Policy Dialogue: Discussions on the Upcoming Digital India Act

Event Report

Author: Mahwash Fatima

Published: Nov 2023

thequantumhub.com

TABLE OF CONTENTS

1. **Executive Summary**
2. **Discussions on the upcoming Digital India Act - Broad Overview**
3. **Key Takeaways**
4. **List of Speakers**
5. **Panel 1: Defining the contours of the Digital India Act**

   Enumeration of User Harms
   Innovation and potential risks
   Regulatory overlaps and co-regulation
   Adjudication

6. **Panel 2: Expectations and concerns with respect to safe harbour under the Digital India Act**

   Need for safeguarding safe harbour
   Expectations of safe harbour under DIA

EXECUTIVE SUMMARY

The Quantum Hub (TQH) organised a policy dialogue on the proposed Digital India Act (DIA) - an upcoming legislation that aims to replace the Information Technology Act, 2000 (IT Act) to provide a comprehensive principle-based legal framework for the digital sector in India. Held in partnership with the US-India Strategic Partnership Forum (USISPF) on October 12, 2023 in New Delhi, the event featured two panel discussions on the contours of DIA and the principle of safe harbour thereunder.

Attended by a diverse group of stakeholders, the event provided a platform for nuanced discussions that highlighted the opportunities and challenges of the DIA and offered some key insights and recommendations for the government and the stakeholders to consider while drafting and implementing the legislation.

The first panel explored the scope of the proposed law in the backdrop of pressing concerns that are necessitating the introduction of DIA. The discussions focused on ensuring user safety in the wake of harms arising out of existing and emerging technologies, regulatory approaches and the establishment of effective institutional bodies. The panel also examined the delicate balance between innovation and regulation. **A key point highlighted by the panel was the necessity of an adaptive risk-based regulatory approach** over exhaustive enumeration of user harms keeping in view the importance of a principles-based regulatory framework to adapt to the dynamic nature of emerging technologies.

The second panel scrutinised the intricate aspects of safe harbour principle. Discussions revolved around the potential impact of rethinking safe harbour on user safety, free speech and the fundamental functioning of digital platforms. **While a complete immunity of platforms was challenged, the panel underscored the importance of safeguarding safe harbour principles** and raised concerns about the potential negative consequences of eliminating safe harbour, impacting innovation and flexibility in response to changing market dynamics.

The points that emerged from this policy dialogue highlight the need for a principled, adaptive framework to navigate the dynamic digital landscape in India, fostering innovation while safeguarding user safety.

DISCUSSIONS ON THE UPCOMING DIGITAL INDIA ACT- BROAD OVERVIEW

Acknowledging the evolving digital ecosystem of India, the Government of India has proposed the enactment of DIA to provide a principle based legal framework for regulating the digital ecosystem and ensuring user safety. With the background that the IT Act is now an outdated legislation that fails to address the current and future challenges of the digital sector in India, the idea of DIA was put forth by the government in 2022. Over time, the government has explained that the IT Act was enacted at a time when the internet was still in its infancy in India, with less number of users and limited types of online services and activities. However, in the past two decades, the internet landscape has undergone a radical transformation, with the number of users coming close to 850 million, alongside the evolution of numerous new technologies and platforms. These new technologies have not only brought new opportunities but also challenges for the users and regulators alike.

It has been argued that the IT Act may be ineffective in terms of regulating this landscape and addressing the emerging issues. Though there have been several attempts to amend the IT Act and introduce new rules and guidelines to fill the gaps, these tend to be insufficient and fragmented when it concerns the comprehensive and holistic regulation of the digital sector. Therefore, the government has proposed a new legislation that can provide an overarching framework for the development and governance of the digital ecosystem in India.

In that context, the Digital India Act is a commendable and ambitious initiative that aims to create a new legal framework for the digital sector. However, there are still many unresolved issues and ambiguities that exist even after two rounds of public consultation. With an aim to contribute to the ongoing discourse on how the legislation should be shaped, what it should encompass, and how it should balance the interests of different stakeholders, including users, without stifling the growth and innovation of the sector, The Quantum Hub (TQH), in partnership with the US-India Strategic Partnership Forum (USISPF), hosted a policy dialogue on October 12, 2023.

