

DIGITAL INDIA ACT Dialogue Series: Inaugural Session

An Overarching Framework for Digital Intermediaries
(with emphasis on aspects such as the need for
Safe Harbor provisions)





Table of Contents

1	Introduction and Context	04
2	Addressing the Legal and Regulatory Landscape for Digital Intermediaries	06
2.1	Current legal framework and regulations governing digital intermediaries	06
2.2	Need for an overarching framework for digital intermediaries	08
3	Key Discussion Items & Pointers	09
3.1	Open Internet: Fostering Choice, Competition, and Fair Market Access	09
3.2	Online Safety and Trust: Tackling Harmful Content and Misinformation	11
3.3	Accountability in the Digital Age: Weighing the Pros and Cons of Safe Harbour	12
3.4	Analysing the scope and effectiveness of self-regulatory mechanisms within the digital ecosystem	14
3.5	Identifying ways to strike a balance between regulatory compliance and fostering a conducive environment for digital innovation: The Sandbox Mechanism	16
4	Final Reflections and Summary of Recommendations: Creating the Right Policy Framework that Enables Digital Bharat	17

01

Introduction

The Information Technology Act of 2000 has long served as India's foundational legislation for regulating the Internet. However, as the digital landscape has evolved over the past two decades, India recognizes the need to adapt its laws to meet the challenges posed by the changing technological landscape. With the rise of artificial intelligence (AI) models and the increasing penetration of the Internet, India is taking proactive steps to ensure a comprehensive framework that addresses the complexities of the rapidly evolving digital ecosystem.

India is currently home to over 750 million active Internet users. ¹ The country has experienced a remarkable surge in digital payments, witnessing a 13% growth in 2022 alone, with 338 million individuals utilizing digital payment methods. ² Furthermore, online shopping has seen a substantial 51% increase, highlighting the significant role of e-commerce in India's economy.

Recognizing the global trend of reevaluating Internet laws, India is actively participating in this process. Countries around the world, including the European Union, the United Kingdom, and Australia, have introduced separate legislations to regulate and address the challenges associated with the Internet.

In response to these developments, the Institute for Competitiveness and Primus Partners are jointly organizing a series of roundtable discussions to explore the intricacies of the proposed Digital India Bill, which is intended to replace the IT Act of 2000. The inaugural session took place on 28th June 2023, providing a platform for insightful deliberations. The roundtable saw participation from a diverse range of stakeholders, including Members of Parliament, state government officials, legal experts, academic think-tanks, and industry representatives.



¹ <https://www.thehindu.com/news/national/over-50-indians-are-active-internet-users-now-base-to-reach-900-million-by-2025-report/article66809522.ece>

² <https://www.afaqs.com/news/digital/india-leads-in-digital-ad-spending-with-22-kantar>

The Digital India Act is poised to address the emerging challenges in the digital, technological, and cybersecurity domains. With its potential to exert a profound impact on all stakeholders involved, the DIA will play a pivotal role in shaping India's digital future. The Hon'ble Minister of State (MoS), Ministry of Electronics and IT, Shri Rajeev Chandrasekhar had presented the possible inclusions of the Act – the driving principles such as Open Internet, Online Safety and Trust including User Harm, Intermediaries and their classification, Measures for Accountability, Regulatory Framework, and Provisions for Emerging Technologies.

This white paper focuses on a key aspect that the Act intends to address, which is the overall structure for digital intermediaries, considering trust, transparency, and responsibility as the main factors. The consultations by the government have already indicated that 'digital intermediaries' will be based on the nature of their activities, the intensity of risks that they represent, and the number of consumers that they represent. The Digital India Act can also classify newer technology either based on risk technology, consumer intensity, or any other kind of criteria emerging in the future.

In this context, digital intermediaries are already playing a crucial role in the digital economy of today. In an increasingly digital world, their role in facilitating e-commerce, online communication, and content sharing is pivotal in advancing India's digital transformation and empowering its citizens. They are driving economic growth, fostering entrepreneurship, and expanding access to information and services. The Digital India Act aims to regulate and provide a legal framework for these intermediaries, ensuring accountability, data privacy, and user protection. By defining their responsibilities and liabilities, the Act should seek to strike a balance between enabling innovation and safeguarding the interests of all stakeholders.

