DGN Policy Brief 07
December 2020

Data Governance Network
Anchored by IDFC Institute

Internet Intermediaries and Online Harms: Regulatory Responses in India[i]

Faiza Rahman and Rishab Bailey

- *There is a lack of considered, holistic and evidence-based policy making in the context of designing solutions to address online harms.*
- *The intermediary liability framework under IT Act should be revisited (or a new law should be enacted), to ensure that calibrated obligations can be imposed on relevant classes of intermediaries, in a risk-based and proportionate manner.*

Introduction

- This paper reviews attempts to regulate intermediaries in India, with a view to answer three questions:
  - What are the harms that are driving calls for regulation?
  - What entities are sought to be regulated?
  - What are the obligations imposed on intermediaries?
- We carry out a detailed analysis of new and draft legislations, policy documents, court cases, and news reports to identify 7 broad categories of illegal/harmful online activity that have driven calls for regulation of intermediaries in India. The paper also examines emerging harms that are drawing regulatory attention. The table below lists these harms, and identifies the intermediaries who are seen as propagating or enabling such harms.

S. No.	Harm	Intermediary
1.	Hateful, offensive & dangerous content	Social media (Twitter, Facebook), Communication apps (Whatsapp)
2.	Obscene content	Social media (Facebook, TikTok), Pornographic websites and classifieds, Communication apps (Whatsapp, Sharechat)
3.	Defamatory content	Social media (Facebook, TikTok), Pornographic websites and classifieds, Communication apps (Whatsapp, Sharechat)
4.	Seditious and terrorism related content	Social media (Facebook, Twitter) and communication apps (Telegram, Whatsapp)
5.	Content harming democratic institutions	Communication apps (Whatsapp), Social media (Twitter, Facebook)
6.	IP infringements	E-commerce platforms (Amazon, Darvey's, Kaunsa.com), Classifieds (Olx, etc.)
7.	Sale/advertisement of regulated goods and services	Search engines (Google, Yahoo) and intermediaries aiding the sale/advertising of regulated goods or services (Dunzo, classifieds services, etc.)
8.	Emerging harms (fake news, online addiction, etc.)	Social media, platforms targeted at children, etc.

What harms are being regulated and how?

Our analysis of the regulatory responses to the above harms shows that policy responses, as well as court decisions have largely been disaggregated.

There have been attempts at setting out legal frameworks targeting certain types of online platforms, though few have been converted into statute.[ii] While a number of government committees have examined specific harms, these rarely discuss the intermediary liability framework in any detail but merely seek to impose greater obligations on different types of intermediaries.

Obligations have typically been imposed through executive writ or through court decisions.[iii] The nature of these obligations varies based on the type of harm at hand.[iv] That said, the preferred method of dealing with online harms is to block access to content/services. The reliance on blocking is problematic, not least due to the often excessive or arbitrary nature of such interventions, the absence of transparency around such measures, and due to the understandable inability of government and court processes to cope with the quantity of illegal content. One of the reasons for this could be that the statutory framework under the IT Act does not provide an adequate range of obligations that can be imposed on intermediaries.[v]

Who is being regulated?

Section 2(w) of the IT Act contains an extremely broad definition of the term "intermediary".[vi] All participants in the online

ecosystem, across the layers of the Internet, who transmit/carry or in any way provide a medium of access to and distribution of third party content, are included within its ambit. However, intermediaries can be of many different types,[vii] each performing a different role in the digital ecosystem. This functional differentiation is not appropriately recognised in the IT Act.[viii]

The issue of classification of intermediaries is critical as it makes little sense to impose similar obligations on a range of entities who provide different functionalities. A risk-based approach is more proportionate than adopting a one-size fits all policy. This is significant given that regulation of intermediaries can affect fundamental rights such as that of speech and privacy, as well as vital interests such as competition and innovation in the digital ecosystem.