The event opened with an insightful **keynote address by Member of Parliament, Mr. Manish Tewari** who set the tone and context for the nuanced discussions on the upcoming law. The first half of the event saw a panel discussion to deliberate the contours of the Digital India Act. This was followed by a panel discussion on expectations around safe harbour provisions under the Act. The session was attended by a diverse group of stakeholders including industry bodies, civil society, academics and journalists.

The key takeaways from these deliberations offer valuable insights and recommendations and could benefit policymakers and stakeholders alike, providing a better understanding of different nuanced considerations and helping set expectations from the upcoming legislation.

KEY TAKEAWAYS

- DIA should create a balanced liability regime acknowledging the role of online platforms, offering safeguards, and incentivizing compliance and cooperation with the law and regulators.
- The proposed DIA should ensure a comprehensive framework to tackle user harm without exhaustively defining each instance to ensure that law remains technology agnostic and adaptive to future developments.
- In formulating DIA, a risk-based approach should be adopted which would require each harm to have a proportionate regulatory response to the risk that is posed.
- Striking a balance to regulate emerging technologies is crucial for crafting a resilient and adaptable regulatory framework which remains technology agnostic and future-ready. This can only be done if a principles-based approach is followed instead of an overtly prescriptive legislation.
- Since regulatory overlap is inevitable given the expanse of the intended Act, it is crucial to clearly set out regulatory limits of the different regulators, rather than trying to avoid overlaps. Instituting a co-regulatory framework including self-regulatory bodies by the industry may be opportune to drive accountability as well as autonomy.

- There is a need for a fast and smooth adjudicatory mechanism in the digital sector given the relevance of time sensitivity, particularly applicable to this sector.
- Eliminating safe harbour immunity would not only disrupt the fundamental functioning of the internet, hindering platform operation and evolution, but also risk suppressing legitimate content, impacting innovation and the diverse expression of views and opinions online.
- The existing viewpoint that looks to weaken safe harbour misses the point that this principle is content-specific and not platform-specific. Thus, the shift from presumed safe harbour to 'earned' safe harbour will move safe harbour away from how the principle was originally conceptualized, ignoring why it came into being.

LIST OF SPEAKERS

PANEL 1:

Rakesh Maheshwari, Former Senior Director and GC (Cyber Laws and Data Governance), MeitY

Mr. Maheshwari is a former government officer having worked for more than 35 years in the Ministry of Electronics and Information Technology (MeitY). He retired on VRS as Sr. Director and Group Co-ordinator, Cyber Law and Data Governance. His work spans across regulatory, policy and administrative matters including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (IT Rules 2021) and its Amendments

Debashish Bhattacharya, Senior Deputy Director General, Broadband India Forum

Mr. Debashish brings extensive experience to the Telecom and IT & Broadcasting sector covering regulatory & policy matters, technology forecasting and corporate strategy. With over three decades of corporate experience, Mr. Bhattacharya is now a key member of the BIF directorate. As part of the team, he leads the formulation of inputs to the government as well as TRAI on various policy & regulatory matters.

Shahana Chatterji, Shardul Amarchand and Mangaldas

Shahana is a Partner with the Public Policy and Regulatory Affairs team at the law firm Shardul Amarchand and Mangaldas. She currently works on a range of regulatory matters with a specialization in data and emerging technology, and technology aspects of the highly regulated sectors in India.

Pallavi Smriti, Meta

Pallavi comes from a law background and is currently working as Public Policy Manager, India at Meta. She navigates the intersection of technology and governance, shaping strategies to align the company's innovations with global regulations and policies.

The panel was moderated by Aparajita Bharti

Aparajita is a Founding Partner of The Quantum Hub (TQH). With an expertise on governance and policy affairs, her work cuts across the domains of tech policy, gender and the design of India's regulatory institutions

PANEL 2:

Shashank Mohan, Centre for Communication Governance (CCG), National Law School, Delhi

Shashank is a Programme Manager with the Technology and Society team at CCG. His work is primarily focused on data protection, data governance, surveillance, intermediary liability, and e-governance.