The purpose of this whitepaper is to give objective recommendations on key themes and principles that can help shape the proposed Digital India Act into a more effective technology regulation framework. The topic being analysed here pertains to the broader realm of digital intermediaries and aspects such as fostering competition, ensuring online safety, accountability of digital intermediaries (safe harbour) among others.



02

Addressing the Legal and Regulatory Landscape for Digital Intermediaries

2.1

Current legal framework and regulations governing digital intermediaries

The Ministry of Electronics and Information Technology (MeitY) notified the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in February 2021, superseding the previous Information Technology (Intermediaries Guidelines) Rules, 2011.

As per Section 2(1)(w) of the IT Act, an "intermediary", with respect to any electronic record, is defined as any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record. As per this definition, an intermediary includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places, and cyber cafes.

In contrast to the 2011 Rules, which controlled all "intermediaries" without regard to their user base or the content hosted on their platform, the 2021 Rules broadly categorise the entities to be regulated as follows:

- i. Social media intermediary: an intermediary having less than 50 lakh registered Indian users.
- iii. Significant social media intermediary: an intermediary having more than 50 lakh registered Indian users.
- v. Publisher of news and current affairs content: which includes news aggregators.
- vii. Publisher of online curated content: which covers all online streaming platforms including Over-the-Top (OTT) platforms.

As per Rule 2(1)(w) of the Intermediary Rules, a "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.

The 2022 Notified Amendments indicated that intermediaries must ensure compliance with rules and regulations, privacy policy, and user agreement, and make reasonable efforts to cause users to not create, upload, or share prohibited content. It also encompassed the provision of central government establishing one or more Grievance Appellate Committee to hear appeals against the decisions of grievance officers.

In April 2023, MeitY further notified amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to online gaming. The amendment defines an online game as a game that is offered on the Internet and is accessible by a user through a computer resource or an intermediary. An online gaming intermediary (OGI) is defined as any intermediary that enables the users of its computer resource to access one or more online games. Thus, another type of intermediary has been recognized by the government.

The 2023 Digital India Law will classify intermediaries basis/vis-à-vis the service it provides, like e-commerce, search engines, gaming, AI, OTT, TSPs, Ad-Tech, and SSIMs.



2.2

Need for an overarching frame-work for digital intermediaries

The rapid growth of digital platforms and services has resulted in a significant increase in online activities, leading to new challenges and risks, like privacy, data security, misinformation, etc. It has become essential to address these challenges to ensure the protection of users' rights and interests, while also providing regulatory certainty to digital intermediaries. The issues that demand this regulatory certainty include clear regulations on user privacy, the extent of what encompasses harm, control over algorithms, user consent, level of transparency, control over content, types and rationale for authentication, and user accessibility and portability. An effective regulatory framework can provide clarity to the businesses, fostering innovation and investment in the digital sector. By establishing transparent rules and regulations, it will make it easier for intermediaries to understand their roles and responsibilities, leading to responsible and accountable practices.

The introduction of the Digital India Act also presents an opportunity for the government to acknowledge that internet intermediaries cannot be treated as a homogeneous group. Instead, they should be classified based on their specific roles and responsibilities. For instance, internet access providers and hosting providers have a more passive role, whereas social media platforms and messaging services actively engage with users. By recognizing these distinctions, the government can introduce differential obligations tailored to the nature of their operations.

The very requirement of classification of intermediaries, which is absent under the current IT Laws, was also substantiated by the Hon'ble MoS. The Ministry's position is that not all intermediaries have the same kinds of risks, and it is thus wrong to categorise them into the same bucket (under function-specific labels). As an example, when qualifying safe harbour with certain sets of obligations, the obligations that apply on any platform will have to differ based on the kinds of functions they impose.

An overarching regulation framework for digital intermediaries in India is necessary to address emerging challenges, protect users' rights, combat digital crimes, ensure the safety of vulnerable groups, promote innovation, and create a secure and trustworthy digital environment.



