content that are required to be regulated by Intermediaries includes:

Obscene, pornographic or paedophilic content, or content that is invasive of another's privacy.
Gender, **racially or ethnically objectionable content or** content that **promotes money laundering or gambling.**

- Content that is **harmful to child or** i**nfringes any intellectual property rights** is also required to be regulated.

Misinformation/ Disinformation

- **Content that threatens the unity, integrity, defence, security or sovereignty of India**
- Contains software virus or any other computer code, file or program designed to interrupt, destroy or **limit the functionality of any computer resource**;
- Content that is in the nature of an online game that is relating to **gambling or betting or the age** at which an individual is competent to enter into a contract;

These guidelines also place an additional burden on Significant Social Media Intermediaries (SSMIs) to remove content after receiving an order from a competent court or regulatory authority on content that is:

- Damaging to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order
- Related to rape, sexually explicit material or child sexual abuse material.
- any information which is identical to information that has previously been removed.

This can be interpreted as Illegal content. The onus of addressing illegal content should not just fall on SSMI's alone, but all other kinds of intermediaries. Furthermore, there needs to be an additional classification of legal but harmful content or underage

exposure to legal content (such as certain kinds of obscene content).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 contains a provision for addressing user harm, although the harms that it addresses have been mentioned previously in the IT Act. The most significant change is the extension of the obligations of intermediaries to include gaming intermediaries. Through this amendment, gaming intermediaries have been brought under the ambit of intermediaries and would have the same due diligence obligations that other intermediaries, such as social media intermediaries, would have for addressing user harms. However, this amendment delegates the development of a framework for addressing these user harms on a self-regulatory body. Sec 4A (8) requires every registered self-regulatory body to evolve a framework to include suitable criteria regarding—

- the content of an online game registered with a view to **safeguard users against harm, including self-harm**;
- appropriate measures to be undertaken to **safeguard children;**
- measures to safeguard users against the risk of **gaming addiction and financial loss**, including repeated warning messages at higher frequency beyond a reasonable duration for a gaming session, provision to enable a user to exclude himself upon user- defined limits for time and money spent; and
- measures to safeguard against the **risk of financial frauds**.

As per these rules, the self-regulatory body for gaming will be responsible for safeguarding users against the risk of gaming addiction, financial loss, and fraud. Since user safety is a priority for both legislators and users, the principles of “responsible play” will have to be developed by SRBs. A report by Federation of Indian Fantasy Sports (FIFS) recommends the implementation of guardrails to protect users from psychological and financial harm. Examples of some such measures could be: a mandatory KYC for paying participants to gatekeep minors and prevent duplicate accounts, algorithmic identification of potentially risky behavior, self-exclusion options, time-outs, and voluntary limits on time spent on these apps.

Gaps in Regulatory Framework

There are certain online harms that have been defined clearly in the Indian legislations and some that have a less clear definition. For instance, the term "obscene" is defined under Section 67 of the Information Technology Act, which criminalizes the publishing or transmitting of obscene material in electronic form. However, the act does not provide an explicit definition of what constitutes "obscene" content. The interpretation of obscenity is often based on community standards, public morality, and case law precedents.

Courts in India have relied on the three-pronged test established by the Supreme Court in the landmark case of Ranjit Udeshi v. State of Maharashtra (1965) to determine obscenity. According to this test, content is considered obscene if it appeals to prurient interests, violates contemporary community standards, and lacks any redeeming artistic, literary, scientific, or social value.

However, it's important to note that the interpretation of obscenity can vary, and what may be considered obscene in one context or community may not be considered so in another. This subjective nature of the definition can sometimes lead to challenges in effectively regulating and addressing online obscenity. While there are provisions in Indian legislations that address certain online harms like obscene content, the precise interpretation and application of these provisions can vary, and clarity in defining certain online harms remains an ongoing challenge.

Therefore, in certain cases, a single offense may fall under the purview of multiple legislations. For example, an act of cyberbullying that involves harassment, intimidation, and threats may attract provisions from both the IT Act and the IPC. This makes it difficult for the law enforcement agencies and the judiciary to choose the appropriate legal provisions based on the nature of the offense and the specific circumstances.

Measures to be implemented to safeguard against user harm

India's IT Act and subordinate Rules do contain provisions for platforms to remove content on the directives of the Government and empowers users to report harmful content on different platforms. Even so, there is a need to implement better standards for measures that should be taken by intermediaries to address illegal and harmful content. Platforms should be required to produce and publish annual accountability reports on the effectiveness of their safety measures. These could include metrics on how prevalent harmful content is on their platforms, user reports they received and acted on, and the process to address harmful content. These measures would ensure that the principles of user empowerment and risk mitigation will be followed.

In UK's Online Safety Bill, the largest and riskiest Category 1 service providers (such as some social media platforms) will be required to offer adult users tools so they can have greater control over the kinds of content they see and who they engage with online. These tools could include human moderation, blocking content flagged by other internet users or sensitivity and warning screens.

In EU, the Digital Services Act sets out effective means for all actors in the online ecosystem to counter illegal content as well as illegal goods and services. A priority channel is created for trusted flaggers (entities which have demonstrated expertise and competence) to report illegal content to which platforms will have to react with priority. When enabled by national laws, Member State authorities will be able to order any platform operating in the EU to remove illegal content.

In Singapore, the Online Safety Bill grants power to Singapore's Infocomm Media Development Authority (IMDA) to direct any social media services to disable user access to what the Government deems as 'extremely harmful content', which is determined as content that is related but not limited to suicide and self-harm, sexual harm, public health, public security, and racial or religious disharmony or intolerance, and to disallow specified online accounts from communicating with users in Singapore.