Vakasha Sachdev, Logically AI

Vakasha, a lawyer by training, is currently working as a Regulatory Policy Manager at Logically AI, a tech company that is working to fight misinformation at scale.

Nikhil Pahwa, Medianama

Nikhil is the founder of Medianama, an online platform covering tech-policy and business developments shaping India's digital ecosystem. He works at the intersection of the internet and civil liberties.

The panel was moderated by Rohit Kumar

Rohit is a Founding Partner of The Quantum Hub (TQH). Rohit's work cuts across sectors, including regulation of new business models, emerging technologies, digital public infrastructure and payments.

DISCUSSION POINTS

PANEL 1: DEFINING THE CONTOURS OF THE DIGITAL INDIA ACT

In exploring the digital landscape of India and the need for regulating the same via the proposed DIA, the Ministry of Information and Technology (MeitY) has underscored a spectrum of concerns that have become increasingly apparent in the evolving digital sphere. Some of the reasons that are said to necessitate the enactment of the DIA include:

- Lack of comprehensive provisions on user rights, trust and safety;
- Limited recognition of harms and new forms of cybercrimes along with an absence of institutional mechanism for creating awareness and prevention;
- Lack of distinct regulatory approaches for harmful and illegal content and the defined scope of intermediary or platform's liability;
- Absence of adequate regulations to address the regulatory requirements of emerging technologies, such as artificial intelligence (AI), augmented reality (AR), virtual reality (VR), blockchain, etc., and the assessments of high-risk automated decision-making systems;
- Lack of clear standards for new-age technologies in addition to models of modern digital businesses and their impact on competition;
- Lack of adequate principles for data and privacy protection;
- Lack of a converged, coordinated, and harmonized institutional regulatory body, a dedicated and efficacious investigatory and enforceability mechanism, and a swift adjudicatory mechanism to ensure effective governance and adjudication.

In this context, the first panel discussion on the DIA explored the potential contours of the proposed legislation and the key issues and challenges involved. It examined the advantages and disadvantages of incorporating specific harms into the legislation and the criteria and principles for defining and addressing such harms. It also discussed the need for ring-fencing the DIA with respect to other laws that regulate the digital economy and the possible overlaps and conflicts. The panel also explored the intricate balance between innovation and potential risks, a tension at the heart of regulating emerging technologies and the ways to ensure that such technologies are ethical, inclusive, and human-centric. The role of the Indian Computer Emergency Response Team (CERT-In) in cybersecurity and the need for imposing limitations on information requests based on their purpose, such as national security, public order, or individual rights, were also touched upon.

Enumeration of User Harms

Protecting India's *'digital nagriks'* and keeping the internet safe and trusted for its users has been identified by MeitY as one of the guiding principles of DIA. Right from conceptualisation to the ongoing formulation, DIA is meant to be driven by a commitment to foster openness, safety, trust, and accountability on the internet. At the core of this lies the aspect of addressing user harms and as has often been pointed out by Minister of State (Mos), MeitY Mr. Rajeev Chadrasekhar, the Act will formulate ways to regulate emerging technologies through the 'prism of user harm'.

In the backdrop of this, the panel discussed how the crucial aspects of this discourse presents two predominant approaches. One perspective advocates for a detailed enumeration and definition of each user harm accompanied by a corresponding adjudication framework. Conversely, an alternative viewpoint emphasizes the development of a comprehensive framework to tackle user harm without exhaustively defining each instance to ensure the law remains technology agnostic and adaptive to future developments. The emphasis was placed on empowering grievance redressal bodies to make final decisions on determining 'harm'.

Upon detailed discussions on the need to identify user harms and incorporate them in DIA, the panel agreed that a risk-based approach to regulation should be adopted. This would require each harm to have a proportionate regulatory response to the risk that is posed. However, some cautioned that given the dynamic nature of platforms, such an approach will be difficult to enforce. It was pointed out that enumerating and defining each harm may not only be unnecessary but also not feasible as many user harms are already recognised and penalised under existing criminal laws and consumer protection laws. Moreover, enumerating user harms may take away the intention of keeping the DIA principle based and adaptive to emerging technologies and new harms that may ensue.