03

Key Discussion Items & Pointers

3.1

Open Internet:

Fostering Choice, Competition, and Fair Market Access

The concept of an open internet emphasizes the principles of choice, competition, and fair market access. It advocates for a digital environment where users have the freedom to access and share information but with reasonable restrictions. By promoting a level playing field, it enables fair competition among service providers, encouraging innovation and diverse offerings. An open internet also empowers users to make informed choices, ensuring they have access to a wide range of content and services. The focus should be towards striking the right balance between the liability of the intermediaries and introducing measures to counter societal risks and user harm. A technology regulatory framework that upholds these principles will be able to foster an inclusive and dynamic digital ecosystem that benefits individuals, businesses, and society as a whole.



Key recommendations



To encourage and sustain innovation & competition, a delicate balance needs to be maintained between choice from a user's perspective and regulation from a policy perspective. In the context of competition in the digital landscape, one first needs to identify the relevant type of intermediary in question. This in turn will require to look at intermediaries not as homogenous entities, but as distinct entities having different nuances and performing distinct functions.



The provisions of the Act will have to be in jurisdictional synonymity with the other upcoming rules focusing on open internet, like 'digital competition' tentatively highlighting "gatekeepers". As an example, provisions under Europe's Digital Services Act and Digital Markets Act complement each other and avoid any possible overlaps, while ensuring prospects of an open internet ecosystem. A balance has to be attained, thus, to avoid overregulation on an intermediary. That is, to foster new businesses and ensure fair market access, compliance burden needs to be minimal and make economic sense from a business perspective for smaller digital intermediaries. This is also in alignment with the Ease of Doing Business criterion that the government intends to incorporate within 'open internet'.



If the government intends to highlight provisions for "non-discriminatory" access to digital services or net neutrality under open internet, the same should be in consultation with key industry players and should incorporate their participation in the dialogue. Net neutrality while it can help to level the playing field for smaller companies and startups, allowing them to compete with larger, more established companies, it can also limit the ability of service providers to manage their networks and offer differentiated services to their customers. There should be a sound consideration that such a measure does not limit the ability of network service providers to invest in infrastructure and innovation.



Any provision for bringing in transparency on the algorithms used for recommending content to users should be in a way such that it does not hinder intellectual property of the service provider or intermediaries.




Aligning open internet regulations with international best practices helps position the Indian digital industry on a global scale. This interoperability can facilitate international collaborations and partnerships, boosting India's competitiveness in the global digital market.


3.2


Online Safety and Trust: Tackling Harmful Content and Misinformation


Addressing harmful content and misinformation is crucial to ensure online safety and foster trust in digital spaces. Regulations can play a vital role in combating these challenges by promoting responsible content moderation practices, empowering users with tools to identify and report harmful content and encouraging transparency from online platforms. By implementing effective measures, such as fact-checking initiatives and educational campaigns, a safer online environment can be created where users can trust the information they encounter and engage with online platforms with confidence.


Key recommendations


 To tackle harmful content and misinformation, imparting digital literacy and building capacity in terms of awareness about how to use the internet in an adequate manner is more important than imposing blanket restrictions.

 DIA should impose new mechanisms allowing users to flag illegal content online, and in an easy and effective way, and for platforms to cooperate with specialised 'trusted flaggers' to identify and remove illegal and harmful content.

 The proposed classification of intermediaries should incorporate sectoral differentiation of what entails harmful content. This will make the intermediaries understand the nuances of complying basis specific content concerns.

 A yearly risk assessment framework can be mandated to allow platforms and intermediaries to showcase the work conducted in curbing harmful content.

 Intermediaries should audit their online interfaces to ensure that they are sufficiently clear, plain, intelligible, user-friendly, and unambiguous when describing compliance with various standards of DIA.

 Provisioning the use of encryption and secure protocols to protect data transmission and storage from interception and tampering. Encryption is a process of transforming data into an unreadable form that can only be decrypted by authorized parties.

