

REPORT ON INTERMEDIARY LIABILITY IN INDIA

The Centre for Communication Governance at
National Law University Delhi

Vasudev Devadasan

December 2022





Published by

National Law University Delhi Press,
Sector 14, Dwarka. New Delhi 110 078

ISBN

978-93-84272-39-5

© National Law University Delhi 2022

All Rights Reserved

Patron: Prof. (Dr.) Harpreet Kaur

Vice Chancellor (I/c), NLU

Faculty Advisor, CCG: Dr. Daniel Mathew

Executive Director, CCG: Jhalak M. Kakkar

Supported by

Friedrich Naumann Foundation For Freedom



Designed by

Simran Kaur

Printed by

Naveen Printers, New Delhi



Report on Intermediary Liability in India

Centre for Communication Governance
Vasudev Devadasan

FOREWORD

The growth of the internet has facilitated unprecedented economic growth and democratic participation. The advent of social media, online streaming, and e-commerce has enriched the lives of all Indians, allowing citizens greater access to each other, online content, and economic goods. However, just as the amount of content on the internet has increased exponentially, so too has the existence of unlawful content and the accompanying need for regulation. Given this new frontier of human interaction, legal systems must adapt to protect citizens from the harms originating from unlawful content on the internet yet must do so without restricting individual rights or sacrificing the social, economic, and democratic goods that the internet has given birth to.

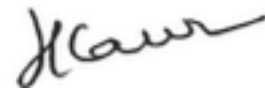
The question of when intermediaries are liable, or conversely *not liable*, for content they host or transmit is at the heart of regulating content on the internet. Section 230(c) of the Communications Decency Act adopted by the United States Congress in 1996 protecting intermediaries from liability arising from content on their networks has often been described as ‘the twenty-six words that made the internet possible’. Ensuring that intermediaries are not strictly liable for content on their networks has led to the revolutions of social media and internet commerce discussed above. It has permitted intermediaries to host billions of pieces of content without the crippling risk associated with being held liable for a bad actor uploading unlawful content onto their sites.

However, the corollary to this ‘immunity’ or ‘safe harbour’ is that intermediaries may turn a blind eye to unlawful content on their networks. Recently, there have been increasing calls to ensure that intermediaries are more responsive and accountable for unlawful content on their networks, without sacrificing the freedom from liability that permits them to host billions of pieces of user generated content. Today, intermediary liability is at cross-roads, with India and countries across the world attempting to strike a balance between requiring intermediaries to be responsive to unlawful

content without curtailing the individual, social, economic, and democratic freedoms the modern internet facilitates.

This report by the Centre for Communication Governance (CCG) at the National Law University Delhi is a timely and excellent initiative to analyse the challenges India's intermediary liability regime faces, particularly as the country moves towards introducing data protection legislation and replacing the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 (IT Act). The report critically engages with the evolution of intermediary liability under IT Act since its adoption until the recently adopted Intermediary Guidelines and Digital Media Ethics Code. The report catalogues and analyses seminal case-law in the field, while also examining the impact of intermediary liability on the allied fields of copyright and e-commerce. The report presents a comprehensive overview of the regulatory environment intermediaries in India face while examining key regulatory debates that will shape upcoming amendments to India's legislative framework for information technology.

I congratulate CCG for this insightful research. I hope they will continue to undertake such projects that are of immense relevance to judges, lawyers, policymakers, industry, students, and Indian citizens at large.



Prof. (Dr.) Harpreet Kaur
Vice Chancellor (I/c)
National Law University Delhi

ACKNOWLEDGEMENTS

This report was made possible by the generous support we received from National Law University Delhi. The Centre for Communication Governance (CCG) would therefore like to thank the Vice Chancellor (I/c) Professor (Dr.) Harpreet Kaur and the Registrar (I/c) Professor (Dr.) Anupama Goel for their guidance. CCG would also like to thank our Faculty Advisor Dr. Daniel Mathew for his continuous direction and mentorship. This report would not be possible without the support provided by the Friedrich Naumann Foundation for Freedom, South Asia. We are grateful for comments received from the Data Governance Network and its reviewers. CCG would also like to thank Faiza Rahman and Shashank Mohan for their review and comments, and Jhalak M. Kakkar and Smitha Krishna Prasad for facilitating the report. We thank Oshika Nayak of National Law University Delhi for providing invaluable research assistance for this report. Special thanks to the ever-present and ever-patient Suman Negi and Preeti Bhandari for the unending support for all the work we do at CCG. Lastly, we would also like to thank all members of CCG for the many ways in which they supported the report.

Author: Vasudev Devadasan,
Project Officer, Centre for Communication Governance

CONTENTS

Key Insights	1
1 Introduction	9
2 India's Internet Landscape	13
2.1. Internet access and usage	15
2.2. Key online intermediaries in India	17
2.3. Internet Shutdowns and banning of apps	19
2.4. Social media, misinformation, and real-world violence	25
3 Intermediaries in India	29
3.1. Defining network and online intermediaries	31
3.2. Licensing system for ISPs	34
4 Safe Harbour Under the Information Technology Act	39
4.1. The Information Technology Act and Intermediary Guidelines 2011	42
4.2. Shreya Singhal vs. Union of India and its aftermath	57
4.3. Intermediary Guidelines 2021: Rule 3	68
4.4. Intermediary Guidelines 2021: Rule 4	85
4.5. Intermediary Guidelines 2021: Subsequent developments	105
5 Safe Harbour Under the Copyright Act, 1957	121
5.1. Secondary infringement and safe harbour under the Copyright Act	123
5.2. Safe harbour under the IT Act for copyright infringement	127
6 Safe Harbour for E-Commerce Entities	133
6.1. Consumer Protection Act 2019 and the E-Commerce Rules 2020	135
6.2. Contested functionality of e-commerce platforms	140
7 Courts, Non-Monetary Liability, and Website Blocking	147
7.1. Injunctions and non-monetary liability	149
7.2. Blocking at the behest of courts	159
8 Blocking Content Under IT Act	163
8.1. Procedure for blocking content	165
8.2. Legal and practical challenges to blocking	169
8.3. Disclosures of blocking by the Union Government	173

LIST OF ABBREVIATIONS

Consumer Protection Act	Consumer Protection Act, 2019
Copyright Act	The Copyright Act, 1957
Copyright Rules	Copyright Rules, 2013
CrPC	The Code of Criminal Procedure, 1973
E-Commerce Rules	Consumer Protection (E-Commerce) Rules, 2020
GAC	Grievance Appellate Committee(s)
Intermediary Guidelines 2011	Information Technology (Intermediary Guidelines) Rules, 2011
Intermediary Guidelines 2021	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
ISP	Internet Service Provider
IT Act	The Information Technology Act, 2000
IT Blocking Rules	Information Technology (Procedure and Safeguards for Blocking of Information by Public) Rules, 2009
MEITY	Ministry for Electronics & Information Technology
MIB	Ministry of Information & Broadcasting
October 2022 Amendment	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022
Patents Act	The Patents Act, 1970
RTI Act	Right to Information Act, 2005
SSM Intermediary	Significant Social Media Intermediary
Telegraph Act	The Indian Telegraph Act, 1885
Trade Marks Act	The Trade Marks Act, 1999
TSP	Telecom Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

KEY INSIGHTS

This report aims to provide a comprehensive overview of the regulation of online intermediaries and their obligations with respect to unlawful content. It updates and expands on the Centre for Communication Governance's 2015 report documenting the liability of online intermediaries to now cover the decisions in *Shreya Singhal vs. Union of India* and *Myspace vs. Super Cassettes Industries Ltd*, the Intermediary Guidelines 2021 (including the October 2022 Amendment), the E-Commerce Rules, and the IT Blocking Rules.

It captures the over two decades of regulatory and judicial practice on the issue of intermediary liability since the adoption of the IT Act. The report aims to provide practitioners, lawmakers and regulators, judges, and academics with valuable insights as they embark on shaping the coming decades of intermediary liability in India. Some key insights that emerge from the report are summarised below.

1. Limitations of intermediary liability as a regulatory approach: Under Section 79(2) of the IT Act, intermediaries must observe “*due diligence*” to enjoy immunity, or ‘safe harbour’, for content they host. By imposing a variety of obligations such as transparency reporting, proactive monitoring, and a dispute settlement process as part of this due diligence requirement (through the Intermediary Guidelines 2021 and the October 2022 Amendment), the conditions precedent for safe harbour have emerged as a key tool to regulate intermediaries. In other words, the government has attempted to use the pre-conditions to safe harbour to modify intermediary behaviour and fulfil its regulatory goal of curbing online harms.

However, the pre-conditions for safe harbour are only evaluated when an intermediary is sought to be held liable (through individual lawsuits or prosecutions) for hosting or transmitting allegedly unlawful content. The success of intermediary liability in achieving the desired regulatory outcomes thus largely depends on the risk intermediaries associate with the loss of safe harbour and lawsuits in India. In the cases analysed in this report, there is little judicial consistency in the application of secondary liability principles to intermediaries, including the obligations set out in Intermediary Guidelines 2021, and monetary damages for transmitting or hosting unlawful content are almost never imposed on intermediaries. This suggests that, in the Indian context, imposing key obligations such as transparency reporting, dispute resolution, and proactive monitoring on intermediaries by altering the pre-conditions to safe harbour may not always be the desired regulatory approach due to its patchwork enforcement through individual legal actions. *See sections 3.1, 4, and 4.4(ii).*

2. Immunity for content moderation and curation: Section 79(2) of the IT Act grants intermediaries safe harbour provided they act as mere conduits, not interfering with the transmission of content. Unlike the European E-Commerce Directive which the IT Act is modelled on, Section 79(2) does not explicitly provide immunity to ‘hosting’ providers. This narrow language in Section 79(2) regularly conflicts with the functionality offered by many modern-day online entities, who may curate content for users through the processes of content moderation and algorithmic ranking. There exists ambiguity as to how such services are to be interpreted in the context of Section 79(2). The Intermediary Guidelines 2021 have attempted to partially remedy this ambiguity by expressly stating that voluntary content moderation will not result in an intermediary ‘interfering’ with the transmission under Section 79(2). However, ultimately amendments to the IT Act are required to provide regulatory certainty over the extent to which content moderation and curation will be immunised. *See sections 4.1(ii) and 4.3(iv).*

3. Intermediary status and immunity to be decided on case-by-case basis:

In several cases examined in this report, courts ruled that the question of whether an entity was an ‘intermediary’ or had complied with the requirements of Section 79 was: (i) a question of fact to be decided at trial; and (ii) assessed based on the overall operations of the entity. Whether an entity is an intermediary should be decided based on its *functionality with respect to the content it is sued for*. An entity’s classification as an intermediary is not a status that applies across all its operations (like a ‘company’ or a ‘partnership’), but rather the function it is performing *vis-à-vis* the specific electronic content in question. Thus, the same website may be an intermediary where it hosts a user’s content, but not an intermediary where it uploads its own content. Similarly, courts should determine whether an intermediary complied with the conditions of Section 79 in the context of the content it is being sued for. Consistently making this determination at a *preliminary stage of litigation* would greatly further the efficacy of Section 79’s safe harbour approach by providing legal certainty as to when intermediaries are liable and when they are not. *See sections 3.1 and 4.*

4. Ambiguity over *Shreya Singhal* and actual knowledge: The Supreme Court in *Shreya Singhal* held that intermediaries were not deemed to have ‘actual knowledge’ of unlawful content (and consequently not at risk of losing safe harbour for failure to remove such content) until they received a court order or are notified by the government. The judgement was hailed as providing crucial free speech protections to an Intermediary Guidelines 2011 regime that provided few safeguards against lawful content being removed and no method for reinstatement. However, the decision has also been criticised

from some quarters for placing the onus and cost of taking down any content (irrespective of the ease of determining its legality) firmly on the aggrieved party, requiring them to obtain a judicial order.

Rule 3(2)(b) of the Intermediary Guidelines 2021 creates a carve out from this judicial-order-first approach, requiring intermediaries to take efforts to remove content where users complain that the content depicts them in nude or sexual contexts. The October 2022 Amendment goes further, requiring intermediaries to make reasonable efforts to “*cause*” their users not to upload certain categories of content and ‘act on’ user complaints against content within seventy-two hours. Requiring intermediaries to remove content at the risk losing safe harbour in circumstances other than the receipt of a court or government order *prima facie* violates the decision of *Shreya Singhal*. While the current regulatory environment does have more safeguards for lawful content than existed in 2015, upcoming judicial decisions will likely shape the future of the ‘actual knowledge’ standard. *See sections 4.2, and 4.5(ii).*

5. Questions over operation of GACs: The October 2022 Amendment allows individuals to appeal to a GAC against the decision by an intermediary’s Grievance Officer to keep up or remove content. While the Amendment stipulates that two members of every GAC shall be independent, no detail is provided as to how such independence shall be secured (e.g., security of tenure and salary, oath of office, minimum judicial qualifications etc.). Such independence is vital as GAC members are appointed by the Union Government but the Union Government or its functionaries or instrumentalities may also be parties before a GAC.