Measures specifically aimed at Children

It is clear that there is scope for the DIA to produce a more nuanced legislative framework that provides a higher degree of protection

to children, minors and other vulnerable groups from illegal and harmful content, especially as India is demographically a youthful country. It also needs more research to determine who falls under the vulnerable groups category (for instance, divorced/widowed women, orphans, and transgenders). Another important classification that the proposed DIA should address is age segregation among non-adults under 18 years. This would be useful in creating regulations to ensure that minors in a certain category, for instance, under 15, are not allowed on specific platforms such as social media sites.

Measures such as those taken in the UK and Singapore would be effective in mitigating some harms that these groups are more susceptible to. In Singapore, platforms are required to have tools that allow parents and guardians to limit who can connect with their children on social media. It also offers filters that limit what is viewed online, that can be activated by default for users below the age of 18.

Penalties for User Harm

Different jurisdictions have different kinds of penalties for user harm (or contravening any other provisions of their IT legislations). The EU imposes a monetary penalty as well as temporarily limits access to the platform's services. Singapore imposes a monetary penalty, possibility of corporate criminal liability and additionally, requires directors to take down, disable or correct content.

Jurisdiction	Potential Maximum Fine for the Platform	Possibility of Corporate Criminal Liability	Possibility of liability for individual directors or employees	Other enforcement tools
EU	Up to 6% of global annual turnover, where a provider has been	No	No	-Requiring commitments from platforms that they will make their services compliant

	found to breach its obligations For VLOPs, periodic penalty payments up to 5% of the average daily turnover in the preceding financial year per day			-Temporarily restricting access to the platform's services Periodic penalty payments of up to 5% of the average daily turnover of the platform
United Kingdom	~22 million USD or up to 10% of global annual turnover, whichever is higher, for "failure to comply" with regulatory obligations	No	Yes	-Compel third parties to withdraw key services that make it less commercially viable for the company to operate within the jurisdiction
Singapore	USD 738,000 per non-compliance with a ministerial direction	Yes	Yes	Directions to take down, disable or correct content

The overarching framework for penalties for causing user harm suggests that the loss of safe harbor provision is an extreme measure. This would not be conducive to promoting digital business in India. The Jan Vishwas Bill aims to simplify the compliance requirements for businesses and reducing corporate criminal liability in certain cases with the aim of enhancing investment opportunities. Monetary penalty seems to be the best way to address user harm, with the option of limiting access to the platform's services only when there is evidence of repeated breaches. The principle of proportionality should be observed while devising penalties for user

harm. This will also ensure asymmetrical obligations on intermediaries causing different levels of harm to users. Asymmetrical obligations means that platforms causing higher levels of user harm would have more responsibilities in terms of developing content monitoring and risk assessment tools. They would also have to face higher penalties in cases of contraventions of the regulation's directives, because the magnitude of their effect on users is greater.

4.2. Principles of online harms and rights

1. Proportional Measures and Penalties

1.1 Proportionality of the regulations and interventions to the severity of the harm

1.2 Provide safeguards for individual rights and freedoms.

1.3 Define rationale for penalties that do not infringe on fundamental rights.

1.4 Regulators deploy necessary and effective measures for tackling online harms that:

1.4.1 Consider alternative approaches

1.4.2 Minimize unnecessary infringement on fundamental rights

(Explanation: The tools for mitigating online harm must be developed without placing undue burdens on intermediaries. Adequate safeguards and regular reviews should be established to protect against abuses and ensure ongoing accountability)

2. Risk Assessment and Management

2.1 Regulatory, including self-regulatory bodies to undertake systematic evaluation of potential risks associated with different types of harm

2.2 Periodic assessments by regulatory, including self-regulatory bodies, enabling the industry to identify:

2.2.1 Specific risks

2.2.2 Likelihood of these risks

2.2.3 Potential impact

2.3 Based on periodic assessments, the regulatory including self-regulatory bodies, must:

2.3.1 Implement appropriate strategies and measures to mitigate and manage the identified risks

2.3.2 Monitor and evaluate to adapt to evolving threats

2.3.3 Ensure efficacy of risk management measures

3. User Empowerment

3.1 Equip users with knowledge, tools, and resources to safely navigate digital landscapes

3.1.1 Providing accessible reporting mechanisms for reporting harmful content

3.1.2 Enabling content moderation options

3.1.3 Offering transparent and user-friendly privacy settings

3.2 User-centric design to promote user agency and control over online engagement

3.3 Measures to address misinformation and disinformation

(Explanation: Measures such as community standards or reporting which can provide factual context to claims and assertions on platforms)

4. Transparency and Accountability

4.1 Provide clear communication about the policies, procedures, and enforcement of actions related to harmful content

4.1.1 Platforms should provide users with easy-to-understand and accessible guidelines on acceptable behavior and content standards.

4.1.2 Ensure consistent and fair enforcement of their policies

(Explanation: Regular reporting on content moderation practices – including the number of flagged and removed posts – promotes transparency, accountability and builds public trust. External audits and independent oversight mechanisms can further strengthen accountability)

5. Human Rights and Due Process

5.1 Protect fundamental rights, such as freedom of expression, privacy, and equality

5.2 Adhere to the established legal frameworks and due process while developing measures to address online harm

5.2.1 Ensure users are provided with fair and transparent procedures, such as a Grievance Redressal Mechanism

(Explanation: Safeguards should be in place to prevent arbitrary or disproportionate actions that may infringe upon these rights)

4.3. User Rights

1. **Right to be forgotten**

(Explanation: The right to be forgotten or the right to erasure is a concept that grants individuals the power to request the removal or deletion of their personal information from online platforms, search engines and other internet mediums. It is closely associated with the right to privacy and data protection in the digital age)

1.1 Balance privacy with public interest, especially when personal information becomes:

1.1.1 Outdated

1.1.2 Inaccurate

1.2.3 No longer serves a legitimate purpose

1.2 Reasonable restrictions should be applied on the grounds of:

1.2.1 Right to freedom of expression and information

1.2.2 Compliance with legal obligations

1.2.3 Performance of tasks in the public interest (such as public health)

1.2.4 Scientific or historical research purposes or statistical purposes

1.2.5 Exercise or defence of legal claims

2. **Right to digital inheritance**

(Explanation: The right to digital inheritance refers to the ability of individuals to transfer or manage their digital assets and online accounts after their death)

2.1 Establish a legal framework for granting fiduciaries (such as executors or trustees) access to a deceased person's digital assets.