Globally, while online platforms have typically been subject to less onerous regulation than intermediaries who provide access to the Internet, in recent years, various jurisdictions have increasingly sought to regulate this space. Regulatory proposals usually target platforms based on the specific risks they pose to the ecosystem.[ix]

An overview of cases shows that network and transport layer intermediaries are rarely involved in content dispute litigation.[x] Courts have largely avoided any discussion on the need to classify intermediaries or impose horizontal obligations, with the exceptions of obligations cast on social media/communication platforms and search engines, in the context of fake news and content that promotes pre-natal sex determination respectively.[xi]

The government has broadly focused on the need to regulate 3 'classes' of intermediaries - social media platforms,[xii] e-commerce and classifieds platforms,[xiii] and communication platforms.[xiv] However, no significant legal changes have been seen, with the exception of consumer protection rules being promulgated pertaining to e-Commerce platforms.

Conclusion

- The IT Act framework lacks clarity on whether different obligations can be imposed on different classes of interemediaries, as well as the nature and scope of such obligations. Therefore one has seen the creative interpretation of statute resulting in a patchwork of obligations, which may not always be consistent or proportionate.

- Any legal framework to address online harms ought to incorporate a calibrated approach to casting obligations on intermediaries.[xv]

- Despite the Supreme Court clarifying that an intermediary can only be required to take down content upon receiving a court order or directions from a government agency, courts have adopted different positions in some contexts, such as when dealing with child pornography and rape related content.[xvi] Further, such measures are increasingly being suggested in other contexts such as in the case of intellectual property violations. This could point to a 'slippery slope' problem.[xvii]

- Courts often resort to broad reading of the Section 79 framework or utilise their general powers, including that of contempt, to impose new substantive obligations. Regulatory interventions by the government have been episodic and frequently lacked transparency. This leads to (a) an arbitrariness in application of obligations, (b) imposition of new substantive obligations not contemplated by statute. Such attempts may not always strike the best balance between the various interests in the digital ecosystem.

- The lack of transparency and consistency in application of terms of service by platforms has been a significant cause for concern. The Section 79 framework needs revision to clarify the scope of self-regulatory processes to be adopted by intermediaries.[xviii] The law must impose clear requirements to ensure transparency and accountability of platforms towards their users.[xix]

- To sum up, the paper points to the need to:
  - impose narrowly tailored obligations on intermediaries based on their functions and the risk they pose.
  - clarify the scope of obligations to be imposed on platforms, most notably that of ex-ante monitoring/filtering of content, the manner of conducting take-downs in different contexts including norms for coordination with state agencies.
  - Clarify the nature and scope of self-regulatory frameworks.

Notes

i) This policy brief is based on a paper by Varun Sen Bahl, Faiza Rahman and Rishab Bailey titled “Internet Intermediaries and Online Harms: Regulatory Responses in India”, March 2020, Data Governance Network Working Paper 06, available at https://datagovernance.org/report/internet-intermediaries-and-online-harms-regulatory-responses-in-india

ii) Legislative changes have often taken the form of amendments to existing laws, to explicitly bring online platforms within their ambit. For instance, platforms selling pets now must now seek registration as "pet shops", ensure appropriate registration processes for third party sellers, etc.

iii) For instance, the government has issued directions to some communication platforms in the context of restricting the distribution of hate speech. Courts have generally refrained from imposing general obligations. Significant duties have been imposed in the context of harms seen as egregious, such as (i) advertisement of pre-natal sex determination kits/services on search engines, (ii) child pornography and rape related content on pornographic websites and social media platforms and (iii) intellectual property infringements on e-commerce platforms.

iv) These include, for instance, the imposition of automated filtering mechanisms, identifying users who post illegal content (or in some cases carrying out surveillance on these individuals), appointment of civil society and other independent entities to report on objectionable material, etc. Often, courts have focussed on the need for better liaison between executive agencies and intermediaries. In certain contexts, they have suggested imposition of data localisation norms, etc.

v) The IT Act permits authorities to block content or impose "due diligence" criteria (on all "intermediaries"). The scope of obligations that can be imposed using this "due diligence" criteria is limited, as this cannot be used to impose substantive obligations that are not contemplated by the statute. See Bailey, Parsheera and Rahman, 2018.