Further, given that the GACs are authorities ‘under the control of the Government of India’, they have an obligation to abide by the principles of natural justice, due process, and comply with the Fundamental Rights set out in the Constitution. In this context, it is concerning that the October 2022 Amendment does not guarantee a hearing for the originator whose content is being adjudicated upon by a GAC (relevant in appeals against alleged failures to remove content), nor is there a requirement that GACs must issue a reasoned written order. Further, if a GAC directs the removal of content beyond the scope of Article 19(2) of the Constitution, questions of an impermissible restriction on free expression may be raised. This is relevant as lots of content on the internet (e.g., spam or misinformation) may not be permissibly restricted under Article 19(2) despite its undesirability. *See section 4.5(ii).*

6. Legal and practical challenges with government blocking: There exists uncertainty over the exact legal source of the government’s power to block content. Section 69A of the IT Act expressly grants the Union Government power to block content, subject to a hearing by the originator (uploader) or intermediary. However, Section 79(3)(b) of the IT Act may also be utilised to require intermediaries to take down content absent some of the safeguards provided in Section 69A. The fact that the Government has relied on both provisions in the past and that it does not voluntarily disclose blocking orders makes a robust legal analysis of the blocking power challenging. *See section 4.3(iii).*

The decision in *Shreya Singhal* and the requirements of due process support the understanding that the originator must be notified and granted a hearing under the Blocking Rules prior to their content being restricted under Section 69A. This obligation would apply where the originator can be contacted through publicly identifiable information. Decisions of the Supreme Court also support the position that blocking orders should be disclosed absent a clearly established need for secrecy that can be tested by courts. However, evidence suggests that the government regularly does not provide originators with hearings, even where the originator is known to the government. Instead, the government directly communicates with intermediaries away from the public eye, raising rule of law concerns. Judicial decisions in the *Tanul Thakur* and *Twitter* writ petitions are likely to provide further guidance on this issue. *See section 8.*

7. Issues with tracing first originators: The stated intention behind requiring messaging services to identify the “*first originator*” of a piece of content is to aid investigations of real-world violence instigated or fuelled by the content. However, both the methods proposed for the implementation of this requirement (hashing unique messages and affixing encrypted originator information) are easily circumvented, require significant technical changes to the architecture of messaging services, offer limited investigatory or evidentiary value, and will likely undermine the privacy and security of all users to catch a few bad actors. Given these considerations, it is unlikely that such a measure would satisfy the proportionality test laid out by current Supreme Court doctrine. While some messaging services continue to share metadata with law enforcement on request, the requirement of tracing first originators has yet to be implemented and has been challenged in courts by WhatsApp and Facebook as well as Indian citizens. *See section 4.4(iii).*

8. Judicial inconsistency and ad-hoc arrangements: When injunctioning online content, courts typically employ a three-part test: (i) whether the plaintiff has established a *prima facie* case; (ii) whether the plaintiff is likely to suffer irreparable harm; and (iii) whom the balance of convenience lies in favour of. However, an analysis of injunction decisions belies the significant discretion this standard confers on judges, often resulting in inconsistent rulings. Crucially, the contents of court orders are often sweeping, imposing vague compliance burdens on intermediaries. When issuing injunctions against online content, courts should limit blocking to specific URLs. Further courts should be cognisant of the fact that intermediaries have themselves not committed any wrongdoing, and the effect of an injunction should be seen as meaningfully dissuading users from accessing content rather than an absolute prohibition.

Content restricted online often re-appears at other locations on the internet. Regularised structures to deal with this issue are yet to emerge, with courts adopting ad-hoc solutions such as permitting plaintiffs to identify similar content or deputing court administrators to determine subsequent takedowns. *See section 7.*

9. Local officers to ensure compliance: The Indian Government is more concerned than ever with the harms resulting from online content and the lack of cooperation between online intermediaries and Indian authorities. A key goal of the Intermediary Guidelines 2021 is ensuring intermediaries, particularly social media platforms, are accountable to both Indian authorities and users for the content they host, and the decisions they make regarding online speech. This has led to a shift in the architecture of regulation, with a greater emphasis on enforcing government speech rules online and increased transparency and accountability from SSM Intermediaries for their decisions *vis-à-vis* online content. The reality of ensuring compliance from social media companies that are global corporations has been addressed by requiring them to have local officers, upon whom penal consequences may be imposed in cases of non-compliance with Indian regulations. *See section 4.4.*

10. Concern over use of rule-making power: The Intermediary Guidelines 2021 and October 2022 Amendment have been promulgated under Sections 87(1), 87(2)(z), and 87(2)(zg) of the IT Act. These provisions empower the MEITY to prescribe the procedure for blocking content under Section 69A of the Act and the guidelines to be followed by intermediaries to retain safe harbour under Section 79(2) respectively. However, the Guidelines and Amendment pertain to a wide range of issues, from encryption and surveillance to the creation of adjudicatory bodies (the GACs). Such regulation could potentially exceed the MEITY's rule making powers under the above-mentioned provisions of the IT Act. It is notable that several legal challenges against the Intermediary Guidelines 2021 have assailed their legality on this ground. *See sections 4.1(ii), 4.4, and 4.5.*

11. Traditional notice and take down for copyright infringement: The Copyright Act imposes secondary liability for copyright infringement but also offers safe harbour to online intermediaries accused of infringement where the storage is temporary. The Copyright Act's safe harbour is contingent on a notice and takedown regime, requiring intermediaries to take down content pursuant to a complaint by the copyright owner, but permits them to reinstate such content unless the complainant obtains a court order within twenty-one days. In 2016, the High Court of Delhi ruled that intermediaries could seek safe harbour under both the Copyright Act and IT Act parallelly. Despite the Supreme Court decision in *Shreya Singhal* holding that a court order was required prior to takedown under the IT Act, the High Court held that in cases of alleged copyright infringement, a notice by the copyright owner would suffice to activate the intermediary's obligation to take down the content. According to the High Court, the decision in *Shreya Singhal* concerned 'unlawful speech' (e.g., hateful or inciteful speech) which was sufficiently distinct from 'copyright infringing content' to justify a different approach. *See section 5.*

12. Express safe harbour protections for e-commerce entities: In 2018, a series of decisions in the High Court of Delhi held that certain e-commerce entities were not intermediaries eligible for safe harbour. The High Court concluded that by providing additional real-world services such as logistics and warehousing, these entities exceeded the functionality of an intermediary under the IT Act. One such decision was overruled, and larger benches of the High Court have since cast doubt on the correctness of these findings. Crucially, in 2020, the Union Government introduced the E-Commerce Rules. The Rules expressly state that 'marketplace e-commerce entities' are eligible for safe harbour under the IT Act. A marketplace e-commerce is a platform that facilitates transactions between buyers and sellers without

selling its own goods on the platform. The E-Commerce Rules provide certainty over the safe harbour protections for e-commerce entities and courts have already begun granting such platforms immunity. While courts have ruled that 'actual knowledge' would require a court order in trademark disputes concerning e-commerce entities, settled judicial practice is yet to emerge. *See section 6.*

We welcome your comments and feedback. You can write to us at ccg@nludelhi.ac.in

1

Introduction

The adoption of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**‘Intermediary Guidelines 2021’**) and their revision in October 2022 represents a paradigm shift in India’s regulation of online intermediaries. However, India’s regulatory regime for intermediaries is no stranger to paradigm shifts. In 2009, the Information Technology Act, 2000 (**‘IT Act’**) was amended to expressly grant online intermediaries immunity for third-party content they host. In 2011, the Indian Government introduced a notice and takedown regime through the Information Technology (Intermediary Guidelines) Rules, 2011 (**‘Intermediary Guidelines 2011’**), requiring intermediaries to take down content in response to private complaints to retain their immunity. In 2015, the Supreme Court of India re-interpreted provisions of the IT Act and the Intermediary Guidelines 2011 to rule that a judicial or government order was necessary before an intermediary was legally required to take down content or risk losing safe harbour.

The Intermediary Guidelines 2021 codifies the 2015 ruling of the Supreme Court and introduces what can best be described as nascent attempts at platform regulation to India’s regulatory regime for intermediaries. The new Guidelines are already subject to numerous legal challenges, and the courts may yet cause further shifts in regulation. In the interim, the proliferation of the internet across different areas of Indian life has led to distinct areas of study *within* the realm of intermediary regulation, most notably copyright infringement, the regulation of e-commerce entities, and the blocking of content by State authorities and courts.

These developments have sharpened the focus on intermediary liability as an area of study. Intermediary liability for unlawful content has emerged as a delicate balancing act between the harms associated with online speech and the need to ensure free speech and democratic participation on the internet. This balance is maintained through the regulation of online intermediaries, particularly large social media platforms, that represent key facilitators of online speech. Governments have a legitimate interest in protecting users from the harms of child sex abuse material, non-consensual intimate content, defamation, and hate speech. On the other hand, overtly strict liability regimes may risk constitutionally protected speech being taken down, impermissibly restricting free expression and democratic participation.

In attempting to strike this balance, the Indian Government has relied almost exclusively on intermediary liability. Thus, this report asks: *When are intermediaries liable for illegal content they host, and who determines the legality of this content?* These questions, and the secondary enquiries they raise, are central to understanding the balance struck between online harms and free speech. For example, allowing users to determine what content is illegal (and

holding intermediaries liable if they fail to respond to user complaints i.e., a notice and take down regime) may reduce the volume of harmful speech on the internet, but it may also result in the silencing of offensive but constitutionally protected speech. This focus on the implications of intermediary liability on *how online content is governed* extends the scope of the present report to include injunctions against online content by courts and blocking orders by the Indian Government but excludes the surveillance obligations imposed on intermediaries.

This report builds on the Centre for Communication Governance's 2015 report documenting the regulation of online intermediaries. It documents subsequent regulations and seminal court cases and analyses the regulatory and judicial trends they represent. The regulation of online intermediaries under the IT Act has always centred around Section 79 of the IT Act and its safe harbour protections. The present report is an effort to document and analyse the evolution of these protections, but also to understand their relationship with other areas where online intermediaries are regulated, such as copyright infringement and consumer protection. These areas receive separate sections in the report due to their distinct regulation of intermediary liability that nonetheless intersects with the IT Act. This exercise is carried out with an awareness of the power dynamics between users, governments, and intermediaries. The intent is to provide a holistic picture of the regulatory environment online intermediaries face in 2022 *vis-à-vis* unlawful content.

Understanding the online and real-world harms that have resulted from online content, and the government's response is essential to understanding the regulatory trends in intermediary regulation. Thus, Section 2 of this report examines the state of internet access in India and how Indians are using the internet. Section 3 examines who 'intermediaries' are under the IT Act, differentiating between service providers such as Internet Service Providers ('ISPs') and Telecom Service Providers ('TSPs') on the one hand, and online intermediaries on the other. Section 4 documents the evolution of safe harbour protections granted to intermediaries under the IT Act, culminating in an analysis of the Intermediary Guidelines 2021 and their amendments in October 2022. Section 5 examines the separate safe harbour granted under the Copyright Act, 1957 ('**Copyright Act**'), and its interaction with the immunity provided by the IT Act. Section 6 documents the rise of actions against e-commerce platforms, and the extent to which safe harbour protections have been extended to these entities. Section 7 analyses how courts have dealt with actions against intermediaries, including injunctions against content, web-site blocking, and the imposition of monitoring obligations. Section 8 documents the procedure for government blocking of content and examines the practical and legal challenges raised by this practice.



2

India's Internet Landscape

Intermediary liability has emerged as the key regulatory tool for the Indian Government to regulate online content, balancing online harms with free expression. While harms from online content are not themselves unique, understanding India's internet landscape and the types of online harms the Indian Government is most concerned with is essential to understand recent developments in the regulation of intermediaries. For example, the mobile-first nature of India's internet landscape coupled with the large number of WhatsApp users has led to the 'traceability' of content on messaging apps becoming an intermediary liability and content governance issue in India. This section of the report provides an overview of India's internet landscape and the types of online harms that are prevalent to contextualise India's approach to intermediary liability.

2.1. Internet access and usage

As of March 2022, India had 824.89 million internet subscribers.¹ An analysis of these subscribers reveals that the Indian internet landscape is characterised by a mobile-first approach, driven by the availability of cheap internet data plans from private telecom providers and the proliferation of smartphones in the country. Of the total internet subscriber base, 797.61 million (97%) were wireless internet subscribers and 27.27 million (3%) were wired internet subscribers.² Of the 797.61 million wireless internet subscribers, 796.43 million users (>99%) accessed the internet using a mobile phone or an internet dongle, with a mere 1.18 million (<1%) accessing the internet through a fixed wireless connection such as wi-fi, wi-max, or point-to-point radio.³

The penetration of high-speed internet connectivity in India has improved significantly over the last decade. Amongst internet users, 788.30 million internet users (96%) were broadband subscribers, and 36.59 million users (4%) were narrowband subscribers.⁴ Amongst wireless data subscribers, 2G data usage contributed 0.24% of the total volume of wireless data usage, with 3G and 4G usage accounting for 1.31% and 98.45% of total data usage, respectively.⁵

However, internet subscriber data also reveals significant inequalities in internet access. Urban districts reported 103 internet subscribers for every 100 people, while rural districts reported only 37 subscribers per 100 people.⁶ Geographic inequalities also exist. For example, Andhra Pradesh (68), Kerala (85), and Maharashtra (79) possessed more internet subscribers per 100 people than Rajasthan (55), Uttar Pradesh (43), and Bihar (35).⁷ Gender may also impact internet access, with a 2019 study noting that only 16% of Indian women used mobile and internet services, and that women were 56% less likely to access the internet on their mobile phones.⁸

As of March 2022, internet access in India was provided by 660 ISPs.⁹ However, 99.07% of all internet subscribers accessed the internet using the top ten ISPs.¹⁰ Amongst Indian ISPs, Reliance Jio held a 49.62% market share, with Bharti Airtel (28.57%), Vodafone Idea (16.45%) and Bharat Sanchar Nigam Limited (3.65%) also key market players.¹¹

1 Telecom Regulatory Authority of India, 'The Indian Telecom Services Performance Indicators: January - March, 2022' (Telecom Regulatory Authority of India 2022) 34 <https://www.trai.gov.in/sites/default/files/QPIR_26072022_0.pdf>.