2.2 Allow users to specify preferences regarding the disclosure or non-disclosure of digital assets in their estate planning documents.

3. Right against discrimination

(Explanation: The right against discrimination includes ensuring equal treatment and non-discrimination in accessing and using digital services. This would include ensuring equal access, opportunities, and treatment for all individuals in the digital realm)

3.1 Prohibition of discriminatory practices based on considerations such as race, colour, gender, religion, sexual orientation, disability, or other factors. This includes addressing hate speech, online harassment, cyberbullying and other harmful acts that target individuals or groups based on these characteristics.

3.2 The right against discrimination to include procedural safeguards that promote **transparency, accountability and due process.**

4. Rights against automated/arbitrary decision-making

(Explanation: The use of automated decision-making systems, such as algorithms and artificial intelligence are associated with risks of potential bias and lack of transparency. Rights against automated decision-making are crucial in ensuring transparency, accountability, and fairness in the use of algorithms and artificial intelligence systems)

4.1 Protect individuals from potential biases, discrimination, and negative consequences that may arise from automated decision-making processes.

4.1.1 Protect user privacy and personal data in the context of automated processing by ensuring fair and lawful processing of personal data, including automated decisions.

5. Right to privacy

5.1 Right to privacy was established in the case of *Justice K.S Puttaswamy and Ors. vs Union of India & Ors.* To safeguard this fundamental right, there is a need for:

5.1.1 Comprehensive data protection legislation

5.1.2 Encryption technologies

5.1.3 Individual control over digital footprints

4.4. Definitions - Online Harms and Rights

Definitions.- In this Act, unless the context otherwise requires,-

(a) **"Deepfakes"**[84] means artificial intelligence-generated synthetic media where a person in an image or video is swapped with another person's likeness;

(b) **"Disinformation"**[85] means false information that is intended to manipulate, cause damage, or guide people, organisations, and countries in the wrong direction;

(c) **"Harassment"**[86] means any type of threatening, abusive, or insulting words, behaviour, or communication patterns transmitted through digital channels with the intention to cause distress or harm to others;

(d) **"Illegal content"** means content that amounts to a relevant offence, or content that contravenes any law for the time being in force. This may include content that causes incitement to the commission of any cognizable offence or prevents investigation of any offence;

(e) **"Inappropriate and harmful content"** means content that may be legal but is still harmful. This includes content that is
   (I) harassing on the basis of gender, racially or ethnically objectionable
   (II) Misinformation, Disinformation and Malinformation;

(f) **"Misinformation"**[87] means false information that is not intended to cause harm;

(g) **"Malinformation"**[88] means information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm;

[84] MIT Sloan School of Management, https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained
[85] Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf
[86] UN Broadband Commission, https://www.broadbandcommission.org/wp-content/uploads/2021/02/WGGender_Executivesummary2015.pdf
[87] Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf
[88] Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf

(h) **"User"**[89] means any person(s) or entity that access or avails any computer resource for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information;

(i) **"User harm"**[90] means any bodily or mental harm caused due to, but not limited to, distortion of information, theft of identity, discrimination, harassment, loss of life, loss of privacy, reputation or employment, disruption in operations or prevention of lawful gain or causation of significant loss, infringement of fundamental rights;

Refer to Appendix 3 for a comparative analysis of definitions in model laws from other jurisdictions

[89] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: "user" means any person who accesses or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and includes other persons jointly participating in using such computer resource and addressee and originator

[90] The Digital Personal Data Protection Bill, 2022 : "Harm", in relation to a Data Principal, means - (a) any bodily harm; or (b) distortion or theft of identity; or (c) harassment; or (d) prevention of lawful gain or causation of significant loss.

Appendix I. Jurisdictional Comparison of Definitions for Intermediary liability and classification

IT Act/Rules, Section/Rule 2(1)	EU Digital Services Act	UK Online Safety Bill	Australia's Online Safety Act, 2021	Key Elements
Intermediaries and Intermediary services				
(w)**'intermediary'**, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting	'intermediary service' means one of the following services: a 'mere conduit' service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; a 'caching' service that consists of the	"User-to-user service" and "search service" (1) In this Act "user-to-user service" means an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service. (2) For the purposes of subsection (1)— (a) it does not matter if content is actually shared with another user or users as long as a service has a	-	• 3 Models of classification should be considered: 1.Classification based on technical functions Intermediaries operate across the Internet stack and have different underlying technologies. 2. Classification based on nature of services • Helps regulate the impact of different types of services. • From the prism of user harms, 2 more factors are critical: i. Use-cases ii. Network effects

service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.	transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; a 'hosting' service that consists of the storage of information provided by, and at the request of, a recipient of the service;	functionality that allows such sharing; (b) it does not matter what proportion of content on a service is content described in that subsection. 4) In this Act "search service" means an internet service that is, or includes, a search engine (see section 230). (5) Subsections (6) and (7) have effect to determine whether an internet service that—(a) is of a kind described in subsection (1), and (b) includes a search engine, is a user-to-user service or a search service for the purposes of this Act. (6) It is a search service if the only content described in subsection (1) that is enabled by the service is content of any of the following kinds—		3. Classification of new and emerging technologies • Separate category to enable regulators, innovators and technologists to work together and build new frameworks.