3.3

Accountability in the Digital Age: Weighing the Pros and Cons of Safe Harbour

The issue of accountability in the digital age has led to discussions around safe harbour provisions. In today's age of diverse digital intermediaries, the relevance of safe harbour provisions becomes paramount. With the proliferation of online platforms, social media networks, e-commerce websites, and other intermediaries, these provisions serve as a crucial legal framework. These provisions offer protection to internet intermediaries from legal liability for user-generated content. Safe harbour provisions encourage innovation, free expression, and information sharing by shielding intermediaries from potential legal repercussions. They provide a conducive environment for online platforms to thrive, facilitating economic growth and the exchange of ideas. However, critics argue that these provisions may inadvertently shield intermediaries from their responsibility to combat harmful content, misinformation, and intellectual property violations. Striking a balance between the advantages of innovation and the need for accountability remains a significant challenge in shaping the regulatory landscape of the digital era. The government might pivot from "blanket immunity" (blanket safe harbour) to "conditional immunity" (conditional safe harbour provisions) for intermediaries.

Key recommendations



Safe harbor provisions provide a level of legal certainty for intermediaries, encouraging them to invest in the

development of new technologies and platforms. The "conditional immunity" should be based on the parameters that does not stall these market growth prospects. The 'Good Samaritan' clause of both US and later EU, where online intermediary services need to adopt proactive monitoring actions in case they face a risk of dissemination of illegal and/or harmful content on the web, is on similar contours and needs as assessment for domestic implementation.



There should be due consideration of the fact that online platforms process enormous volumes of user-generated content every day. It's practically impossible for intermediaries to review and moderate every piece of content before it's posted. Safe harbor provisions acknowledge this limitation and provide a practical framework for managing user content while addressing illegal content removal through proper channels.



Intermediaries should not be liable for content hosted on their service so long as they either do not know the content is illegal or infringing, or they promptly remove or block access to that content once aware that it is illegal or infringing.

Key recommendations (contd.)



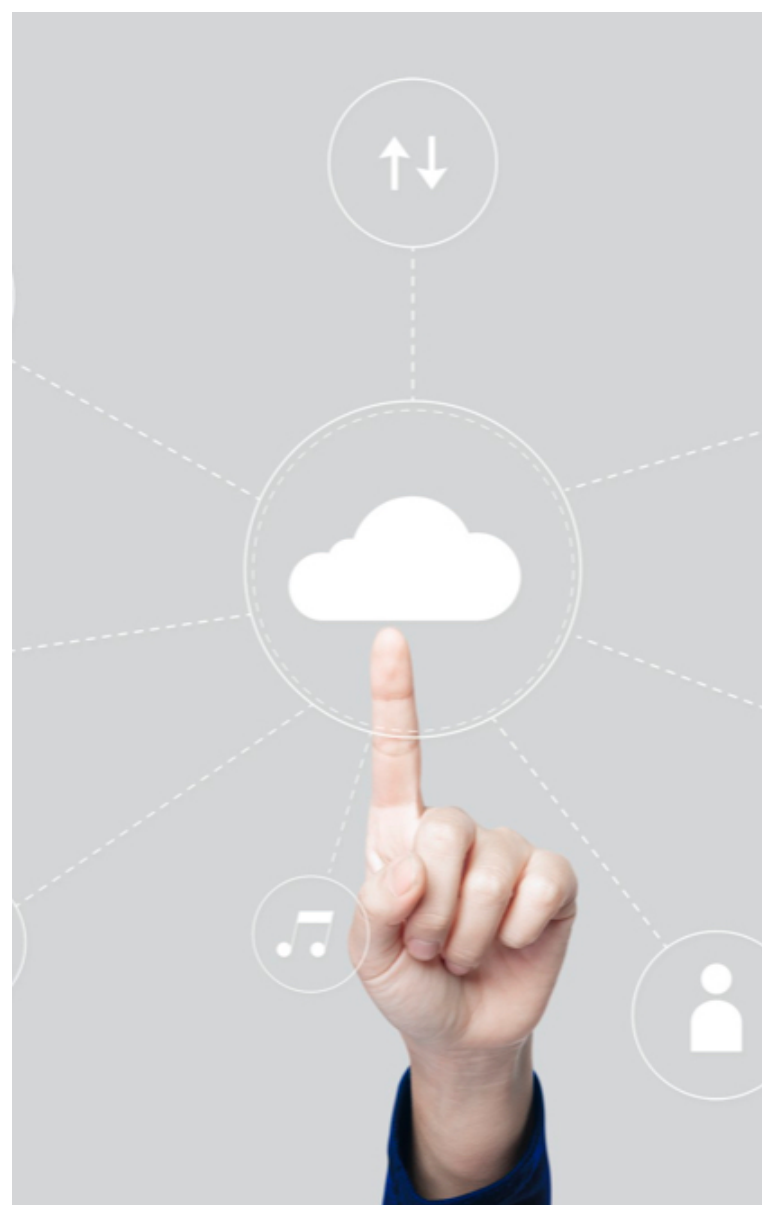
There should be provisions of 'Reasoned Order' and subsequently, a 'Right to Recourse' as systemic alternates to a conditional immunity clause. This ensures that the intermediary has received clear and legally grounded instructions from the relevant authority before taking any action against user content. This requirement prevents intermediaries from being compelled to remove content arbitrarily. Moreover, if an intermediary receives a reasoned order to remove or restrict content, it should have the right to challenge the order through appropriate legal channels vis-à-vis a right to recourse. Similarly, users whose content has been affected by such an order should have a mechanism to appeal against its enforcement.