2 *ibid.*

3 *ibid.* 35.

4 *ibid.* India's telecom regulator defines narrowband users as users with a bandwidth of less than 512 kbit/s and broadband users as users with a minimum bandwidth of 512 kbit/s or greater.

5 *ibid.* 21.

6 *ibid.* 42–43. Population data is based on both subscriber data provided by operators and reports by the National Commission on Population, Ministry of Health & Family Welfare (Government of India).

7 *ibid.*

8 Smriti Parsheera, 'India's on a Digital Sprint That Is Leaving Millions Behind' *BBC News* (17 October 2019) <<https://www.bbc.com/news/world-asia-india-49085846>> accessed 10 September 2021.

9 Telecom Regulatory Authority of India (n 1) 34.

10 *ibid.* 39.

11 *ibid.*

It is estimated that more than half of India's internet users are non-English language users, and this category is expected to grow significantly faster than the number of English language users.¹² A 2017 study by KPMG and Google estimated that between 2017 and 2021, Indian-language internet users would grow from 234 million to 536 million, while English-language internet users were expected to grow from 176 million to 199 million.¹³

12 KPMG India and Google India, 'Indian Languages – Defining India's Internet' (2017) <<https://assets.kpmg/content/dam/kpmg/in/pdf/2017/04/Indian-languages-Defining-Indias-Internet.pdf>>. The study was based on multi-phased research that included quantitative interviews of 7060 Indian internet users aged 15-50 in both rural and urban areas. Respondents had primary educational qualifications in at least one of eight identified Indian languages and accessed the internet at least once a week.

13 *ibid.*

2.2. Key online intermediaries in India

According to data from the popular web analytics tool Alexa, the top ten websites in India as of April 2022 are: ¹⁴

14 Alexa, 'Top Sites in India' (*Alexa*, 25 April 2022) <<https://www.alexa.com/topsites/countries/IN>> accessed 25 April 2022.

RANK	WEBSITE
1	Google.com
2	YouTube.com
3	Facebook.com
4	Amazon.in
5	Instagram.com
6	Linkedin.com
7	Whatsapp.com
8	Google.co.in
9	Twitter.com
10	Flipkart.com

This list demonstrates how the internet experience of Indians is significantly structured around search, social media, and online commerce. Given the mobile-first nature of India's internet subscriber base, mobile applications serve as crucial platforms for users to interact with content on the internet. The mobile applications with the most average monthly users in India in 2021 were:¹⁵

15 Data Reportal, 'Digital 2022: India' (*DataReportal – Global Digital Insights*) <<https://datareportal.com/reports/digital-2022-india>> accessed 25 April 2022.

RANK	APPLICATION
1	WhatsApp
2	Facebook
3	Truecaller
4	Instagram
5	Facebook Messenger
6	Amazon
7	PhonePe
8	Flipkart
9	MX Player
10	MyJio

2.3. Internet Shutdowns and banning of apps

The increased use of the internet to engage in social, political, and commercial activity has also led to scrutiny and interference by State authorities. A range of measures have been employed to restrict and regulate online activity including blanket restrictions to internet access, prohibitions on specific online platforms, and the restriction of individual websites. The following sections examine the first two interventions with website blocking independently examined in section 8 of this report.

(i) Internet Shutdowns

India has experienced several localised instances of 'Internet Shutdowns', where the government has intentionally disrupted or totally severed access to internet and telecom communications, adversely impacting users' ability to freely access the internet. Internet Shutdowns may be distinguished from website-blocking (which the Union Government also conducts), with the former restricting users' access to the internet as a whole, and the latter restricting access to select destinations on the internet.¹⁶ Although documenting Internet Shutdowns remains a challenge, media reports indicate that Internet Shutdowns are typically localised to a single district or a cluster of districts and imposed for a duration of eight to seventy two hours.¹⁷ However, more wide-ranging, and longer Internet Shutdowns have been imposed in Rajasthan,¹⁸ West Bengal¹⁹ and the (now) Union Territory of Jammu and Kashmir.²⁰

Internet Shutdowns are by their nature difficult to report on, and statistics on the exact number of Shutdowns in India vary.²¹ Indian authorities do not voluntarily disclose statistics on the number of Internet Shutdowns or the reasons for imposing Shutdowns. Despite this, based on verified media reports of Internet Shutdowns, India topped the list of countries that have shut down the internet in both 2018 and 2019 by a considerable margin (e.g., Access Now reported that in 2019, India shut the internet down 105 times, compared to twelve times by Venezuela, the country in second place).²² The number of Internet Shutdowns between 2012 and 2021 in India, based on verified media reports, is set out in the table below.

¹⁶ *Anuradha Bhasin v Union of India* 2020 (3) SCC 637 [89].

¹⁷ Software Freedom Law Centre, 'Internet Shutdowns in India' (*Internet Shutdowns*, 26 September 2020) <<https://internetsutdowns.in>> accessed 26 September 2020. The website compiles verified media reports of internet shutdowns across India.

¹⁸ Aihik Sur, 'Internet Shutdown at Karauli in Rajasthan Enters 5th Day, to Continue till April 7' *MediaNama* (6 April 2022) <<https://www.medianama.com/2022/04/223-internet-shutdown-karauli-rajasthan-extended/>> accessed 25 April 2022; Milan Sharma, 'India's Internet Shutdowns: Looking beyond J&K, Rajasthan the New Hotbed' (*India Today*, 3 July 2022) <<https://www.indiatoday.in/india/story/india-internet-shutdowns-looking-beyond-j-k-rajasthan-new-hotbed-1969664-2022-07-03>> accessed 25 July 2022.

¹⁹ Roshan Gupta, 'Darjeeling's 100-Day Internet Shutdown | Internet and Banking: A Trust Broken' (*MediaNama*, 1 October 2018) <<https://www.medianama.com/2018/10/223-darjeelings-100-day-internet-shutdown-trust-broken-internet-and-banking/>> accessed 25 July 2022.

²⁰ Prashasti Awasthi, 'How the Internet Was Restored in Kashmir: Timeline' *Business Line* (5 March 2020) <<https://www.thehindubusinessline.com/news/national/how-the-internet-was-restored-in-kashmir-timeline/article30989727.ece>> accessed 23 September 2020.

²¹ Software Freedom Law Centre, 'IT Standing Committee's Report on Internet Shutdowns' (*SFLC.in*, 12 August 2021) <<https://sflc.in/it-standing-committees-report-internet-shutdowns>> accessed 25 April 2022.

²² Access Now, 'Access Now: Keep It On 2021 Report' (Access Now 2021) 2 <<https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>>.

YEAR	NUMBER OF SHUTDOWNS ²³	CUMULATIVE TOTAL
2012	3	3
2013	5	8
2014	6	14
2015	14	28
2016	31	59
2017	79	138
2018	134	272
2019	106	378
2020	129	507
2021	88	595

23 Software Freedom Law Centre, 'Internet Shutdowns in India' (n 17).

Internet Shutdowns are imposed using Section 144 of the Code of Criminal Procedure, 1973 (“CrPC”) and the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017.²⁴ Both the Union Government and State Governments have resorted to Internet Shutdowns, citing several reasons including terrorism,²⁵ public order,²⁶ public protests,²⁷ and the need to curb cheating during school examinations.²⁸ In December 2021, the Parliamentary Standing Committee on Communications and Information Technology noted that Internet Shutdowns were resorted to on the “*slightest pretext of maintaining law and order*” and recommended that:

- the Department of Telecommunications and Ministry of Home Affairs create uniform guidelines and standard operating procedures for Internet Shutdowns;
- maintain a central record of all Internet Shutdowns in the country that is available to the public;
- avoid the use of Section 144 of the CrPC and comply with guidelines issued by the Supreme Court of India when conducting Internet Shutdowns; and
- study the efficacy and proportionality of Internet Shutdowns to achieve the State’s intended aims.²⁹

24 *Anuradha Bhasin v Union of India* 2020 (3) SCC 637 [90]-[91]; Software Freedom Law Centre, ‘Legality of Internet Shutdowns under Section 144 CrPC’ (SFLC.in, 2 October 2016) <<https://sflc.in/legality-internet-shutdowns-under-section-144-crpc>> accessed 17 July 2021.

25 ‘Terrorists Inciting People via Fake News, J&K Tells SC; Opposes 4G Internet in UT’ *The Hindu* (New Delhi, 1 May 2020) <<https://www.thehindu.com/news/national/other-states/terrorists-inciting-people-via-fake-news-jk-tells-sc-opposes-4g-internet-in-ut/article31479428.ece>> accessed 26 September 2020.

26 ‘Indian State Cuts Internet after Lynchings over Online Rumours’ *The Guardian* (29 June 2018) <<https://www.theguardian.com/world/2018/jun/29/indian-state-cuts-internet-after-lynchings-over-online-rumours>> accessed 26 September 2020.

27 Trisha Jalan, ‘Indian Govt Uses Internet Shutdowns to Curb Anti-CAA Protests – in UP, Delhi, Assam, and 6 Other States’ *MediaNama* (2 January 2020) <<https://www.medianama.com/2020/01/223-indian-govt-internet-shutdowns-citizenship-protests/>> accessed 26 September 2020; Vijaita Singh, ‘Union Home Ministry Blocks Internet at Farmer Protest Sites on Delhi’s Border for Two Days’ *The Hindu* (New Delhi, 30 January 2021) <<https://www.thehindu.com/news/national/mha-blocks-internet-at-farm-protest-sites-on-delhis-border-for-2-days/article33702623.ece>> accessed 4 February 2021.

28 ‘Net Curb in 7 Districts for Madhyamik’ *The Telegraph Online* (17 February 2020) <<https://www.telegraphindia.com/west-bengal/net-curb-in-7-districts-for-madhyamik/cid/1746162>> accessed 26 September 2020.

29 Software Freedom Law Centre, ‘IT Standing Committee’s Report on Internet Shutdowns’ (n 21); Anushka Jain, ‘Summary: IT Standing Committee Report on Impact of Internet Shutdowns in India’ *MediaNama* (6 December 2021) <<https://www.medianama.com/2021/12/223-summary-internet-shutdown-report-it-committee/>> accessed 25 April 2022.

Legal challenges to Internet Shutdowns

Legal challenges to Internet Shutdowns have met with limited success. In August 2019, the Union Government imposed an Internet Shutdown in Kashmir as part of a broader lockdown following the revocation of Article 370 of the Indian Constitution.³⁰ In adjudicating the constitutionality of Internet Shutdowns in Kashmir, the Supreme Court of India in *Anuradha Bhasin vs. Union of India* recognised that expression on the internet, and the practice of any trade or business using the medium of the internet, are constitutionally protected under Article 19 of the Indian Constitution.³¹ Thus, internet access, as a necessary prerequisite for expression and trade on the internet, should also be protected under Article 19.

The Court ruled that access to the internet could not be restricted “indefinitely”.³² However, the Supreme Court did not rule that the Constitution imposed a positive obligation on the State to guarantee internet access.³³ Further, the Court did not order a restoration of internet services in Kashmir; instead it directed Indian authorities to publish all orders mandating the suspension of telecom and internet services (they were not previously published), and directed that these orders be reviewed by a committee of senior civil servants as prescribed by The Indian Telegraph Act, 1885 (‘Telegraph Act’).³⁴

In cases where Internet Shutdowns have been imposed for shorter durations, courts have refused to intervene on the ground that the internet will be restored shortly (or already has been restored) at the time of adjudication.³⁵ However, in December 2019 the Gauhati High Court did direct the restoration of the internet in ten districts in the State of Assam, as the State Government failed to produce any material demonstrating incidents of violence which would justify restrictions on the internet.³⁶ More recently, in March 2022 the Calcutta High Court stayed the application of an Internet Shutdown order that sought to restrict internet access during upcoming school examinations to prevent cheating.³⁷ The High Court noted that the government order had been passed under Section 144 of the CrPC instead of the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017 under the Telegraph Act, and State should have resorted to less restrictive measures to deal with the threat of cheating during examinations.³⁸

30 ‘Kashmir in Lockdown after Autonomy Scrapped’ *BBC News* (6 August 2019) <<https://www.bbc.com/news/world-asia-india-49246434>> accessed 10 September 2021. Article 370 granted Kashmir a measure of autonomy from India such as the power to have its own flag and make its own rules for residency and property.

31 2020 (3) SCC 637 [160].

32 *ibid* [108]. Subsequently, by Department of Telecommunications Notification G.S.R. 694(E) dated November 10, 2020, the Union Government amended the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 to state that an order suspending internet or telecom services shall not be in operation for more than fifteen days.

33 Devdutta Mukhopadhyay and Apar Gupta, ‘Jammu & Kashmir Internet Restrictions Cases: A Missed Opportunity to Redefine Fundamental Rights in the Digital Age’ 9 *Indian Journal of Constitutional Law* 207, 214.