Innovation and potential risks

In its pursuit of fostering a secure and progressive digital landscape, DIA is slated to place significant emphasis on regulating and addressing challenges related to emerging technologies. Minister, Rajeev Chandrasekhar, has time and again emphasized DIA's focus on harmonizing laws, regulating emerging technologies and integrating industry input on such regulation to ensure user safety.

Expressing concerns about the DIA, one participant highlighted the government's dual expectations for platforms to regulate speech responsibly while avoiding the concentration of power with major tech platforms. The participant expressed worries about potential inflexibility in the DIA, drawing parallels with the iterative nature of the IT Rules, anticipating the possibility of frequent rule changes every few months.

The panel discussed that the inherent challenges in regulating disruptive technologies highlights the need for a balanced approach. Indian policymakers, while planning the ambitious DIA, must therefore navigate the complexities of regulating technologies that are ever-evolving. While agreeing that striking this balance is crucial to crafting a resilient and adaptable regulatory framework, most discussants agreed that it is essential to have a law that is technology agnostic and future-ready. This can only be done if a principles-based approach is followed instead of an overly prescriptive law. The consensus amongst the discussants was that this would ensure that the new law can keep pace with fast changing technologies and will also give more regulatory certainty to the industry which is a crucial industry expectation from this legislation.

Regulatory overlaps and co-regulation

Given the expansive scope of DIA, the discussions focused on the potential regulatory overlaps that may arise with existing sectoral laws and regulators. The broad mandate of the proposed law suggests a potential overlap of regulatory jurisdiction, raising questions about the coexistence and delineation of responsibilities between DIA and other sector-specific regulations.

It was in this background that the panel discussed how the challenge is looming and has not received much clarity from the government. In the past the MoS has explained that while MeitY or the internet regulator may oversee the conduct and address user harms generally, it is the sectoral regulators in health, finance etc. who will be expected to regulate the services these platforms offer.

It is this dynamic that took the center stage of discussion in this panel where the discussants pointed out that since it is inevitable that there will be overlap of regulatory jurisdiction, it is crucial to clearly set out regulatory limits of the authorities rather than trying to avoid overlaps. This way there can be reduced uncertainty and litigation. In this respect, specifically the case of competition law was discussed. The discussants highlighted how any attempt to address competition in technology markets under DIA would necessarily overlap with the competition law as it is also a horizontal legislation. In other words, both DIA and the Competition Act, 2002 will span all sectors and applications and hence increase the potential of conflicting overlaps. The panel thus agreed that the need for a clear demarcation with sectoral regulations would be imperative.

At this juncture, the panel also acknowledged the need to explore **co-regulatory models** in more detail. One participant emphasized a need to align with the goals set by the IT rules, delineating three key objectives: enhancing platform accountability, facilitating user grievance redressal, and ensuring transparency. Given the expanse, instituting a co-regulatory framework including self-regulatory bodies by the industry may be opportune to drive accountability as well as autonomy. The discussants advocated for the establishment of such a co-regulatory framework recognizing that addressing online harms requires a collaborative effort involving multiple stakeholders. There was consensus amongst the panellists that such an approach should be explored under DIA where the industry with direction from the government can formulate appropriate norms and drive enforcement.

Adjudication

During the public consultation on DIA, it has been pointed out by the government that one of the goals of DIA is to address the urgent need for a specialized and dedicated adjudicatory mechanism for online civil and criminal offences. It has been acknowledged that the adjudicatory mechanism under the Act should be easily accessible to deliver timely remedies to citizens, resolve cyber disputes, and develop a unified cyber jurisprudence, thereby enforcing the rule of law online. This is in light of the fact that the current IT Act lacks a swift adjudicatory mechanism which is necessary for accountable and responsive digital operators.

Picking up on this point, the panellists agreed that there is a need for a fast and smooth adjudicatory mechanism in the digital sector given the relevance of time sensitivity especially applicable to this sector. It was highlighted that although efforts had been made to expedite the adjudication process under the IT Intermediary Rules and that both state and central adjudication mechanisms exist under the current regime, there is still room for significant improvement in institutionalizing these mechanisms. It was thus concluded that the DIA should indeed implement a swift adjudication procedure to ensure the Act effectively meets its intended goals.