		(a) content mentioned in paragraph 1, 2 or 3 of Schedule 1 (emails, SMS and MMS messages, one-to-one live aural communications) and related identifying content; (b) content arising in connection with any of the activities described in paragraph 4(1) of Schedule 1 (comments etc on provider content); (c) content present on a part of the service in relation to which the conditions in paragraph 7(2) of Schedule 1 are met (internal business service conditions). (7) Otherwise, it is a user-to-user service. **227 Provider of internet service** User-to-user services (other than combined services) (2) The provider of a user-to-		

		user service is to be treated as being the entity that has control over who can use the user-to-user part of the service (and that entity alone). (3) If no entity has control over who can use the user-to-user part of a user-to-user service, but an individual or individuals have control over who can use that part, the provider of the service is to be treated as being that individual or those individuals. Search services (4) The provider of a search service is to be treated as being the entity that has control over the operations of the search engine (and that entity alone). (5) If no entity has control over the operations of the search engine, but an		

		individual or individuals have control over those operations, the provider of the search service is to be treated as being that individual or those individuals. Combined services (6) The provider of a combined service is to be treated as being the entity that has control over both— (a) who can use the user-to-user part of the service, and (b) the operations of the search engine, (and that entity alone). (7) If no entity has control over the matters mentioned in paragraphs (a) and (b) of subsection (6), but an individual or individuals have control over both those matters, the provider of the combined service is to be treated as being that		

		individual or those individuals.		
(w) 'social media intermediary' means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;			**Social media service** – "(a) an electronic service that satisfies the following conditions: (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users; (ii) the service allows end-users to link to, or interact with, some or all of the other end-users; (iii) the service allows end-users to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules;"	- the purpose of the service is to enable online interaction between two or more users.

(v) 'Significant social media intermediary' - means a social media intermediary having number of registered users in India above such threshold as notified by the Central Government.	**'Very large online platforms'** - "online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3. The Commission shall adopt delegated acts in accordance with Article 69 to adjust the number of average monthly			The Act needs to prescribe a formula to account for network effects. Periodic impact assessments would be useful to reveal other impact of these intermediaries and allow for better regulation.

	recipients of the service in the Union referred to in paragraph 1, where the Union's population increases or decreases at least with 5 % in relation to its population in 2020 or, after adjustment by means of a delegated act, of its population in the year in which the latest delegated act was adopted. In that case, it shall adjust the number so that it corresponds to 10% of the Union's population in the year in which it adopts the delegated act,			

	rounded up or down to allow the number to be expressed in millions. The Commission shall adopt delegated acts in accordance with Article 69, after consulting the Board, to lay down a specific methodology for calculating the number of average monthly active recipients of the service in the Union, for the purposes of paragraph 1. The methodology shall specify, in particular, how to determine the Union's population			

	and criteria to determine the average monthly active recipients of the service in the Union, taking into account different accessibility features. The Digital Services Coordinator of establishment shall verify, at least every six months, whether the number of average monthly active recipients of the service in the Union of online platforms under their jurisdiction is equal to or higher than the number referred to in paragraph 1. On the basis of that			

	verification, it shall adopt a decision designating the online platform as a very large online platform for the purposes of this Regulation, or terminating that designation, and communicate that decision, without undue delay, to the online platform concerned and to the Commission. The Commission shall ensure that the list of designated very large online platforms is published in the Official Journal of the European Union and keep that list updated.			

	The obligations of this Section shall apply, or cease to apply, to the very large online platforms concerned from four months after that publication."			
-		**Internet service** - "(1) In this Act "internet service" means a service that is made available by means of the internet. (2) For the purposes of subsection (1) a service is "made available by means of the internet" even where it is made available by means of a combination of— (a) the internet, and (b) an electronic	**'Internet service provider'** – "For the purposes of this Act, if a person supplies, or proposes to supply, an internet carriage service to the public, the person is an internet service provider." **internet carriage service** means a listed carriage service that enables end-users to access the internet..	The definition should cover the technical function of an internet service provider. OECD[91] - A company which provides end-users with a data connection allowing access to the internet and the associated services.

[91] https://data.oecd.org/ict/internet-access.htm

		communications service. (3)Electronic communications service" has the same meaning as in the Communications Act (see section 32(2) of that Act)."		
-		**'Search engine'** "(1) In this Act "search engine"— (a) includes a service or functionality which enables a person to search some websites or databases (as well as a service or functionality which enables a person to search (in principle) all websites or databases); (b) does not include a service		Internet search engines[92] and portals operate websites that use a search engine to generate and maintain extensive databases of Internet addresses and content in an easily searchable format. Content may consist of web pages, images or other types of digital files. (OECD, 2014) **Search Engine[93] - software** (3.1.12.14) searching the **internet** (3.1.9.01) for **digital documents** (3.3.3.02) or pieces

[92] https://www.oecd.org/digital/ieconomy/44949023.pdf
[93] https://www.iso.org/obp/ui#iso:std:iso:5127:ed-2:v1:en:term:3.3.3.02

		which enables a person to search just one website or database. (2) For the purposes of this Act, a search engine is not to be taken to be "included" in an internet service or a user-to-user service if the search engine is controlled by a person who does not control other parts of the service."		thereof requested by an **information user** (3.11.2.05) **information** (3.1.1.16) unit with a defined content that has been digitised or was originally produced in digital form
-		**'Proactive technology'** – "(1) In this Act "proactive technology" means— (a) content identification technology, (b) user profiling technology, or (c) behaviour identification technology, but this is		Content identification technology should be classified on the basis of proactiveness. Aspects of user-profiling, such as analysis of metadata should be incorporated. Legally mandated age-verification should not be part of user-profiling technology.

		subject to subsections (3) and (7)." **'Content identification technology'** means technology, such as algorithms, keyword matching, image matching or image classification, which analyses content to assess whether it is content of a particular kind (for example, illegal content). But content identification technology is not to be regarded as proactive technology if it is used in response to a report from a user or other person about particular content.		