34 *Anuradha Bhasin v Union of India* 2020 (3) SCC 637 [160].

35 *Software Freedom Law Centre India v State of West Bengal* 2020 SCC OnLine Cal 926; ‘HC Dismisses Plea Claiming Telecom Services Illegally Stopped during Protests in Delhi’ *The Hindu* (New Delhi, 24 December 2019) <<https://www.thehindu.com/news/cities/Delhi/hc-dismisses-plea-claiming-telecom-services-illegally-stopped-during-protests-in-delhi/article30388497.ece>> accessed 23 September 2020.

36 *Banashree Gogoi v Union of India* PIL 78 of 2019 (Gauhati High Court, 19 December 2019).

37 *Ashlesh Biradar v State of West Bengal* WPA (P) 104 of 2022 (Calcutta High Court, 10 March 2022).

38 *ibid*.

(ii) Banning of mobile applications

As stated earlier, apart from shutting down the Internet, the Union Government has also engaged in restricting access to specific websites or banning specific applications from time to time.³⁹ While the Union Government has routinely blocked specific Uniform Resource Locators ('URLs') since the early 2010s,⁴⁰ more recently the Government has blocked access to a number of mobile applications.⁴¹ In June 2020, the Union Government temporarily 'banned' fifty nine mobile applications including popular social media platforms such as TikTok, WeChat and Helo.⁴² The Government is said to have issued instructions to Google and Apple to remove the restricted mobile applications from their respective application stores.⁴³ The Government also directed ISPs to block traffic to these platforms on their networks.⁴⁴

39 Revathi Krishnan, 'Modi Govt Blocked 3,635 Websites & Webpages in 2019 – over Twice of 2017 Figures' *The Print* (17 September 2020) <<https://theprint.in/tech/modi-govt-blocked-3635-websites-webpages-in-2019-over-twice-of-2017-figures/504816/>> accessed 2 March 2021; 'Government Blocked 296 Mobile Apps since 2014, Says Union Minister Sanjay Dhotre' *The New Indian Express* (4 February 2021) <<https://www.newindianexpress.com/business/2021/feb/04/government-blocked-296-mobile-apps-since-2014-says-union-minister-sanjay-dhotre-2259598.html>> accessed 2 March 2021.

40 Software Freedom Law Centre, 'Access Denied: One Info-Graphic That Tells You Everything about Internet Censorship in India since 2012' *NewsLaundry* (9 December 2015) <<https://www.newslaundry.com/2015/12/09/access-denied-one-info-graphic-that-tells-you-everything-about-internet-censorship-in-india-since-2012>> accessed 10 September 2021.

41 "Government Blocked 296 Mobile Apps since 2014, Says Union Minister Sanjay Dhotre" (n 39).

42 Chinese Apps Banned in India: India Bans 59 Chinese Apps Including TikTok, WeChat, Helo' *The Economic Times* (29 July 2020) <<https://economictimes.indiatimes.com/tech/software/india-bans-59-chinese-apps-including-tiktok-helo-wechat/articleshow/76694814.cms>> accessed 26 September 2020.

43 Yuthika Bhargava, 'Government Bans 59 Apps Including China-Based TikTok, WeChat' *The Hindu* (New Delhi, 29 June 2020) <<https://www.thehindu.com/news/national/govt-bans-59-apps-including-tiktok-wechat/article31947445.ece>> accessed 26 September 2020.

44 *ibid.*

In September 2020, the Government added an additional 118 mobile applications to the its earlier list of fifty nine restricted applications.⁴⁵ A month later, the Government restricted the use of a further forty three mobile applications.⁴⁶ In January 2021, it was reported that the Government had sent fresh notices to the application developers of the restricted applications, informing them that the restrictions would be permanent.⁴⁷ More recently, in February 2022, the Government restricted an additional fifty four applications that were allegedly identical to previously restricted applications.⁴⁸

The Government invoked Section 69A of the IT Act as the basis for these restrictions on mobile applications.⁴⁹ Section 69A empowers the Union Government to block access to specified content where it is “*necessary*” to do so in the interests of public order, the defence, sovereignty, integrity, or security of India or its friendly relations with foreign States, or to prevent the incitement of an offence against the aforementioned interests.⁵⁰ In a press release, the Union Government invoked the language of Section 69A, stating that the mobile applications were engaged in activities ‘prejudicial to the sovereignty and integrity of India, the defence of India, the security of the State and public order.’⁵¹ The Government stated that it had received complaints that the applications had been “*stealing and surreptitiously transmitting*” user data to servers located outside India.⁵² Given that the mobile applications were primarily created by Chinese developers and the banning of the applications was contemporaneous with rising tensions between India and China over a border dispute, media reports suggested that banning the applications was a decision by the Indian Government to exert pressure on its Chinese counterpart.⁵³

45 ‘PUBG Mobile, 117 Chinese Apps Banned in India: Check the Full List’ *The Indian Express* (5 September 2020) <<https://indianexpress.com/article/technology/tech-news-technology/india-bans-pubg-mobile-116-chinese-apps-full-list-6580365/>> accessed 22 September 2020.

46 Press Information Bureau, ‘Government of India Blocks 43 Mobile Apps from Accessing by Users in India’ (24 November 2020) <www.pib.gov.in/Pressreleaseshare.aspx?PRID=1675335> accessed 20 April 2021.

47 Surajeet Das Gupta, ‘Govt to Impose a Permanent Ban on Some Chinese Apps Including TikTok’ *Business Standard India* (22 January 2021) <https://www.business-standard.com/article/companies/govt-to-impose-a-permanent-ban-on-some-chinese-apps-including-tiktok-121012201460_1.html> accessed 20 April 2021.

48 ‘Govt Bans 54 Chinese Apps over Security Threat Concerns’ *Hindustan Times* (14 February 2022) <<https://www.hindustantimes.com/india-news/govt-to-ban-54-chinese-apps-that-pose-threat-to-india-report-101644814634095.html>> accessed 26 April 2022.

49 Press Information Bureau (n 46).

50 The Information Technology Act, 2000 s. 69A.

51 ‘Chinese Apps Banned in India: India Bans 59 Chinese Apps Including TikTok, WeChat, Hello’ (n 42).

52 ‘India Bans PUBG, Baidu and More than 100 Apps Linked to China’ *BBC News* (2 September 2020) <<https://www.bbc.com/news/technology-53998205>> accessed 22 September 2020.

53 Sameer Yasir and Hari Kumar, ‘India Bans 118 Chinese Apps as Indian Soldier Is Killed on Disputed Border’ *The New York Times* (2 September 2020) <<https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html>> accessed 14 March 2021.

2.4. Social media, misinformation, and real-world violence

The widespread use of social media has resulted in a section of Indian internet users accessing and sharing information about matters of public concern online. A study of English-language internet users in India found that 52% of respondents received news from both Facebook and WhatsApp.⁵⁴ Other social media platforms that respondents relied on for news included Instagram (26%), Twitter (18%), and Facebook Messenger (16%).⁵⁵ As in many countries, the shift of public debate to online platforms, coupled with the decentralised and rapid nature of the internet, has led to the increased spread of disinformation and disputed claims to facts.⁵⁶ However, this phenomenon has also been made more complex by India's existing 'socio-cultural' tensions.⁵⁷ Microsoft's Digital Civility Index for 2021 ranked India eighteen out of the twenty two countries surveyed.⁵⁸

Misinformation on social media has led to real-world violence in India. According to a BBC analysis of English language news reports between 2014 and 2018, at least thirty one people have been killed in mob attacks allegedly fuelled by false rumours on social media (in particular, on WhatsApp).⁵⁹ In July 2018 the Indian Ministry for Electronics and Information Technology ('MEITY') issued a statement noting that while law enforcement officials continued to investigate and apprehend the culprits behind the physical violence, the Ministry had taken serious note of the "*abuse of platforms like WhatsApp for repeated circulation of such provocative content*".⁶⁰ In response to a motion in Parliament, the Minister of Electronics and Information Technology stated that the Union Government was committed to "*strengthen the legal framework and make the social media platforms accountable under the law.*"⁶¹

The Government has since cited three key considerations to justify this stronger framework: (i) the rapid growth of the online intermediary ecosystem and the ability of social media platforms to influence citizens; (ii) the need for a framework to deal with online messages that have resulted in real-world violence and crimes concerning the "*dignity of women and sexual abuse of children*"; and (iii) the investigative requirements of Indian law enforcement agencies.⁶²

These statements indicate that the Union Government believes that online intermediaries, and in particular large social media companies, should both: (i) take a more active role in monitoring

⁵⁴ Zeenab Aneez and others, 'Reuters Institute India Digital News Report' (Reuters Institute 2019) 9 <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-03/India_DNR_FINAL.pdf> accessed 26 September 2020.

⁵⁵ Aneez and others (n 54).

⁵⁶ See Ari Ezra Waldman, 'The Marketplace of Fake News' (2018) 20 University of Pennsylvania Journal of Constitutional Law 845; Soroush Vosoughi, Deb Roy and Sinan Aral, 'The Spread of True and False News Online' (2018) 359 Science 1146.

⁵⁷ Maya Mirchandani, 'Digital Hatred, Real Violence: Majoritarian Radicalisation and Social Media in India' [2018] Observer Research Foundation <https://www.orfonline.org/wp-content/uploads/2018/08/ORF_OccasionalPaper_167_DigitalHatred.pdf>; Maya Mirchandani, Ojasvi Goel and Dhananjay Sahai, 'Encouraging Counter-Speech by Mapping the Contours of Hate Speech on Facebook in India' (Observer Research Foundation 2018) <https://www.orfonline.org/wp-content/uploads/2018/03/ORF_Report_Counter_Speech.pdf>.

⁵⁸ 'Digital Civility Index 2021' (Microsoft) <<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWSvpX>> accessed 25 July 2022.

⁵⁹ Shadab Nazmi, Dhruv Nenwani and Gagan Narhe, 'Social Media Rumours in India: Counting the Dead' (BBC News) <<https://www.bbc.co.uk/news/resources/idt-e5043092-f7f0-42e9-9848-5274ac896e6d>> accessed 25 September 2020.

⁶⁰ Taylor Hatmaker, 'WhatsApp Now Marks Forwarded Messages to Curb the Spread of Deadly Misinformation' (TechCrunch) <<https://social.techcrunch.com/2018/07/10/whatsapp-forwarded-messages-india/>> accessed 25 September 2020.

⁶¹ Tariq Ahmad, 'Government Responses to Disinformation on Social Media Platforms: India' (September 2019) <<https://www.loc.gov/law/help/social-media-disinformation/india.php>> accessed 26 September 2020.

⁶² Ministry of Electronics and Information Technology, 'Frequently Asked Questions (FAQs) - The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' <https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf> accessed 3 November 2021.

and regulating content on their platforms; and (ii) be more accountable to Indian authorities and users for their decisions vis-à-vis content on their platforms. As the remainder of this report evidences, intermediary liability has emerged as a key tool to operationalise these goals.

3

Intermediaries in India

Section 2(1)(w) of the IT Act defines an “intermediary” as any person who, “*on behalf of another person receives, stores, or transmits (...) or provides any service with respect to*” an electronic record “*and 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;*”.⁶³ The IT Act’s definition thus includes both: (i) physical intermediaries that provide the network infrastructure and services necessary for internet access, typically TSPs and ISPs; and (ii) online intermediaries that provide platforms where “content is transacted” (e.g., Dropbox or Twitter).⁶⁴ Thus, the IT Act’s definition includes both entities that merely transport data and entities that actively host content that users interact with.⁶⁵

Using the words “*or provides any service with respect to*” in Section 2(1)(w), the IT Act recognises that an intermediary may provide additional services beyond merely acting as a neutral platform to store and transmit data.⁶⁶ For example, in a case concerning whether domain name registrars were intermediaries under the IT Act, the High Court of Delhi ruled that because domain names constituted electronic records (sourced from a domain name registry), and registrars provided services with respect to domain names, registrars were intermediaries under the Act.⁶⁷

63 The Information Technology Act, 2000 s. 2(1)(w) (s. 2(1)(t) defines “electronic record” as “data, record or data generated” and s. 2(1)(o) defines “data” as a “representation of information, knowledge, facts, concepts or instructions (...) intended to be processed, is being processed, or has been processed in a computer system or network”).

64 See Graeme Dinwoodie, ‘Who Are Internet Intermediaries?’ in Giancarlo Frosio (ed), Graeme Dinwoodie, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 47. Setting out a taxonomy of intermediaries generally.

65 Varun Sen Bahl, Faiza Rahman and Rishab Bailey, ‘Internet Intermediaries and Online Harms: Regulatory Responses in India’ (National Institute of Public Finance and Policy 2020) 11 <https://datagovernance.org/files/research/BahlRahmanBailey_-_Paper_6-2.pdf>.

66 See *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454 [144].

67 *Snapdeal Pvt Ltd v GoDaddy LLC CS* (Comm) 176 of 2021 (High Court of Delhi, 18 April 2022).

3.1. Defining network and online intermediaries

The regulatory regimes for physical network intermediaries (TSPs and ISPs) and online intermediaries diverge significantly. Physical or network intermediaries are required to obtain a license to operate in India.⁶⁸ The licenses issued by the Union Government impose several obligations on TSPs and ISPs, and failure to fulfil these contractual obligations can result in withdrawal of an intermediary's license to operate in India.⁶⁹ In contrast, online intermediaries do not need to obtain a license to operate in India, and are primarily regulated through the conditions they must satisfy to obtain legal immunity for unlawful third-party content on their platforms.⁷⁰ (Recent proposals to amend this regulatory distinction are discussed in section 3.2(iii) of this report.)