Removing safe harbour altogether is a concern because that essentially turns digital media intermediaries into gatekeepers of free speech and thought. This also holds constitutional and historical eminence, as the court during 'Shreya Singhal v. Union of India' had ruled that intermediaries cannot be held liable for third-party content unless they have actual knowledge of its illegal nature and fail to take action to remove it, and also suggesting clearer standards.



Practicality of implementation is as important as the provision itself. In the absence of safe harbour, there is a threat of take-down requests being misdirected, especially in sectors that invest significant time, R&D and/or money in developing or acquiring content, such as online gaming intermediaries and OTT platforms.



3.4

Analysing the scope and effectiveness of self-regulatory mechanisms within the digital ecosystem

Self-regulatory mechanisms within the digital ecosystem have gained prominence as a means to address various challenges and promote responsible practices. They provide an opportunity for industry stakeholders to collaborate, share best practices, and establish standards tailored to the specific needs of the digital ecosystem. These mechanisms encompass industry-led initiatives, codes of conduct, and voluntary guidelines. Self-regulatory mechanisms can be more flexible and responsive to the evolving digital landscape compared to traditional legislation. They allow for

quicker adaptations to technological advancements and changing user behaviours. Moreover, industry-led initiatives tend to foster a sense of ownership and responsibility among stakeholders, promoting proactive measures to address concerns. While they offer flexibility and agility, their effectiveness depends on industry participation, adherence, and harmonization with legal frameworks when necessary. Achieving a balance between self-regulation and appropriate regulatory oversight is key to fostering a responsible and trustworthy digital environment.



Key recommendations



Self-regulatory mechanisms within the digital ecosystem have garnered significant attention and hold considerable importance. They offer the industry the liberty and adaptability required for fostering innovation. Therefore, it is recommended that dedicated Self-Regulatory Organizations (SROs) tailored to specific sectors be established.



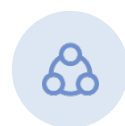
Defining distinct goals and foundational principles could prove valuable in structuring effective governance for a Self-Regulatory Organization (SRO), all while permitting the necessary room for it to fulfill its responsibilities flexibly. This process will involve precisely outlining the objectives of the SRO framework and defining key governance principles that will guide the SRO's activities within the established framework.