		'User profiling technology' means technology which analyses (any or all of)— (a) relevant content, (b) user data, or (c) metadata relating to relevant content or user data, for the purposes of building a profile of a user to assess characteristics such as age. Technology which— (a) analyses data specifically provided by a user for the purposes of the provider assessing or establishing the user's age in order to decide whether to allow the user to access a service (or part of a service) or particular content, and (b) does not analyse any other data or		

		content, is not to be regarded as user profiling technology. **'Behaviour identification technology'** means technology which analyses (any or all of)— (a) relevant content, (b) user data, or (c) metadata relating to relevant content or user data, to assess a user's online behaviour or patterns of online behaviour (for example, to assess whether a user may be involved in, or be the victim of, illegal activity). But behaviour identification technology is not to be regarded as proactive technology if it is used		

		in response to concerns identified by another person or an automated tool about a particular user.		
-	**'Mere conduit'-** "a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;"			This consists of "the transmission in a communication network of information provided by a recipient of the service., The ISP is playing a passive role in such activities by acting as a mere "carrier" of data provided by third parties through its network. The second type of mere conduit activity is commonly known as "providing Internet access." Mere conduit activities include the automatic, intermediate and transient storage of the information transmitted, in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the

				information is not stored for any period longer than is reasonably necessary for the transmission.
-	**'Caching'** - "a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients			Classification based on technical functions performed by intermediaries on the Internet stack is required.

	upon their request;"			
-	**'Hosting'** - "a hosting service, consisting of the storage of information provided by, and at the request of, a recipient of the service;"		**'Hosting service provider'** – "a person who provides a hosting service." Hosting service has been defined in S. 17 as – "(a) a person (the first person) hosts stored material that has been provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the first person or another person provides: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service;	Classification based on technical functions performed by intermediaries on the Internet stack is required.

			on which the hosted material is provided." **'Australian hosting service provider'** – "a person who provides a hosting service that involves hosting material in Australia."	
2(qa) 'online game' means a game that is offered on the Internet and is accessible by a user through a computer resource or an intermediary. Explanation.—In this clause, 'Internet' means the combination of computer facilities and electromagnetic				• The definition should specify "skill-based game" in order to remove any confusion between the Centre and State lists. • Real money games need to be well-defined. • Explanation of prize pool, service fee, winnings are essential to lend regulatory clarity.

transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that transmits information based on a protocol for controlling such transmission; **2(qb) 'online gaming intermediary'** means any intermediary that enables the users of its computer resource to access one or more online games.				

-	**'Online platform'** - means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the			• Online platforms are built on top of the Application layer of the Internet stack. They need to be defined. • The definition would also allow to further categorise the types of services offered by online platforms.

	applicability of this Regulation.			
Cloud service provider				Cloud computing[94] is a service model that provides clients with flexible, on-demand access to a range of computing resources (OECD, 2014) Cloud computing[95] is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, 2011)

[94] https://www.oecd-ilibrary.org/docserver/5jxzf4lcc7f5-en.pdf?expires=1690344929&id=id&accname=guest&checksum=54E63AADA61BC49C4A24BF9384657BD4

[95] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

				Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. (ITU,
Users				
(x) 'user' means any person who accesses or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and	**'Recipient of the service'** means any natural or legal person who uses the relevant intermediary service; **'consumer'** means any natural person who is acting for purposes which are outside his or her trade, business or profession;	'**User'**, '**United Kingdom user' and 'interested person'** (1) For the purposes of this Act a user is a "United Kingdom user" of a service if— (a) where the user is an individual, the individual is in the United Kingdom; (b) where the user is an entity, the entity is incorporated or formed under the law of any part of the United Kingdom.	-	• Identification of users as individuals or entities is required. • Inclusion of negative definitions is required to identify who shall not qualify as a user. • Identification of consumers as a subset of users is required. This will validate the economic identity and rights of users.

includes other persons jointly participating in using such computer resource and addressee and originator; **(y) 'user account'** means the account registration of a user with an intermediary or publisher and includes profiles, accounts, pages, handles and other similar presences by means of which a user is able to access the services offered by the intermediary or publisher.		(3) References in this Act to a user of a service do not include references to any of the following when acting in the course of the provider's business— (a) where the provider of the service is an individual or individuals, that individual or those individuals; (b) where the provider is an entity, officers of the entity; (c) persons who work for the provider (including as employees or volunteers); (d) any other person providing a business service to the provider such as a contractor, consultant or auditor.		

Content				
-	-	**'publish'** means publish by any means (including by broadcasting), and references to a publisher and publication are to be construed accordingly;		• A clear definition of the act of "publish" is required from a platform liability perspective. This will help clarify the activities that separate intermediaries from publishers.
Rule 3(2) 'prominently publish' shall mean publishing in a clearly visible manner on the home page of the website or the home screen of the mobile based application, or both, as the case may be, or on a web page or an	-	-		• This definition is suitable for India's due diligence framework.

app screen directly accessible from the home page or home screen.				
(g) 'content' means the electronic record defined in clause (t) of section 2 of the Act; —electronic record‖ means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche; **(i) 'digital media'** means digitized	-	**'content'** means anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description; **'Regulated user-generated content'**, in relation to a regulated user-to-user service, means user-generated content, except— (a) emails, (b) SMS		• Clear description of the various forms online content may take is required. • Clear identification of content that is not to be regulated by the Centre, such as comments and reviews, is required.

content that can be transmitted over the internet or computer networks and includes content received, stored, transmitted, edited or processed by- (i) an intermediary; or (ii) a publisher of news and current affairs content or a publisher of online curated content; **(q)'online curated content'** means any curated catalogue of audio-visual content, other than news and		messages, (c) MMS messages, (d) one-to-one live aural communications (see subsection (5)), (e) comments and reviews on provider content (see subsection (6)), (f) identifying content that accompanies content within any of paragraphs (a) to (e), and (g) news publisher content (see subsection (8)).		

current affairs content, which is owned by, licensed to or contracted to be transmitted by a publisher of online curated content, and made available on demand, including but not limited through subscription, over the internet or computer networks, and includes films, audio visual programmes, documentaries, television programmes, serials, podcasts and other such content				