The distinction between physical network intermediaries and online intermediaries does not negate the fact that both categories represent a range of undertakings offering diverse functionality. This is further complicated by the fact that a single intermediary may perform functions that span across the physical/online intermediary divide. For example, an ISP may also operate an online payment site and an online marketplace hosting third-party content.⁷¹ The question of how closely regulation should mirror the empirical reality of intermediary functionality is debatable,⁷² though prior to imposing liability on an intermediary, courts should clearly understand how an entity's technology has been used in the commission of an unlawful act.⁷³

Only an “*intermediary*” under Section 2(1)(w) is entitled to the qualified legal immunity for unlawful third-party content, or ‘safe harbour’, provided by the IT Act.⁷⁴ Thus, the definition in Section 2(1)(w) implicitly contains some of the core conditions for availing this safe harbour; to be entitled to immunity, the entity seeking immunity must first be an “*intermediary*”. Crucially, the definition states that an intermediary receives, stores, or transmits content “*on behalf of another person*”, clarifying that intermediaries deal with third-party content and do not host their own content in the manner a web-publisher would. Infrastructural providers such as ISPs almost always fall under the definition. However, the situation may be more complicated in the case of online intermediaries.

One method for courts to determine whether an entity is an “*intermediary*” is to examine whether the entity transmits, stores, or provides any service with respect to the third-party content

⁶⁸ The Indian Telegraph Act, 1885 s. 4; Chinmayi Arun and Sarvjeet Singh, ‘NoC Online Intermediaries Case Studies Series: Online Intermediaries in India’ (National Law University Delhi 2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566952>.

⁶⁹ The Indian Telegraph Act, 1885 s. 8.

⁷⁰ The Information Technology Act, 2000 s. 79 read with Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) dated 25 February 2021, Part II.

⁷¹ See ‘JioMart Integration Allows MyJio App Users to Order Groceries’ *NDTV Gadgets 360* (22 September 2020) <<https://gadgets360.com/apps/news/jio-mart-myjio-order-groceries-directly-within-app-reliance-2299355>> accessed 26 April 2022.

⁷² Dinwoodie (n 64) 48.

⁷³ Jaani Riordan, ‘A Taxonomy of Internet Intermediaries’ in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 36.

⁷⁴ The Information Technology Act, 2000 s. 79(1) (stating that an “intermediary shall not be liable for any third party information”).

from which the alleged liability originates.⁷⁵ In other words, the question of whether an entity is transmitting or storing third party content should be assessed in relation to the content the intermediary is being sued for. This approach is supported by the language Section 2(1)(w) which expressly defines an intermediary “with respect to any particular electronic records”. Thus, it is better to think of an “intermediary” as a categorisation applicable to an entity when it performs a specific function, rather than a categorisation applicable across all an entity’s functions.⁷⁶ For example, one may classify an entity as a ‘borrower’ only in relation to a loan it has taken but classify the entity as a ‘company’ or ‘partnership’ across all its functions. Similarly, a website may be an “intermediary” when it transmits ‘Picture A’ that is third-party content shared by a user, but not an “intermediary” when it transmits ‘Picture B’ that is its own content. As any liability imposed on an intermediary will fundamentally be tied to the unlawfulness of the underlying content, it makes sense to examine the entity’s intermediary status in relation to the allegedly unlawful content. Thus, if the same entity was sued for ‘Picture A’, it would be an “intermediary” eligible for safe harbour but if it was sued for ‘Picture B’, it would not be an “intermediary”. Thus, rather than courts asking whether an entity is an intermediary, the more appropriate judicial inquiry may be, is this entity an intermediary *with respect to* the allegedly unlawful content it is being sued for.

Courts have not always adopted this approach. Where no dispute exists between the parties about whether the entity’s functionality falls within Section 2(1)(w), courts have often not scrutinized whether a specific entity falls within the definition of an intermediary under the IT Act.⁷⁷ For example, when dealing with websites hosting third-party content, the High Court of Delhi repeatedly began its analysis with the assumption that the website was an intermediary,⁷⁸ or noted that the platform “facially falls within Section 2(1)(w) and qualifies as an intermediary”.⁷⁹

75 Divij Joshi, ‘Is the Clock Ticking for TikTok’s Intermediary Liability Exemptions?’ (*SpicyIP*, 2 September 2019) <<https://spicyip.com/2019/09/is-the-clock-ticking-for-tiktoks-intermediary-liability-exemptions.html>> accessed 27 October 2022.

76 *ibid.*

77 See *Nirmaljit Singh Narula v Indijobs at Hubpages.Com* 2012 SCC OnLine Del 1946; *Vyakti Vikas Kendra, India Public Charitable Trust v Jitender Bagga* 2012 SCC OnLine Del 2710; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382.

78 *Nirmaljit Singh Narula v Indijobs at Hubpages.Com* 2012 SCC OnLine Del 1946 [23]; *Vyakti Vikas Kendra, India Public Charitable Trust v Jitender Bagga* 2012 SCC OnLine Del 2710 [11].

79 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [45]. See also *Flipkart Internet Pvt Ltd v State of NCT of Delhi* Writ Petition (Cri) 1376 of 2020 (High Court of Delhi, 17 August 2022).

However, where parties disagreed over whether the functionality offered by an entity was covered under Section 2(1)(w), courts have often ruled that the question of whether an entity is an intermediary should be answered at trial (as opposed to an interim or preliminary stage).⁸⁰ For example, where a party alleged that Amazon was acting beyond the scope of an “intermediary” through its active involvement in selling products, the High Court of Delhi held that, “Given the disputed questions of facts that emerge from the pleadings in the suit, it is obvious that the issue of whether an entity is an intermediary or not can be decided only after a trial.”⁸¹ As none of the trials where the functionality of an intermediary was disputed have been completed, the exact evidentiary burdens required for an entity to satisfy the definition of ‘intermediary’ remain unclear. However, as noted above, the determination of whether an entity is an intermediary is likely better made based on the entity’s relationship with the allegedly unlawful content.

80 See *Google India Pvt Ltd v Visaka Industries* 2020 (4) SCC 162 [153]; *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454 [141]; *Sorting Hat Technologies Pvt Ltd v Fermat Education* 2019 SCC OnLine Mad 33436 [20].

81 *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454 [18]-[19], [141].

3.2. Licensing system for ISPs

Under the Telegraph Act, TSPs and ISPs are required to obtain a license to operate in India.⁸² The Department of Telecommunications is the Union Government authority that provides operators the right to provide telecommunications and internet services to end-users by issuing an “Unified License Agreement”. The Unified License Agreement requires ISPs to satisfy numerous operating and security conditions, the breach of which will constitute grounds for the termination of the license.⁸³ The duration of a Unified License Agreement is typically twenty years.⁸⁴ However, the Union Government retains the right to suspend,⁸⁵ revoke,⁸⁶ or modify the terms of the license⁸⁷ in the interest of the public or the security of the State.

(i) Infrastructure for interception and monitoring

Section 5(2) of the Telegraph Act empowers both the Union and State Governments to restrict or intercept communications in the event of a public emergency or in the interests of public safety.⁸⁸ Where such circumstances exist, the Union or a State Government may block or intercept the communications to any person or class of people, on any subject, if it believes it is expedient to do so in the interests of: “*the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement for the commission of an offence*”.⁸⁹ To operationalise these powers, the Unified License Agreement obligates all licensees (TSPs and ISPs) to install and maintain monitoring and interception facilities,⁹⁰ provide the traceable identity of their subscribers,⁹¹ provide the geographical location of their subscribers at a given point in time,⁹² and prevent their networks for being used for “*anti-national activities*”.⁹³ Licensees are not permitted to employ bulk encryption equipment on their networks, but must ensure the privacy of communications on their network.⁹⁴

In the case of ISPs, the Unified License Agreement mandates that they block internet sites, URLs, Uniform Resource Identifiers (‘URIs’), or individual internet subscribers when directed by the Union Government in “*the interest of national security or public interest.*”⁹⁵ ISPs are also required to install and maintain interception and monitoring equipment at their internet gateways or nodes⁹⁶ and make available copies of all packets originating

⁸² The Indian Telegraph Act, 1885 s. 4

⁸³ Department of Telecommunications, “License Agreement for Unified License (Version Dated 29.03.2016)”, https://dot.gov.in/sites/default/files/2016_03_30%20UL-AS-I.pdf?download=1 [Unified License Agreement] Unified License Agreement, ch I, Condition 10.2.

⁸⁴ Unified License Agreement, recitals.

⁸⁵ Unified License Agreement, ch I, Condition 10.1.

⁸⁶ Unified License Agreement, ch. 1, Condition 10.4.

⁸⁷ Unified License Agreement, ch 1, Condition 5.1.

⁸⁸ The Indian Telegraph Act, 1885 s. 5(2).

⁸⁹ *ibid.*

⁹⁰ Unified License Agreement, ch IV, Condition 23.2, Ch. VI, Condition 39.12.

⁹¹ Unified License Agreement, ch VI, Condition 39.23 (ix).

⁹² Unified License Agreement, ch VI, Condition 39.23 (x).

⁹³ Unified License Agreement, ch VI, Condition 39.14.

⁹⁴ Unified License Agreement, ch VI, Condition 37.1.

⁹⁵ Unified License Agreement ch IX, Condition 7.12.

⁹⁶ Unified License Agreement ch IX, Condition 8.1.1.

from or terminating at customer equipment when required.⁹⁷

97 Unified License Agreement ch. IX, Condition 7.3.

(ii) Impact of licensing regime

The provisions of the Telegraph Act coupled with the conditions in the Unified License Agreement create the techno-legal infrastructure necessary for the Indian Government to monitor individual communications and if necessary, restrict access to the internet. The use of broad terms such as ‘national security’ or ‘public interest’ creates a low bar of justification to initiate surveillance. Surveillance is also increasingly centralised. The Unified License Agreement allows for the government to monitor networks from a central location⁹⁸ and in 2016 the Union Government confirmed that the ‘Central Monitoring System’ was operational in India’s two largest cities.⁹⁹ The system is intended to centralise and automate interception and monitoring in the hands of the Union Government by eliminating TSPs from the interception process.¹⁰⁰

98 Unified License Agreement ch. IX, Condition 8.4.

99 Sneha Johari, ‘Govt’s Central Monitoring System Already Live in Delhi & Mumbai’ *MediaNama* (11 May 2016) <<https://www.medianama.com/2016/05/223-india-central-monitoring-system-live-in-delhi-mumbai/>> accessed 20 October 2020.

100 Maria Xynou, ‘India’s Central Monitoring System (CMS): Something to Worry About?’ (*The Centre for Internet and Society*, 30 January 2014) <<https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about>> accessed 10 February 2021.

The centrality of the licenses to the business models of TSPs and ISPs allows the government and courts to ensure TSPs and ISPs comply with their directions to monitor, restrict, or block content, at the risk of losing their licenses.¹⁰¹ For example, on July 31, 2015 the (then) Ministry of Communications & Information Technology’s Department of Technology issued a notification directing the blocking of several URLs containing pornographic material.¹⁰² In a 2018 judicial proceeding concerning the rise of sexual assaults against minors, the High Court of Uttarakhand noted that ISPs had failed to implement the government’s 2015 notification.¹⁰³ The High Court directed the websites be blocked immediately and directed the government to suspend the licenses of the ISPs if they failed to comply with the directions.¹⁰⁴ While aspecific legal power to block content is found in the IT Act and judicial orders, the licensing regime created by the Telegraph Act creates powerful incentives for ISPs to comply with the directions of State authorities.

101 See *In Re “In the matter of, Incidence of Gang Rape in a Boarding School situated in Bhauwala” v State of Uttarakhand* (2018) SCC OnLine Utt 871; *Dept of Electronics and Information Technology v Star India Pvt Ltd* FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016).

102 Software Freedom Law Centre, *DOT orders blockage of porn websites*, SFLC.in, <https://sflc.in/dot-orders-blockage-porn-websites>.

103 *In Re “In the matter of, Incidence of Gang Rape in a Boarding School situated in Bhauwala” v State of Uttarakhand* (2018) SCC OnLine Utt 871 [20].

104 *ibid* [21].