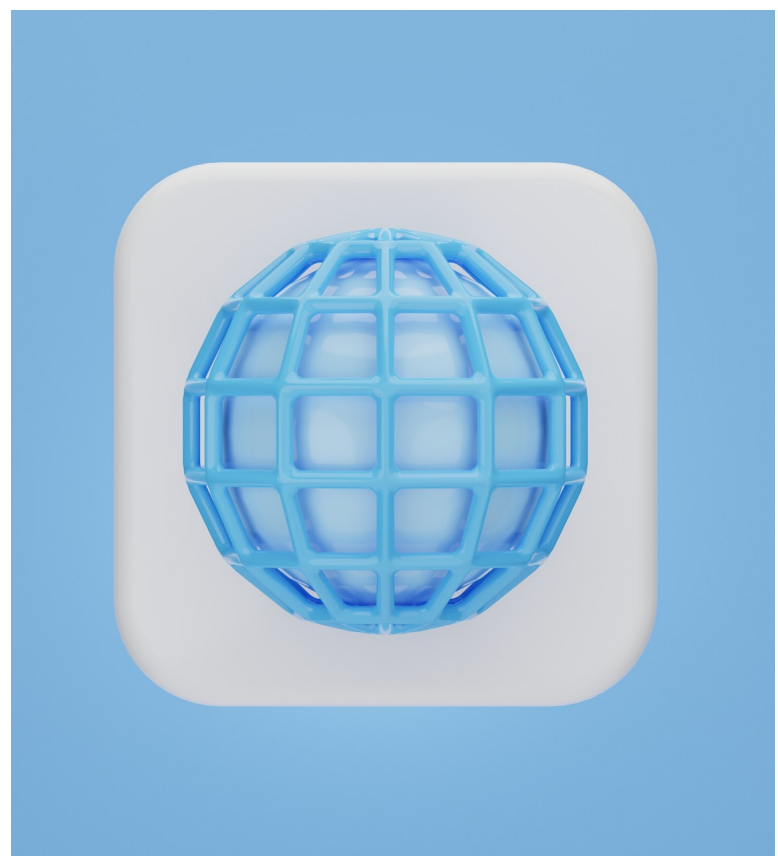
It is important to establish a clear and defined count of authorized SROs. The governance structure of SROs should consist of a balanced composition, incorporating both impartial individuals and industry experts, customized to suit the specific sector. In this regard, the introduction of independent directors into the governance framework could be considered.



It is encouraged to grant authority to industry associations for the formulation of codes of conduct and best practice guidelines particularly around user safety and accountability. This strategy will effectively harness the industry's specialized knowledge and facilitate quick adjustments to the swiftly evolving digital environment.



The SROs can establish channels for regular communication between self-regulatory bodies and government agencies. Collaboration will ensure alignment with national laws like DIA while leveraging the expertise of both parties.



3.5

Identifying ways to strike a balance between regulatory compliance and fostering a conducive environment for digital innovation: The Sandbox Mechanism

Addressing the concept of a regulatory sandbox offers a potential way to strike a balance between regulatory compliance and fostering a conducive environment for digital innovation. A regulatory sandbox provides a controlled testing environment where innovative products, services, or business models can be piloted under regulatory supervision. It allows businesses to experiment with emerging technologies while regulators can assess their impact and risks. By providing temporary relaxations or waivers of certain regulations, the sandbox enables innovative ideas to flourish without stifling them under burdensome compliance requirements. Sandbox also allows regulators to mitigate unforeseen risks for users and the wider economy. This becomes important from the context of Digital India Act where a sandbox treatment should be adopted before any widespread implementation.

provide legal certainty and protection for the participants and the consumers in case of disputes or failures.



Engaging with relevant stakeholders, such as other government departments (like the Department of Telecom), industry associations, consumer groups, academia, and civil society, to solicit feedback and input on the sandbox design, implementation, and evaluation. This can help to ensure that the sandbox is aligned with the broader policy objectives and market needs, and that it addresses the potential risks and challenges of the innovations. Stakeholder engagement can also foster collaboration and trust among different actors in the digital ecosystem.

Key recommendations



Establishing a clear and transparent legal framework that defines the objectives, scope, eligibility criteria, application process, testing parameters, consumer protection measures, and exit strategies for the sandbox is a requisite. This can help to ensure consistency, fairness, and accountability in the sandbox operation, and to communicate the expectations and responsibilities of the Law's provisions and the innovator. A legal framework can also



Defining the testing parameters for each innovation based on a case-by-case analysis of its specific features, risks, and impacts. The testing parameters may include aspects such as the duration, scope, scale, target market segment, performance indicators, reporting requirements, and consumer safeguards of the testing. There should also be a clear exit strategy for each innovation that specifies the conditions and procedures for graduation, extension, suspension, or termination of the testing.