-	**'illegal content'** means any information,, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law;	-	-	• Clear identification of illegal content is required for India's intermediary liability regime. This will prevent platforms from having to adjudicate on the legal validity of content.
Content Moderation/take down- not defined	**'content moderation'** means the activities undertaken by providers of intermediary services aimed at	references to "**taking action" in relation to content** are to— (i) taking down content, (ii) restricting users' access to content, or (iii) taking other action in relation to content		• Activities involved in content moderation require definition for legal clarity. • Clear definition of taking action against content or against a person is required.

	detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination	(for example, adding warning labels to content); **"taking down" (content)**: any reference to taking down content is to any action that results in content being removed from a user-to-user service or being permanently hidden so users of the service cannot encounter it (and related expressions are to be read accordingly); References to "**taking action" against a person** are to giving a warning to a person, or suspending or banning a person from using a service, or in		• Clear identification of what qualifies as "taking down" content is required. • Clear definition of any other action taken in relation to content, such as adding warning labels, is required. • Identification of what qualifies as taking action against a person is needed, and may include the following: – Giving a warning – Suspending or banning – Restricting a person's ability to use a service

	or suspension of a recipient's account;	any way restricting a person's ability to use a service		
(m) 'news and current affairs content' includes newly received or noteworthy content, including analysis, especially about recent events primarily of socio-political, economic or cultural nature, made available over the internet or computer networks, and any digital media shall be news and current affairs content where the context,	-	**'news-related material"** means material consisting of— (a) news or information about current affairs, (b) opinion about matters relating to the news or current affairs, or (c) gossip about celebrities, other public figures or other persons in the news;		• No change required to the definition.

substance, purpose, import and meaning of such information is in the nature of news and current affairs content.				
-	**'advertisement'** means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and displayed by an online platform on its online interface against remuneration specifically for	-		• A definition of advertisement is required that accurately captures various aspects of digital advertisements.

	promoting that information;			
Oversight and Grievance Redressal				
-	-	A service restriction order is an order imposing requirements on one or more persons who provide an ancillary service (whether from within or outside the United Kingdom) in relation to a regulated service. An interim service restriction order is an interim order imposing requirements on one or more persons who provide an ancillary service (whether from within or outside the United Kingdom) in		• Clear definition of orders or notices is required. This will help determine a baseline standard for actual knowledge. • The definition requires identification of the entities on whom orders can be imposed, and in relation to what.

		relation to a regulated service. An access restriction order is an order imposing requirements on one or more persons who provide an access facility (whether from within or outside the United Kingdom) in relation to a regulated service. An interim access restriction order is an interim order imposing requirements on one or more persons who provide an access facility (whether from within or outside the United Kingdom) in relation to a regulated service.		

(e) 'committee' means the Inter-Departmental Committee constituted under rule 14 **(j) 'grievance'** includes any complaint, whether regarding any content, any duties of an intermediary or publisher under the Act, or other matters pertaining to the computer resource of an intermediary or publisher, as the case may be; **(k) 'Grievance Officer'** means an	-	-		• Existing definitions are suitable.

officer appointed by the intermediary or the publisher, as the case may be, for the purposes of these rules; **(ka) 'Grievance Appellate Committee'** means a grievance appellate committee constituted under rule 3A;". **(qc)'online gaming self-regulatory body'** means an entity designated as such under rule 4A;				

Appendix II. Jurisdictional Comparison of Definitions for Digital Competition and Emerging Technology

Key Terms	India Competition Act, 2002	UK Competition and Markets Authority	EU Digital Markets Act	Key Elements
Digital competition				
SIDIs **(Systemically Important Digital Intermediaries)**		In the UK, the concept of **strategic market status ("SMS")** was introduced by the Furman Report. "include firms that have obtained gatekeeper positions and have been enduring market power over the users of their products"and would be based on evidence.	**'gatekeeper'** means an undertaking providing core platform services, designated pursuant to Article 3.	1. The identification of a SIDI must be based on data dominance, High network effects, and user behaviour. 2. Identify SIDIs based on exclusionary practices, not only towards other businesses but also end-users. 3. the essential facilities doctrine could be used to ensure that dominant platforms do not abuse their power by refusing to provide access to their platforms to other companies. This would foster the concept of an open internet.
Digital Markets Unit (DMU)		*The DMU is established on a non-statutory basis, with a focus on preparing for a new regulatory regime for digital firms.*		1. Legislative powers should not be given to this body. 2. Will assess criterias based on which firms will be designated as SIDIs. 3. All decisions will be subject to judicial review.
Relevant market	**Section 2(r) 'relevant market'** means the market		**Germany revised its competition law in 2017** to adapt its legal	Competition authorities need to employ additional criteria for the definition of the

	which may be determined by the Commission with reference to the relevant product market or the relevant geographic market or with reference to both the markets;		framework and tools to the new features of the digital economy, and introduced a provision recognizing free products or services provided by platforms as a market, stating that "the assumption of a market shall not be invalidated by the fact that a good or service is provided free of charge"	relevant market in digital sectors.
Digital platforms[96]			**The European Commission has defined an online platform** as "an undertaking operating in two (or multi) sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups" **OECD** has defined online platforms as "a digital service that facilitates interactions between two or more distinct but interdependent sets of users	1. Multi-sided markets must be identified and specified as; * Entities that engage in digital spaces/marketplace 3. Shift from the 'online platform' definition to defining 'digital platforms' covers a broader spectrum of market players than restricting the ones who solely function online.

[96] **In Australia** – The ACCC does not define digital platforms but categorises digital platform services. Only so they can be assessed over a period of 5 years inquiry period.