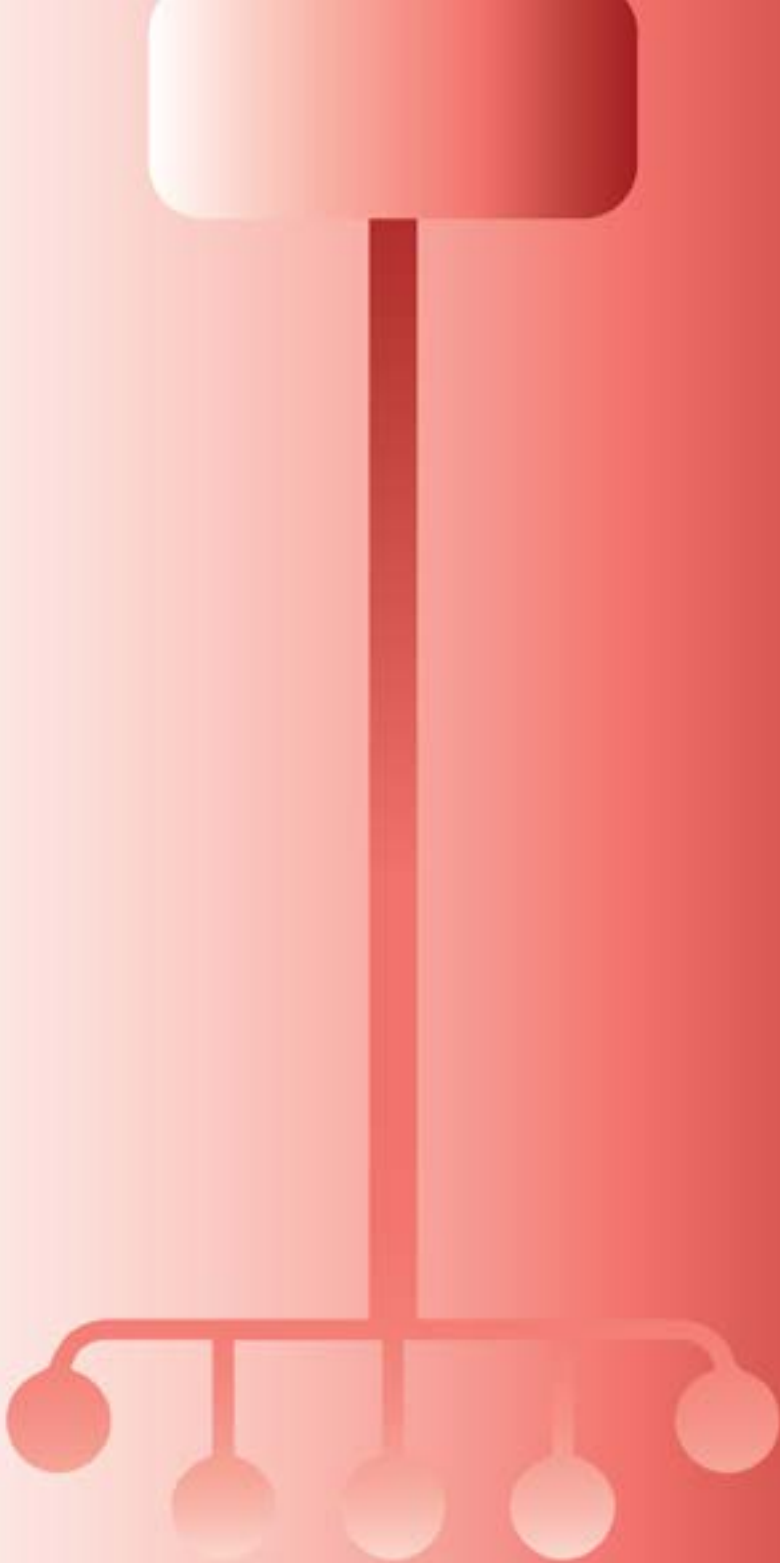
(iii) Proposals to bring online intermediaries under licensing regime.

In September 2022, the Indian Government released a draft ‘Indian Telecommunications Bill’.¹⁰⁵ Section 3(2) of the Bill would require entities providing “*telecommunication services*” in India to obtain a license from the Union Government. The Bill defines the term “*telecommunication services*” very broadly to include ‘electronic mail, video and data communication services, internet and broadband services, internet-based communication services, interpersonal communication services, and over-the-top communication services made available to users by telecommunication’.¹⁰⁶

This proposed regulatory regime could potentially result in online intermediaries, such as e-mail, social media services, and e-commerce services being required to obtain a license from the Union Government to operate in India. As seen in the case of TSPs and ISPs, making the operation of intermediaries in India contingent on a license from the Union Government provides intermediaries with powerful incentives to comply with government regulation, which may extend to the regulation of content. However, at the time of writing this report, the proposed legislation is still at the draft stage and the Indian Government is consulting various stakeholders. Further, Section 3(3) of the Telecommunications Bill itself allows the Union Government to exempt entities from requiring a license.

105 ‘Draft Indian Telecommunications Bill’ (Department of Telecommunications 2022) <<https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf>>.

106 *ibid* 6–7.



4

Safe Harbour Under the Information Technology Act

The functionality provided by online intermediaries may lead to them enabling the spread of unlawful content by primary wrongdoers (i.e., “*originators*”) despite intermediaries themselves not engaging in any wrongdoing.¹⁰⁷ When originators upload or transmit unlawful content using intermediaries’ networks, intermediaries have been described as “*necessary but insufficient causes*” of online harms.¹⁰⁸ Thus, intermediaries may be held secondarily liable for content on their networks. Intermediaries thus incur a substantial risk of secondary liability for the unlawful content on their networks, given the large volume of users and content interacting on their networks. To ensure that intermediaries can operate despite this potential risk, they are granted ‘safe harbour’.

Section 79 of the IT Act offers intermediaries qualified immunity from liability for hosting or making available third-party content. The text of the provision is fundamentally “*liability exempting*” and not “*liability imposing*”, i.e., the provision determines when intermediaries are not liable and does not itself impose liability for any specific act or omission.¹⁰⁹ Section 79 has been described as an “*affirmative defence*”¹¹⁰ to be invoked by intermediaries where secondary liability is sought to be imposed on them for making available unlawful content uploaded by their users. The defence of safe harbour bars claims for monetary damages and criminal liability against intermediaries¹¹¹ but does not restrict the imposition of non-monetary liability in the form of injunctions.¹¹²

Where intermediaries fail to successfully invoke the defence, intermediaries may incur civil and criminal liability for content on their networks under a wide range of offences that may be applicable to the content in question, such as: hate speech,¹¹³ defamation,¹¹⁴ obscenity,¹¹⁵ prohibitions on child sex abuse material,¹¹⁶ sedition,¹¹⁷ trademark infringement,¹¹⁸ or copyright infringement.¹¹⁹ However, even in the absence of a safe harbour defence, an intermediary’s liability would be subject to a determination of: (i) the illegality of the content made available by the intermediary; and (ii) the secondary liability of the intermediary in hosting or making available the illegal content.

Section 81 of the IT Act states that the provisions of the IT Act (including the safe harbour under Section 79) override any inconsistent provisions in other statutes except the Copyright Act and the Patents Act, 1970 (‘**Patents Act**’).¹²⁰

107 Jaani Riordan, ‘Principles of Secondary Liability’ in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 113.

108 Riordan, ‘A Taxonomy of Internet Intermediaries’ (n 73) 27.

109 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121] (“It must first be appreciated that Section 79 is an exemption provision”); Kyung-Sin Park, ‘From Liability Trap to the World’s Safest Harbour: Lessons from China, India, Japan, South Korea, Indonesia, and Malaysia’ in Giancarlo Frosio (ed), Kyung-Sin Park, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 255.

110 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [51].

111 *Flipkart Internet Pvt Ltd v State of NCT of Delhi* Writ Petition (Cri) 1376 of 2020 (High Court of Delhi, 17 August 2022) [26].

112 Jaani Riordan, ‘Safe Harbours’ in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 379–380. The Supreme Court of India in *Shreya Singhal v Union of India* 2015 (5) SCC 1 required intermediaries to comply with court orders to remove content.

113 The Indian Penal Code, 1860 ss. 153A, 295A, 298, and 505; The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989 ss. 3(1)(r), 3(1)(s).

114 The Indian Penal Code, 1860 s. 499.

115 The Indian Penal Code, 1860 s. 292; The Information Technology Act, 2000 s. 67.

116 The Information Technology Act, 2000 s. 67B.

117 The Indian Penal Code, 1860 s. 124A.

118 The Trade Marks Act, 1999 s. 102.

119 The Copyright Act, 1957 s. 51.

120 The Information Technology Act, 2000 s. 81. For an analysis of Section 81 and the implications of the proviso, refer to Section 5.2(i) of this report.

Therefore, the qualified immunity offered by Section 79 has a horizontal effect across different areas of law. Additionally, the High Court of Delhi has clarified that Section 81 does not prevent intermediaries from seeking safe harbour under the IT Act even in copyright infringement disputes.¹²¹ The High Court held that as Section 79 offered only a conditional immunity to intermediaries, it did not extinguish the rights of copyright owners.¹²² According to the Court, this meant there was no ‘inconsistency’ between the Copyright Act and the IT Act, and thus Section 81 of the IT Act did not exclude the operation of Section 79 in copyright disputes.¹²³ The intersection of the IT Act and the Copyright Act, along with the High Court’s decision are analysed in section 5.2 of this report.

121 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [66]. For an analysis of the High Court’s reasoning, refer to Section 5.2 of this report.

122 *ibid* [51]-[52]. For an analysis of the High Court’s reasoning, refer to Section 5.2 of this report.

123 *ibid* [51]-[52], [66]. For an analysis of the High Court’s reasoning, refer to Section 5.2 of this report.

India’s safe harbour regime under the IT Act has changed substantially since it was first adopted in the year 2000. This section of the report documents the evolution of the immunity under Section 79 and its cognate regulations in four stages:

- The adoption of the IT Act in 2000, its amendment in 2009, and the Intermediary Guidelines 2011;
- the decision of the Supreme Court of India in *Shreya Singhal vs. Union of India* in 2015 and its aftermath;
- the adoption of the Intermediary Guidelines 2021; and
- the legal challenges to the Intermediary Guidelines 2021 and October 2022 amendments to the Intermediary Guidelines by way of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022.

4.1. The Information Technology Act and Intermediary Guidelines 2011

The IT Act was enacted on June 9, 2000 and sought to provide legal recognition for electronic commerce, facilitate the electronic filings of documents with government agencies, and promote the efficient delivery of government services by maintaining reliable electronic records.¹²⁴ Although the original Act included a safe harbour provision, a substantial amendment to the IT Act in 2009 expanded both, the range of intermediaries that could claim immunity, as well as the nature of the immunity itself.¹²⁵

Prior to the 2009 amendment, Section 79 of the IT Act extended safe harbour only to “network service providers”.¹²⁶ This raised concerns that online intermediaries would not be entitled to the immunity offered by the Act. However, the amendment in 2009 extended the immunity offered by Section 79 to ‘intermediaries’ under the IT Act,¹²⁷ thus firmly including online intermediaries. Further, as originally enacted, intermediaries were only offered safe harbour from offences ‘under the IT Act’.¹²⁸ (The IT Act itself sets out certain offences related to online content.¹²⁹) This was significant as, prior to 2009, courts refused to grant safe harbour to intermediaries for liability originating outside the IT Act, most notably the Indian Penal Code – expressly holding that immunity under Section 79 only extended to offences under the IT Act itself.¹³⁰ But after 2009, this immunity has been extended to offences “contained in any law for the time being in force”.¹³¹

(i) Conditions for safe harbour under Section 79

The three sub-sections of Section 79 grant intermediaries qualified, or conditional, immunity for hosting or making available illegal third-party content. Section 79(1) grants immunity to intermediaries for third-party content. Sections 79(2) and (3) provide a set of conditions that an intermediary must fulfil to avail of the immunity. Section 79(2) requires that intermediaries either (i) merely provide access to a network over which content is transmitted; or (ii) if they do store content, that they do not interfere with the content by selecting or modifying the content in any way.¹³² They must also act with ‘due diligence’ (a standard elaborated on in subsidiary government regulation).¹³³ Section 79(3) requires that intermediaries (i) do not aid or abet the commission of an illegal act,¹³⁴ and (ii) take down content

124 The Information Technology Act, 2000 Preamble.

125 See The Information Technology (Amendment) Act 2008 s. 40. The Act was passed by Parliament in December 2008 and received the assent of the President on 5 February 2009. See also Expert Committee, ‘Report of the Expert Committee on Proposed Amendments to Information Technology Act 2000’, (Department of Information Technology, Ministry of Communications & Information Technology) https://www.meity.gov.in/writereaddata/files/ITAct_0.doc accessed 14 October 2021 (documenting revisions to s. 79).

126 The Information Technology Act, 2000 s. 79 (prior to amendment in 2008).

127 The Information Technology Act, 2000 s. 79 (as amended by The Information Technology (Amendment) Act, 2008).

128 The Information Technology Act, 2000 s. 79(1) (prior to its amendment by The Information Technology (Amendment) Act), 2008.

129 The Information Technology Act, 2000 ss. 66E (Punishment for violation of privacy), 67 (Punishment for publishing or transmitting obscene material in electronic form), 67A (Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form), 67B (Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form).

130 See *Sanjay Kumar Kedia v Narcotics Control Bureau* 2008 (2) SCC 294; *Google India Pvt Ltd v Visaka Industries Ltd* 2011 SCC OnLine Ap 1056.

131 The Information Technology Act, 2000 s. 79(1). The proviso to s. 81 of the IT Act states that provisions of the Act will not override any inconsistent provisions contained in The Copyright Act, 1957 and The Patent Act, 1970. The applicability of s. 79(1) is limited to this extent.

132 The Information Technology Act, 2000 ss. 79(2)(a), 79(2)(b).

133 *ibid* s. 79(2)(c).

134 *ibid* s. 79(3)(a)

expeditiously when they have “actual knowledge” of unlawful content on their networks.¹³⁵

135 *ibid* s. 79(3)(b)

As the text of Sections 79(2) and 79(3) is central to understanding the debates surrounding safe harbour in India, a detailed description of the conditions under the two sub-Sections are set out below. If an intermediary seeks to claim safe harbour, it must satisfy the following conditions:

(1) **Section 79(2)(a):** The intermediary’s function should be limited to providing access to a communication system over which third-party content is transmitted, temporarily stored, or hosted;

OR

Section 79(2)(b): The intermediary should not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission;

AND

(2) **Section 79(2)(c):** The intermediary should observe due diligence in discharging their duties under the IT Act including observing guidelines promulgated by the government.