vi) It includes “any person who receives, stores or transmits an electronic record, or provides a service with respect of that record, on behalf of another person.”

vii) These may range from those not visible to the user for instance content delivery networks, internet exchange points, backhaul providers, etc. to those that actively host user information, such as WhatsApp, Facebook, Instagram, cloud-based services, etc.

viii) Section 79 recognises a basic functional difference between conduits, cache and hosts. Further, it confers immunity from prosecution to intermediaries based on the role they play in the ecosystem and their `participation' in the specific harm at hand. While certain intermediaries - notably cyber cafes - have had specific obligations placed on them in the form of rules notified under Section 79, there is doubt on whether different obligations can be imposed under this provision on different classes of intermediaries, going beyond the basic conduit/cache/host classification. See Bailey, Parsheera and Rahman, 2018

ix) Jurisdictions such as Germany, the United Kingdom and Europe for instance, have sought to impose additional obligations on large social media platforms, intermediaries hosting user-generated content and e-commerce platforms.

x) With some exceptions pertaining to say, to the ban of pornographic/obscene content.

xi) Even in such cases however, it is unclear to what extent obligations have been applied across the board, including to smaller or marginal service providers.

xii) Such as Facebook, Twitter, YouTube, Sharechat and TikTok.

xiii) Such as Amazon, Flipkart, Olx, etc.

xiv) WhatsApp, Telegram, etc.

xv) This is in view of the multiplicity of functions performed by different intermediaries, the distinct approaches being adopted by other jurisdictions, and the key concerns that have animated the call for regulation of intermediaries in India. Note that a more targeted approach has been followed in the recently announced regulations pertaining to e-commerce platforms. However, these rules have been implemented under the Consumer Protection Act, 1934, which targets certain specific types of harms. While defining these categories with precision may be difficult, an early attempt has been made in the draft e-Commerce Policy of 2019, which recognises the need to impose differential obligations on marketplaces, search engines and payment gateways.

xvi) See Shreya Singhal v. Union of India, Myspace Inc v. Super Cassettes Industries Ltd. and Kent RO v. Amit Kotak. However, in the Sabu Mathew George case, the Supreme Court directed search engines to preemptively block access to content based on identified key-words. This essentially: (1) creates an alternative way to deem that intermediaries receive "actual knowledge", not in form of orders for individual pieces of content, but through a single order setting out a list of key-words that would operate on a standing basis; and (2) creates an implicit pre-screening requirement, by requiring intermediaries to "proactively" filter content that maps against these key-words. Decisions with similar implications were pronounced in In Re:Prajwala (2015), Christian Louboutin v. Nakul Bajaj (2018) and in the Blue Whale case (2017).

xvii) That is, where proactive interventions are incrementally being considered for broader (and arguably less harmful) types of online content.

xviii) The IT Act framework currently provides for a bare-bones list of self-regulatory processes to be followed by intermediaries. Intermediaries must provide notice to users of what constitutes illegal behaviour, warn them of possible action that may be taken, institute a grievance redress process, etc.

xix) The Manila Principles on Intermediary Liability and Santa Clara Principles on Transparency and Accountability in Content Moderation, may provide a minimum set of standards with which to begin such a conversation.

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The National Institute of Public Finance and Policy (NIPFP) is a centre for research in public economics and policies. Founded in 1976, the institute undertakes research, policy advocacy and capacity building in a number of areas, including technology policy. Our work in this space has involved providing research and policy support to government agencies and contributing to the creation and dissemination of public knowledge in this field. Our current topics of interest include privacy and surveillance reform; digital identity; Internet governance and rights, and regulation of emerging technologies. We also focus on research that lies at the intersection of technology policy, regulatory governance and competition policy.

About the Author

The authors are technology policy researchers at the National Institute of Public Finance and Policy (NIPFP), New Delhi.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the National Institute of Public Finance and Policy.

IDFC Institute
3rd Floor, Makhija Chambers, 196 Turner Road,
Bandra(W), Mumbai 400050

/idfcinstitute @idfcinstitute /IDFCInstitute