			(whether firms or individuals) who interact through the service via the Internet."	
Users	**Section2(f) 'consumer'** means any person who-- (i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment when such use is made with the approval of such person, whether such purchase of goods is for resale or for any			It is necessary to define the term 'users' and it must be interpreted in a broad manner. Among those who use and benefit from digital platforms are not just individual consumers, but also employees, governments and businesses, both large and small, they may act as buyers or sellers. - Identification of users as individuals or entities. - Inclusion of negative definitions. - Identification of consumers as distinct from users (EU)- validates the economic identity and rights of users.

	commercial purpose or for personal use; (ii) hires or avails of any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first-mentioned person whether such hiring or availing of services is for any commercial purpose or for personal use			
Emerging Technologies				

Key Terms	India	USA Algorithmic Accountability Act of 2019	EU The Artificial Intelligence Act (AIA)	Key Elements
Emerging Technology				Recommended Definition - *digitally-enabled tools representing new and significant developments within a **particular field**.* - *Particular fields must be all inclusive of processes and functions of emerging technologies.*
Emerging Tech Committee			**European Innovation Council (EIC)** has been established to identify, develop and scale up emerging technologies and breakthrough innovations.	
AI systems	**Niti Ayog** - **"Narrow AI"** is a comprehensive label used to describe artificial intelligence systems specifically created to address specific problems that typically necessitate expertise in a particular field. This examination focuses solely on narrow AI, encompassing both technical aspects and societal implications.		**AI Act EU** '**Artificial intelligence system**'- a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions,	The definition of an AI system must: 1. Mention the significance of autonomy. - The evaluation of an AI system's performance must be based on accuracy, precision, and sensitivity.

			recommendations or decisions , influencing the environments with which the AI system interacts. **OECD** - **machine-based system** that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives.	
High Risk		**In the USA, the Algorithmic Accountability Act of 2019** is a proposed bill that requires specified commercial entities to conduct assessments of high-risk systems that involve personal information or make automated decisions, such as systems that use artificial intelligence or machine learning.	- **Chapter 1 of Title III (High-Risk AI Systems) of the EU AI Act.** The concept of "high- risk AI system" is not explicitly defined. Instead, a group of AI systems are classified as such provided that certain conditions are met.	Offences must be assessed based on the impact made.
Regulatory sandbox			A. 53 AI Act EU – *AI regulatory sandbox* https://eur-lex.europa.eu/legal-	1. Provide clear guidance tailored to each product or service under experimentation.

			content/EN/TXT/?uri=celex%3A52021PC0206 **OECD -** A regulatory sandbox refers to a limited form of regulatory waiver or flexibility for firms, enabling them to test new business models with reduced regulatory requirements. Sandboxes often include mechanisms intended to ensure overarching regulatory objectives, including consumer protection. Regulatory sandboxes are typically organised and administered on a case-by-case basis by the relevant regulatory authorities.	2. Encourage cooperation and alignment of regulations among different countries 3. Budgetary allocation of adequate funding 4. Assess environmental Impact (Sustainability) 5. Provisions pertaining to consumer interests and public safety to be held in highest of priority. 6. Inclusivity 7. Testing timeline and evaluation timeline must be provided to participants before entering a sandbox.
Empowered committee				1. An overseeing body that will monitor the sandboxing process from start to finish. 2. The members must be industry experts in the public as well as private sector, assigned by the regulator. The Law must have these factors enlisted, while assigning an empowering committee- • Functions • Duties

				• limitations

Appendix III. Jurisdictional Comparison of Definitions for Online harms and rights

IT Act, 2000 and Other Indian Laws	DSA (EU)	OSB (UK)	Australia	Singapore	Key Elements
User					
"**user"** means any person who accesses or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and includes other persons jointly participating in using such computer resource and	**"recipient of the service"** means any natural or legal person who uses the relevant intermediary service; **"consumer"** means any natural person who is acting for purposes which are outside his or	"**User**", **"United Kingdom user" and "interested person**" a user is a "United Kingdom user" of a service if— (a) where the user is an individual, the individual is in the United Kingdom; (b) where the user is an entity, the entity is incorporated or formed under the law of any		Broadcasting Act 1994: "end-user", in relation to an electronic service, means an individual who, or an entity that, and whether or not in the course of business — (a) has access to content or something which contains content; or (b) communicates content, or something which contains content, on	• Identification of users as individuals or entities. • Inclusion of negative definitions. • Identification of consumers as distinct from users (EU)- validates the economic identity and rights of users.

addressee and originator;	her trade, business or profession;	part of the United Kingdom.		or by means of the electronic service, but excludes a person who is prescribed by the Minister by order in the Gazette	
User Harm					
IT Act, 2000 and Other Indian Legislations	**DSA (EU)**	**OSB (UK)**	**Australia**	**Singapore**	**Key Elements**
"User harm" and "harm" mean any effect which is detrimental to a user or child, as the case may be				"harm" includes harm to an individual's mental health	• Needs to be more exhaustive White paper on Online Harms by UK Gov: 'online harm' has been defined as any online behavior or content that can cause

DPDP Bill 2022, the term 'harm', in relation to a data principal, has been defined under Section 2(10) to include 4 different categories, ranging from bodily harm to distortion or theft of identity to harassment, and even to prevention of lawful gain or causation of significant loss.					physical or emotional hurt to a person and **may result from harmful information that is posted online to that which is sent to any individua**l
Obscene Content					
IT Act, 2000 and Other Indian Legislations	**DSA (EU)**	**OSB (UK)**	**Australia**	**Singapore**	**Key Elements**
Section 292 (1), IPC lays a list of materials					The interpretation of obscenity can vary, and