AND

(3) **Section 79(3)(a):** The intermediary should not have conspired, abetted, aided, or induced by threat, promise, or otherwise the commission of an unlawful act;

AND

(4) **Section 79(3)(b):** Upon receiving actual knowledge or being notified by the government or its agencies that the intermediary is being used to commit an unlawful act, the intermediary should expeditiously remove or disable access to the material in question.

A Single Judge of the High Court of Delhi ruled that the requirements of Sections 79(2) should be read “disjunctively”, suggesting that intermediaries must satisfy both Sections 79(2)(a) and 79(2)(b).¹³⁶ However, this approach contradicts the text of the statutory provision, which clearly separates Sections 79(2)(a) and 79(2)(b) with the term “or”. Intermediaries can thus satisfy either Section 79(2)(a) or 79(2)(b) and continue to avail of safe harbour, provided they also satisfy Sections 79(2)(c) and 79(3).

136 *Snapdeal Pvt Ltd v GoDaddy LLC* CS (Comm) 176 of 2021 (High Court of Delhi, 18 April 2022) [81]-[84].

Sections 79(2)(c) and 79(3)(b) impose the additional obligations of “due diligence” and expeditiously taking down content upon obtaining “actual knowledge” of its illegal character. The content of these obligations was outlined in the Intermediary Guidelines 2011. In February 2021, these guidelines were replaced by the Intermediary Guidelines 2021. Section 79(3)(a) imposes one further requirement to secure immunity, that an intermediary must not have conspired or abetted an unlawful act.

(ii) ‘Neutrality’ under Sections 79(2)(a) and (b)

Sections 79(2)(a) and 79(2)(b) sets up the well-worn distinction, originally found in the European E-Commerce Directive, between intermediaries acting as “neutral and transient conduits” (such as ISPs) and those who host content, albeit without any knowledge or interference with the content.¹³⁷ Under Section 79(2)(a), intermediaries that solely provide access to the internet may avail of safe harbour. Section 79(2)(b) permits other types of intermediaries to also avail of immunity provided that the intermediary does not initiate a transmission, select the receiver, or modify the content of the transmission.

137 Dinwoodie (n 64) 42–43. Referring to the distinction in the European E-Commerce Directive.

This approach is in line with the European requirement that the conduct of intermediaries be ‘technical, automatic, and neutral’ to avail of safe harbour.¹³⁸ Functions that would clearly fall under Section 79(2)(a) include telecommunications carriers, ISPs, and other infrastructural services.¹³⁹ Where an intermediary hosts content, it should fall under Section 79(2)(b); however, if it provides additional functionality that may be construed as modifying the content, an assessment of the intermediary’s operations is necessary to determine whether it satisfies the requirements of non-interference with content. However, this notion of intermediaries as neutral entities with no control over

138 *ibid* 43. Referring to the European Court of Justice decisions in C-236-238/08 *Google France SARL v Louis Vuitton Malletier* [2010] 159 and C-324/09 *L’Oreal SA v eBay Int’l AG* [2011] 474.

139 Rajendra Kumar and Latha R Nair, ‘Information Technology Act, 2000 and the Copyright Act, 1957: Searching for the Safest Harbor?’ [2012] NUJS Law Review 555, 562.

content does not reflect the operations of modern-day online entities. Most recent legislation across the world has differentiated between various types of intermediaries based on the type of functionality the intermediary offers and the risk of online harms to users.¹⁴⁰

A plain reading of Section 79(2) would indicate that wielding editorial control would exclude an online intermediary from safe harbour.¹⁴¹ Editorial control would amount to selection of information, causing the intermediary to violate the condition of non-interference set out by the provision.¹⁴² Section 79 is modelled on the European E-Commerce Directive, and the requirement of not selecting or interfering with content in Section 79(2)(b) can be traced to Article 12 of the European Directive ('Mere conduit').¹⁴³ However, Article 14 of the same Directive ('Hosting') goes on to state that even when intermediaries are not mere conduits, they remain entitled to safe harbour provided they remove content upon receiving actual knowledge.

Section 79 does not contain a parallel to Article 14 of the European E-Commerce Directive. The text of Section 79 thus appears to limit the availability of safe harbour to network intermediaries and mere conduits; requiring even application layer intermediaries to both be mere conduits and remove content upon receiving actual knowledge. This is not to say that Section 79 is not applicable to hosting providers. As documented in the body of this report, Section 79 has regularly been interpreted as applicable to hosting providers. This has prompted commentators to view the lack of express protection for hosting providers as an oversight, with Arun and Singh noting, "*There is no reason why service providers who offer hosting services and do not fall afoul of the preconditions to the safe harbour protection should not qualify for immunity under Section 79.*"¹⁴⁴ However, the text of Section 79(2)(b) proscribes any interference in content. (A limited exemption for content moderation under the Intermediary Guidelines 2021 is discussed below.)

140 Bahl, Rahman and Bailey (n 65) 13.

141 Arun and Singh (n 68) 11.

142 *ibid.* citing Aditya Gupta, 'The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws – The Road Ahead' (2010) 15 *Journal of Intellectual Property Rights* 35, 37.

143 Directive 2000/31/EC of 8 June 2000 on electronic commerce, art. 12 exempts service providers from liability on the condition that they do not: (a) initiate the transmission; (b) select the receiver of the transmission; and (c) select or modify the information contained in the transmission.

144 Arun and Singh (n 68) 11.

One way to contend that hosting providers whose functionality exceeds that of a mere conduit under Section 79(2)(b) are also eligible for safe harbour is to suggest that each sub-section of Section 79(2) be read disjunctively. On this reading, an intermediary would be eligible for safe harbour if: (i) it provided access to a communication system; OR (ii) it was a mere conduit; OR (iii) it observed due diligence. Thus, an intermediary could provide services beyond that of a mere conduit under Section 79(2)(b), but still be eligible for safe harbour provided it complied with Section 79(2)(c) (due diligence). While Sections 79(2) (a) (network access) and 79(2)(b) (mere conduit) are clearly separated by the word “or”, the text of Section 79 uses neither ‘or’ nor ‘and’ between Sections 79(2)(b) (mere conduit) and 79(2) (c) (due diligence), creating some ambiguity. However, under this reading, the due diligence obligations of Section 79(2)(c) would not apply to network intermediaries and mere conduits. This has caused the commentators to converge on the interpretation that safe harbour is limited to access providers and mere conduits, and the requirement for due diligence is applicable to both types of intermediaries; to avail of safe harbour, intermediaries must comply with Sections 79(2)(a) (network access) OR 79(2)(b) (mere conduit) AND Section 79(2)(c) (due diligence).¹⁴⁵

145 *ibid.*

The question of the neutrality required under Sections 79(2)(a) and 79(2)(b) is also particularly relevant from the perspective of content moderation. Several modern-day online intermediaries voluntarily remove content to improve the users’ experience; functionality that may be viewed as exceeding that of a mere conduit. The ambiguity with respect to content moderation has largely been remedied by the Intermediary Guidelines 2021. Rule 3(1)(d) of the new Guidelines expressly permits intermediaries to take down certain broad categories of ‘prohibited content’¹⁴⁶ “on a voluntary basis”.¹⁴⁷ The Rule states that such voluntary removal of ‘prohibited’ content would not amount to a violation of the non-interference requirements of Sections 79(2)(a) or (b) of the IT Act.¹⁴⁸ However, ambiguity continues to exist with respect to intermediaries that engage in ranking (algorithmic or manual) of content.

146 See Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 G.S.R. 139(E) dated 25 February 2021 [Intermediary Guidelines 2021] r. 3(1) (b) (undesirable content includes content that is defamatory, obscene, pornographic, insulting, harassing, infringes intellectual property, impersonates another person, threatens public order or the defence or security of India, is deceptive or patently false).

147 Intermediary Guidelines 2021 r. 3(1) (d) (third proviso).

148 Intermediary Guidelines 2021 r. 3(1) (d) (third proviso).

Limits on delegated legislation

Rule 3(1)(d) of the Intermediary Guidelines 2021 expressly recognises that the content moderation activities of online intermediaries will not lead to a violation of the neutrality required under Section 79(2)(b). Irrespective of the question around the desirability of permitting intermediaries to voluntarily remove unlawful content, it remains unclear whether the prohibition on editorial control found in Section 79(2)(b) can be modified through delegated legislation that is the Intermediary Guidelines 2021. A delegated legislation may be invalid if it contravenes the parent legislation¹⁴⁹ or if its contents exceed the rulemaking power conferred by the parent legislation.¹⁵⁰ In the past, courts have ruled that executive authorities cannot change ‘essential features’ of existing laws through subordinate legislation.¹⁵¹ What constitutes an ‘essential feature’ remains contested and contextual, but courts have held that questions of ‘policy and binding rules of conduct’ must be determined first by Parliament through primary legislation.¹⁵²

Rule 3(1)(d) effectively exempts intermediaries in certain situations from the prohibition on selecting or modifying content set out in Section 79(2)(b) of the IT Act. However, the power conferred by Parliament to make delegated legislation with respect to Section 79 is limited to “the guidelines to be observed by the intermediaries under sub-section (2) of Section 79”.¹⁵³ In this context, it could be argued that the rule-making power of the executive is limited to setting out the “due diligence” obligations to be followed by an intermediary under Section 79(2)(c) (the only sub-section to use the term “guidelines”). Thus, the rule-making power pertains to Section 79(2)(c) and does not extend to creating what effectively amounts to an exemption to Section 79(2)(b). If this were the case, Rule 3(1)(d) would be void, and a legislative amendment to Section 79(2)(b) of the IT Act would be required to allow intermediaries that voluntarily remove unlawful content to retain safe harbour in certain situations.

149 *Indian Express (Bombay) Pvt Ltd v Union of India* 1985 (1) SCC 641 [75].

150 *Mahachandra Prasad Singh v Bihar Legislative Council* 2004 (8) SCC 747 [13].

151 *Rajnarain Singh v Chairman, Patna Administration Committee* 1955 (1) SCR 290 [30].

152 *Municipal Corporation of Delhi v Birla Cotton Spg and Wvg Mills* 1968 (3) SCR 251 [13].

153 The Information Technology Act, 2000 s. 87(2)(zg).

The above argument is admittedly formalistic. The true nature of the change is that while the legislative text of Section 79(2)(b) granted safe harbour only to entities that were neutral towards content (not modifying the content or choosing receivers), with the advent of Rule 3(1)(d) even entities that curate content through content moderation are now expressly eligible for safe harbour. Ultimately, this issue shines a light on how the changing role of intermediaries, and the rise of social media platforms and content moderation, are at odds with the character of intermediaries envisaged by Parliament when adopting the IT Act. Reading Section 79 as only granting the equivalent of mere conduits safe harbour would both disincentivise voluntary content moderation and likely disentitle many intermediaries from safe harbour. While the form of the clarification (through delegated legislation) may be less than ideal, the substance of Rule 3(1)(d) provides valuable clarity.

Judicial Decisions on neutrality

Expressly permitting intermediaries to take down certain categories of ‘prohibited content’ voluntarily is a new development. Thus, it remains unclear how courts will reconcile the new permissiveness of voluntary takedowns found in the Intermediary Guidelines 2021 with the text of Section 79(2) of the IT Act. However, prior to the adoption of the Intermediary Guidelines 2021, courts have ruled on whether the conduct of intermediaries falls within the non-interference requirements of Sections 79(2)(a) and (b).

The High Court of Delhi issued two preliminary rulings (subject to evidence being led at trial) on the question of what qualifies as an intermediary initiating a transmission or selecting the receiver of content. In the first case concerning Myspace, the High Court held that the existence of a ‘share’ button on an online intermediary’s platform would not amount to the intermediary initiating a transmission or selecting a receiver, as the decision to click the button and share content rested with the end-user.¹⁵⁴ In the second case concerning Amazon, it held that in the case of e-commerce platforms, it was the customer who initiated the transmission and the e-commerce platforms did not modify the information contained in the transmission (e.g. choice of product and number of units) when they transmitted this information to sellers.¹⁵⁵

154 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [64].

155 *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454 [139]-[144].

In the Myspace case, the High Court of Delhi also found that an automated editorial system which inserted advertisements into infringing content amounted to modifying the “format” and not the “content” of the transmission, and that its automatic nature fell outside the “tacit or expressed control or knowledge” of the intermediary, *prima facie* satisfying the threshold of Section 79(2) (b).¹⁵⁶ Thus, the High Court excluded interference that was outside the control and knowledge of the intermediary when evaluating whether it satisfied the requirements of Section 79(2)(b).