04

Final Reflections & Summary of Recommendations: Creating the Right Policy Framework that Enables Digital Bharat

i.

Principle-Based Approach over Prescriptive Rules

The Digital India Act should adopt a principle-based approach, setting forth broad guiding principles that reflect the fundamental values of the digital ecosystem, rather than overly detailed and rigid rules. This allows for flexibility as technology evolves rapidly, ensuring that the law remains relevant and adaptable.

ii.

Dynamic Formulation to Accommodate Technological Evolution:

The Act should aim to strike a balance between keeping up with rapidly evolving technology while maintaining the essence of safe harbor provisions. It should be designed to adapt and adjust as new technologies emerge, ensuring that user safety and platform responsibility remain central.

iii.

Shared Responsibility and Governance Challenges:

The Act should promote shared responsibility between platform users and intermediaries for content posted on the platform. However, governance challenges can arise due to unclear regulatory jurisdictions, especially within a federal structure of government. Addressing these challenges through well-defined collaboration mechanisms is essential.

iv.

Enabling Growth of Ideas, Businesses & Technology:

The Act should aim to strike a balance between keeping up with rapidly evolving technology while maintaining the essence of safe harbor provisions. It should be designed to adapt and adjust as new technologies emerge, ensuring that user safety and platform responsibility remain central.

v.

Comprehensive Scope of Harm:

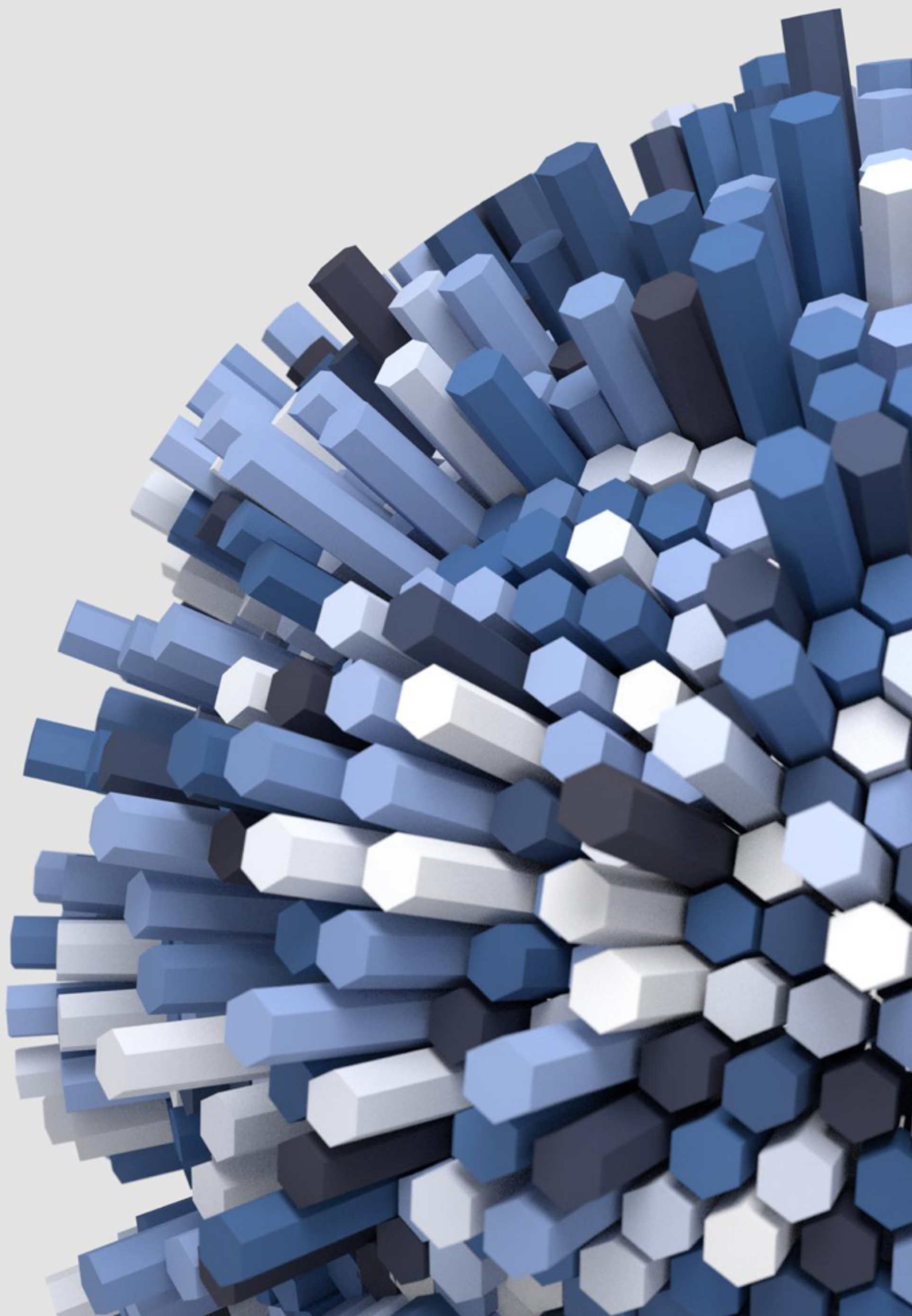
The scope of harm should expand beyond harm to individual users and extend to entities, enterprises, and even society at large. As emerging technologies evolve, they can amplify the impact of harmful activities, necessitating a broader definition of harm to ensure comprehensive protection.