which would be deemed as obscene if it strikes at the lascivious, voyeuristic, salacious or lustful interests of a person and consequently depraves or corrupts a person in sexual context. Section 67 of the IT Act deals with publishing obscene information in electronic form.					what may be considered obscene in one context or community may not be considered so in another. This subjective nature of the definition can sometimes lead to challenges in effectively regulating and addressing online obscenity
Illegal Content					
IT Act, 2000 and Other Indian Legislations	**DSA (EU)**	**OSB (UK)**	**Australia**	**Singapore**	**Key Elements**
IT Rules, 2021 (2023 amendment) to remove content after	illegal content' means any	"Illegal content" means content that amounts to		Meaning of "egregious content" 45D.—(1) In this	• Illegal Content should be classified and a nuanced

receiving an order from a competent court or regulatory authority on content that is: Damaging to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order Related to rape, sexually explicit material or child sexual abuse material. any information which is identical to information that has previously been removed.	information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law;	a relevant offence. (3) Content consisting of certain words, images, speech or sounds amounts to a relevant offence if— (a) the use of the words, images, speech or sounds amounts to a relevant offence, (b) (in the case of a user-to-user service) the use of the words, images, speech or sounds, when taken together with other regulated user generated		Part, "egregious content" means — (a) content that advocates or instructs on suicide or self-harm; (b) content that advocates or instructs on violence or cruelty to, physical abuse of, or acts of torture or other infliction of serious physical harm on, human beings; (c) content that advocates or instructs on sexual violence or coercion in association with sexual conduct, whether or not involving the commission of a heinous sex crime;	approach should be taken keeping in mind the socio-cultural context and the prevalence of harms on each intermediary

		content present on the service, amounts to a relevant offence, (c) the possession, viewing or accessing of the content constitutes a relevant offence, or (d) the publication or dissemination of the content constitutes a relevant offence. (4) “Relevant offence” means— (a) an offence specified in Schedule 5 (terrorism offences), 5 10 15 20 25 30 35		(d) content depicting for a sexual purpose, or that exploits, the nudity of a child or part of a child in a 15 way that reasonable persons would regard as being offensive, whether or not sexual activity is involved; (e) content that advocates engaging in conduct in a way that — (i) obstructs or is likely to obstruct any public 20 health measure carried out in Singapore; or (ii) results or is likely to result in a public health risk in Singapore; (f)	

		40 45 Online Safety Bill Part 3 — Providers of regulated user-to-user services and regulated search services: duties of care Chapter 7 — Interpretation of Part 3 49 (b) an offence specified in Schedule 6 (offences related to child sexual exploitation and abuse), (c) an offence specified in Schedule 7 (other priority offences), or (d) an offence, not within paragraph (a), (b) or (c), of which the victim		content dealing with matters of race or religion in a way that is likely to cause feelings of enmity, hatred, 25 ill will or hostility against, or contempt for or ridicule of, different racial or religious groups in Singapore; (g) content that advocates or instructs on terrorism; or (h) any other content that is prescribed by Part 10A regulations as egregious content.	

		or intended victim is an individual (or individuals)			

Clearly defined actions and harms	**Ambiguously defined actions and harms**
• **CSAM and Other Harms to Children:** **Sections 13, 14 and 15 of Protection of Children from Sexual Offenses (POCSO) Act** criminalizes the use of a child for sexual gratification. According to Section 13, the use of a child for sexual gratification includes – • representation of the sexual organs of the child; • usage of a child engaged in real or simulated sexual acts (with or without penetration); • indecent or obscene representation of a child. **Section 67B of the IT Act** specifically pertains to children less than 18 years of age and criminalizes any act depicting children in sexually explicit act in electronic form or inducing children to an online relationship for a sexually explicit act. It also criminalizes facilitating the online abuse of children.	• **Obscene Content** **Section 292, IPC, Clause 1** lays a list of materials which would be deemed as obscene if it strikes at the lascivious, voyeuristic, salacious or lustful interests of a person and consequently **depraves or corrupts a person in sexual context**. **Section 67 of the IT Act** deals with publishing obscene information in electronic form.

The Handbook for Adolescents/Students on Cyber Safety developed by the Indian Ministry of Home Affairs defines online grooming as "a practice where someone builds an emotional bond with a child through social media or chat window with an objective of gaining their trust for sexual abuse or exploitation" (Ministry of Home Affairs, 2018, p. 9).[3]	
• **Content relating to harassment and intimidation** **Sections 503, IPC** relates to criminal intimidation **Section 504, IPC** criminalizes intentional insult with intent to provoke breach of the peace **Section 509, IPC** criminalizes word, gesture or act intended to insult the modesty of a woman IT Act (I**ntermediary Guidelines and Digital Media Ethics Code)** requires Intermediaries to regulate gender, racially or ethnically objectionable content.	• **Content that is harmful to children** **Section 293 of the IPC** deals with a similar subject-matter as Section 292 (obscenity) and punishes any act that constitute sale or distribution of obscene objects to a person under 20 years of age. **67B, IT Act**
• **Financial Harms** Online financial harms refer to fraudulent activities and scams that target individuals or organisations through digital platforms and technologies, with the intention of unlawfully obtaining money or sensitive financial information. These types of harms can have	• **Content Violating Privacy of a Person:** Section 66E criminalizes any person who knowingly and intentionally captures the image of a private area of a person without his or her consent.

significant financial and personal consequences for the victims. **The following sections of the IT Act address the different kinds of financial harms affecting users:** **Section 43: Penalty and Compensation for damage to computer, computer system, etc** **Section 65: Tampering with Computer Source Documents** **Section 66C: Punishment for identity theft** **Section 66D: Punishment for cheating by impersonation by using computer resource**	**Justice K.S. Puttaswamy v Union of India:** A nine judge Bench held that a fundamental right to privacy is guaranteed under the Constitution of India, 1950.
• **Section 66F: Cyber Terrorism** The use of cyber space to cause harm to the general public and disrupt the integrity and sovereignty of the target country **Unlawful Activities (Prevention) Act, 1967**	

Contact Us

If you need to know more about us or our research, get in touch with us via our website, email, or call.

DEEPSTRAT

STRATEGY . POLICY . ACTION

www.deepstrat.in

contact@deepstrat.in