PANEL 2: EXPECTATIONS AND CONCERNS WITH RESPECT TO SAFE HARBOUR UNDER THE DIGITAL INDIA ACT

In the ongoing drafting of the DIA, a focal point of discussion revolves around the intricacies surrounding intermediary liability, particularly the nature and extent of these obligations. Notably, in previous consultations, MoS Rajeev Chandrasekhar, expressed his reservations concerning the principle of safe harbour. One of the regulatory interventions proposed in the upcoming Act is re-thinking the safe harbour provision under Section 79 of the IT Act which protects online platforms like social media intermediaries from being accountable for the content posted on them by their users.

The Minister's apprehensions in this regard underscore a critical facet of the ongoing discourse. As the event transitioned to its next panel discussion, the spotlight turned to this nuanced and pivotal conversation surrounding safe harbour—a foundational principle shaping the manner in which the platforms operate. The panel delved into the multifaceted considerations and implications, probing the need for a balanced approach that aligns with the evolving digital ecosystem, while ensuring user safety.

Need for safeguarding safe harbour

While acknowledging that concerns about the safety of users online are valid, the panellists considered the need for safeguarding the immunity currently provided under the IT Act. It was discussed that doing away with the immunity altogether may not advance user safety. Moreover, it will have a potential negative impact on free speech.

During the discussion, there were compelling arguments made in favor of safeguarding safe harbour principles. Most of the panellists agreed that removing the safe harbour immunity would disrupt the fundamental functioning of the internet, as it serves as a crucial pillar for the operation of the platforms and how they are essentially modelled. Additionally, the removal of safe harbour could have wide-reaching consequences, impacting platforms' flexibility to evolve and adapt to the changing market dynamics, hindering their ability to find the right product-market fit, ultimately impacting innovation.

A discussant emphasised that the elimination of safe harbour from DIA jeopardizes the proper functioning of the entire digital ecosystem. While some classes of intermediaries adopt the perspective that the issue of safe harbour concerns only social media platforms that allow users to post, as seen with a few OTT platforms dismissing its relevance, this perspective overlooks the broader impact that the removal of safe harbour would have on the internet as a whole. A discussant also remarked that eliminating safe harbour immunity would necessitate or result in another *“save the internet” campaign* in India.

Moreover, in the absence of safe harbour protection, online platforms may indulge in excessively removing legitimate content as well, leading to the suppression of views and opinions online. This is underscored by the Supreme Court's stance in the Shreya Singhal case, emphasizing that platforms like Facebook and Google should not find themselves obligated to adjudicate the legality of the takedown requests they receive.

Expectations of safe harbour under the DIA

In the course of the public consultation on DIA, the MoS, MeitY had raised a fundamental question surrounding this debate: Is there a necessity for a safe harbour provision at all? And if such a provision exists, what criteria should determine the entitlement of intermediaries or platforms to it?

Making safe harbour a qualified immunity will not only be difficult to implement but will also detrimentally impact the very digital citizens the government aims to protect. In this backdrop, the discussants highlighted that the safe harbour principle is content-specific and not platform-specific, and the existing viewpoint that looks to weaken safe harbour misses this conceptual clarity. Therefore, the shift from presumed safe harbour to 'earned' safe harbour will move safe harbour away from how the principle was originally conceptualized, ignoring why it came into being.

A discussant highlighted a fundamental question that lies at the core of the safe harbour debate: Is posting something online an act of communication or publishing? The perspective aligned with publishing argued against safe harbour, contending that content platforms should not be treated differently from other broadcasters. In this regard, the argument drew a parallel to newspapers, emphasizing that, like traditional media, online platforms should bear vicarious responsibility for what is disseminated. The participant asserted that online platforms publishing content and taking the protection of safe harbour is an absurd proposition, especially given the editorializing aspect at the backend.

Contrarily, the communication standpoint suggested considering the analogy of sending a message via post, wherein the postal system is not held responsible for the content. In this view, comparing online platforms to broadcast entities may be an apples-to-oranges comparison.

The event concluded with an engaging round of stakeholder interaction which together with the panel discussions brought to the forefront some few key takeaways that have been provided at the beginning of this report.