vi.

Timely and Effective Implementation:

The success of the Digital India Act lies in its timely and effective implementation. Ensuring that the law is enacted swiftly and executed rigorously is crucial to realizing the vision of a robust digital India. This may involve setting up dedicated enforcement mechanisms and providing adequate resources for their operation.

Incorporating these principles and considerations into the Digital India Act can lead to a framework that not only addresses current challenges but also adapts to the rapid changes in technology and the digital landscape. It emphasizes shared responsibility, user safety, and innovation while navigating the complexities of governance and jurisdiction.



ABOUT Institute for Competitiveness (IFC)



The Institute for Competitiveness is a global initiative based in India, committed to expanding and effectively sharing research and knowledge on competition and strategy. By offering various programs and initiatives, the Institute aims to improve competitiveness and foster an innovative and growth-oriented environment.

ABOUT Primus Partners



Primus Partners has been set up to partner with clients in 'navigating' India, by experts with decades of experience in doing so for large global firms. Set up on the principle of 'Idea Realization', it brings to bear 'experience in action'. 'Idea Realization'— a unique approach to examine futuristic ideas required for the growth of an organization or a sector or geography, from the perspective of assured on ground implementability. Our core strength comes from our founding partners, who are goal-oriented, with extensive hands-on experience and subject-matter expertise, which is well recognized in the industry. Our core founders form a diverse cohort of leaders from both genders with experience across industries (Public Sector, Healthcare, Transport, Education, etc.), and with varied specialization (engineers, lawyers, tax professionals, management, etc.).

Disclaimer

The report is prepared using information of a general nature and is not intended to address the circumstances of any particular individual or entity. The report has been prepared from various public sources and the information received from these sources is believed to be reliable. The information available in the report is selective and subject to updation, revision and amendment. While the information provided herein is believed to be accurate and reliable, Primus Partners Private Limited does not make any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and data available in the public domain. While due care has been taken while preparing the report, Primus Partners Private Limited does not accept any liability whatsoever, for any direct or consequential loss arising from this document or its contents.

We do not claim ownership over the images used in this document.



The Institute for Competitiveness

Suite 228, V John Building,
Udyog Vihar, Gurgaon 122 002
Haryana, India

Phone: +91-124-437-6676
Email: info@competitiveness.in

www.competitiveness.in

Primus Partners Private Limited

15, Tolstoy Road, Atul Grove Road,
Janpath, Connaught Place,
New Delhi 110 001, India

Phone: +91-11-XXXX-XXXX
Email: info@primuspartners.in

www.primuspartners.in