Outlook on neutrality and content moderation

The neutrality required of intermediaries to avail of safe harbour under Section 79(2) of the IT Act has also been used to question whether modern social media platforms should be entitled to immunity to begin with. A joint parliamentary committee report scrutinising India’s draft data protection legislation opined that the IT Act was no longer suited to regulate social media platforms, which algorithmically select the receivers of content.¹⁵⁷ The committee went on to suggest that social media platforms that “do not act as intermediaries” should be treated as publishers and made liable for hosting unlawful content.¹⁵⁸ The committee also amended the term used in the draft data protection legislation from “social media intermediary” to “social media platform” to reflect its observation that the functionality of social media companies may have transcended the neutral functionality associated with intermediaries under the IT Act.¹⁵⁹ However, the committee’s observations have been criticised as beyond the remit of data protection.¹⁶⁰ In the long run, as India gets ready to adopt a new data protection legislation and begins re-appraising the IT Act,¹⁶¹ the neutrality expected of intermediaries to avail of safe harbour is likely to be a key issue that needs addressing. As noted above, where neutrality is regulated, legislation in other countries has differentiated between various types of intermediaries rather than make neutrality and non-interference with content a pre-requisite to safe harbour for all intermediaries.¹⁶²

156 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [64]. The finding was preliminary and subject to evidence being led at trial.

157 Joint Committee on the Personal Data Protection Bill, 2019, ‘Report of the Joint Committee on the Personal Data Protection Bill, 2019’ (2021) 32–33 <<http://loksabhadocs.nic.in/LSSCOMMITTEE/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/Introduction/introduction.pdf>> accessed 2 May 2022.

158 *ibid* 33.

159 *ibid* 56.

160 Shweta Venkatesan, ‘Parliamentary Committee’s PDP Bill Report Isn’t Enough. Social Media Liability Needs Better’ *ThePrint* (4 December 2021) <<https://theprint.in/opinion/parliamentary-committees-pdp-bill-report-a-low-hanging-fruit-data-privacy-needs-rethink/776015/>> accessed 2 May 2022.

161 Viraj Gaur, ‘India Is Moving To Replace Two-Decade-Old IT Act With New ‘Digital India Act’ *TheQuint* (11 April 2022) <<https://www.thequint.com/tech-and-auto/tech-news/india-is-moving-to-replace-decades-old-it-act-with-new-digital-india-act-and-data-governance-framework-rajeev-chandrasekar>> accessed 2 May 2022.

162 Electronic Communications and Transactions Act, 2002 ss. 73-75 (South Africa); Directive 2000/31/EC of 8 June 2000 on electronic commerce, Arts. 12-14 (Europe); Bahl, Rahman and Bailey (n 65) 13.

The new Intermediary Guidelines 2021 expressly permit intermediaries to voluntarily take down a wide range of ‘prohibited’ content¹⁶³ without violating the non-interference requirement set out in Section 79(2)(b).¹⁶⁴ On the one hand, it permits and incentivises responsible private moderation by intermediaries who seek to create “hospitable environments” for end-users by removing content such as hate speech and pornography.¹⁶⁵ On the other hand, it increasingly vests the regulation of speech of internet users in the hands of a few large social media and search companies, creating a system of “private governance”.¹⁶⁶ This may be particularly problematic as large social media companies central to online speech struggle to moderate content in a consistent and transparent manner,¹⁶⁷ often even marginalising the role of moderation among corporate priorities.¹⁶⁸ Thus, the express recognition of content moderation provides valuable legal certainty for content moderation activities and incentivises intermediaries to remove harmful content. However, it also highlights the need to ensure that the content moderation activities of online intermediaries, particularly large social media companies, is transparent and accountable to users.

163 See Intermediary Guidelines 2021 r. 3(1)(b) (‘prohibited’ content includes content that is defamatory, obscene, pornographic, insulting, harassing, infringes intellectual property, impersonates another person, threatens public order or the defence or security of India, is deceptive or patently false).

164 Intermediary Guidelines 2021 r. 3(1)(d) (third proviso). For an analysis on the discretion granted to intermediaries under this proviso, refer to Section 4.3(iv) of this report.

165 Jack M Balkin, ‘Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation’ (2018) 51 UC Davis Law Review 1149, 1183.

166 *ibid* 1184.

167 Faiza Patel and Laura Hecht-Felella, ‘Facebook’s Content Moderation Rules Are a Mess’ (*Brennan Center for Justice*, 22 February 2021) <<https://www.brennancenter.org/our-work/analysis-opinion/facebooks-content-moderation-rules-are-mess>> accessed 7 October 2021.

168 Paul Barrett, ‘Who Moderates the Social Media Giants’ (New York University - Centre for Business and Human Rights 2020) <https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/5ed9854bf618c710cb55be98/1591313740497/NYU+Content+Moderation+Report_June+8+2020.pdf> accessed 7 October 2021; Sheera Frenkel and Davey Alba, ‘In India, Facebook Grapples With an Amplified Version of Its Problems’ *The New York Times* (23 October 2021) <<https://www.nytimes.com/2021/10/23/technology/facebook-india-misinformation.html>> accessed 7 February 2022.

(iii) ‘Due Diligence’ under Section 79(2)(c)

Section 79(2)(c) of the IT Act stipulates a key condition that intermediaries must satisfy to avail of safe harbour: “due diligence”.¹⁶⁹ While the contents of this due diligence obligation are discussed in subsequent sections of this report dealing with the Intermediary Guidelines 2021, it is pertinent to note that Section 79(2)(c) provides that an intermediary must observe due diligence while discharging its duties under the IT Act “and also” observes “such other guidelines” that the Union Government may prescribe.¹⁷⁰ The use of the term “and also” has led to the suggestion that Section 79(2)(c) creates two distinct obligations: (i) due diligence; and (ii) compliance with the Union Government’s guidelines.¹⁷¹ Admittedly, statutory interpretation requires giving effect to every word of a statute, and holding that the contents of due diligence are encapsulated by the guidelines would be to ignore the words “and also” in Section 79(2)(c).¹⁷² Indeed, a Single Judge of the High Court of Delhi had suggested that “*due diligence provided in the Act, has to be construed as being broad and not restricted merely to the guidelines themselves.*”¹⁷³ Similarly, the High Court of Andhra Pradesh (in a since overruled decision) noted that for an intermediary to satisfy its due diligence obligations, its actions must have been akin to that of a “*ordinary reasonable prudent man*”.¹⁷⁴

However, an alternative reading of the statutory and regulatory history would mitigate against this free-standing requirement of due diligence. When the IT Act was originally enacted in 2000, Section 79 did not include any reference to guidelines, merely stating that an intermediary would not be liable if it proved that it “had exercised all due diligence to prevent” the hosting and publishing of unlawful content.¹⁷⁵ However, by an amendment in the year 2009, the legislature amended Section 79 to expressly refer to guidelines issued by the Union Government.¹⁷⁶ The 2009 amendment also expressly granted the Union Government the power to promulgate guidelines under Section 79 (an enabling provision absent from the original IT Act).¹⁷⁷ Thus, the reference to guidelines may be viewed as an effort by Parliament to expressly limit the contours of due diligence to those prescribed by the guidelines.¹⁷⁸ In 2011, the Union Government introduced the Intermediary Guidelines 2011; Rule 3 of the Guidelines were titled “Due Diligence to be observed by intermediary”.¹⁷⁹ The Rule went on to state, “The intermediary shall observe following due diligence while discharging his duties, namely:-”¹⁸⁰ Identical language is used in the Intermediary Guidelines 2021.¹⁸¹

169 The Information Technology Act, 2000 s. 79(2)(c).

170 *ibid.*

171 T Prashant Reddy, ‘Back to the Drawing Board: What Should Be the New Direction of Intermediary Liability Law?’ (2019) 1 NLUJ Journal of Legal Studies 38, 48.

172 Gurshabad Grover and Anna Liz Thomas, ‘Intermediary Liability and Safe Harbour: On Due Diligence and Automated Filtering’ (*Law and Other Things*, 25 November 2020) <<https://lawandotherthings.com/intermediary-liability-and-safe-harbour-on-due-diligence-and-automated-filtering/>> accessed 27 October 2022.

173 *Christian Louboutin Sas v Nakul Bajaj* 2018 SCC OnLine Del 12215 [73]. Procedure questioned in *Clues Network Pvt Ltd v L’Oreal* 2019 SCC OnLine Del 7984 [34]-[36].

174 *Google India Pvt Ltd v Visaka Industries Ltd* 2016 SCC OnLine Hyd 393 [76] overruled by *Google India Pvt Ltd v Visaka Industries Ltd* (2020) 4 SCC 162.

175 The Information Technology Act, 2000 s. 79 (prior to its amendment in 2008).

176 The Information Technology (Amendment) Act, 2008 s. 40.

177 *ibid* s. 46.

178 Grover and Thomas (n 172).

179 The Information Technology (Intermediary Guidelines) Rules, 2011 G.S.R. 314(E) dated 11 April 2011 [Intermediary Guidelines 2011] r. 3.

180 Intermediary Guidelines 2011 r. 3.

181 Intermediary Guidelines 2021 r. 3.

Neither courts nor statute has definitively settled the issue of whether intermediaries possess any due diligence obligations outside the Intermediary Guidelines. However, the statutory and regulatory history of the due diligence obligation suggest that the legislature has expressly sought to narrow the interpretation of the broad term 'due diligence'; choosing instead to provide specific regulatory content to the obligation imposed on intermediaries through the Intermediary Guidelines. This interpretation has been recognised by some courts.¹⁸² For example, a Division Bench (two judges) of the High Court of Delhi read the contents of Rule 3 as constituting the substance of an intermediary's due diligence obligations under Section 79(2)(c).¹⁸³

182 *Flipkart Internet Pvt Ltd v State of NCT of Delhi* Writ Petition (Cri) 1376 of 2020 (High Court of Delhi, 17 August 2022) [20]; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [65].

183 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [65].

(iv) The Intermediary Guidelines 2011

The Intermediary Guidelines 2011 constituted the delegated legislation under Section 79(2)(c) of the IT Act. The Guidelines provided the conditions that intermediaries must observe to satisfy the requirements of Section 79(2)(c) as part of a broader safe harbour defence. The Intermediary Guidelines 2011 were promulgated on April 11, 2011, and have been replaced by the Intermediary Guidelines 2021 on February 25, 2021. Nonetheless, the Intermediary Guidelines 2011 remain relevant to understanding India’s regulatory regime. Several elements of the 2011 Guidelines were carried over into the 2021 Guidelines, and these are discussed in their newest iteration in the section of this report detailing the 2021 Guidelines. However, there are also notable differences between the 2011 and 2021 Guidelines, which highlight key regulatory trends.

Further, several important judicial decisions informing the contours of intermediary liability were given in the context of the 2011 Guidelines. Finally, there exists a lack of judicial and academic literature surrounding the newly notified 2021 Guidelines. Thus, the 2011 Guidelines serve as a useful backdrop to understand both: (i) how best to interpret the 2021 Guidelines, especially language that has been carried forward from the 2011 Guidelines; and (ii) what and how the Union Government has sought to change in 2021.

“Knowledge” under the Intermediary Guidelines 2011

The Intermediary Guidelines 2011 provided a broad list of what may be termed ‘prohibited third-party content’. This included content which is grossly harmful, blasphemous, defamatory, obscene, pornographic, invasive of a user’s privacy, hateful, disparaging, harmful to minors, infringing of intellectual property rights, violative of any Indian law, contains viruses, insults other nations or threatens the unity or security of India or public order, or causes incitement of a serious offence.¹⁸⁴ Rule 3(3) of the Intermediary Guidelines 2011 stipulated that an intermediary must not “knowingly” publish or host such ‘prohibited’ third-party content.¹⁸⁵ Thus, under the 2011 Guidelines, understanding when an intermediary is deemed to ‘know’ of ‘prohibited’ third-party content was critical to the larger question of immunity.

184 Intermediary Guidelines 2011 r. 3(2).

185 Intermediary Guidelines 2011 r. 3(3).

Knowledge may be actual or constructive, and it may be general or specific.¹⁸⁶ Actual knowledge requires the intermediary's knowledge of content to be actually demonstrable (e.g., a notice complaining against the content or a court/government order directing takedown), whereas under constructive knowledge standards the intermediary is deemed to know of content on its platform.¹⁸⁷ Knowledge may also be a general awareness of unlawful content, or specific awareness vis-à-vis identified and located pieces of content.¹⁸⁸

In addition to individuated cases of liability, the knowledge standard may significantly impact intermediary behaviour more generally. Narrowly construing the knowledge standard may cause intermediaries to be purposefully ignorant of unlawful content,¹⁸⁹ while broad interpretations such as constructive knowledge may cause intermediaries to take down lawful content due to the fear of liability.¹⁹⁰

Rule 3(4) of the 2011 Guidelines stated that an intermediary may obtain knowledge “by itself” or information may be “brought to [its] actual knowledge by an affected person in writing”.¹⁹¹ Although the text of the Guidelines opened the door to imposing constructive knowledge on intermediaries, courts clarified that the standard to be applied is that of actual knowledge.¹⁹² By applying the actual as opposed to the constructive knowledge standard, courts also militated against the imposition of a general monitoring obligation on intermediaries.¹⁹³ Further, in a series of cases discussing whether knowledge of ‘prohibited’ third-party content must be general or specific, courts have consistently insisted that the knowledge must be specific, typically in the form of URLs.¹⁹⁴ As the remainder of this section documents, the question of what exactly constitutes actual knowledge was the subject of significant controversy. The language ‘brought to its knowledge by an affected party’ in Rule 3(4) envisaged a private complaint resulting in actual knowledge for the intermediary, setting up a system that risked intermediaries taking down legitimate content in response to frivolous complaints.¹⁹⁵

186 Aradhya Sethia, ‘The Troubled Waters of Copyright Safe Harbours in India’ (2017) 12 *Journal of Intellectual Property Law & Practice* 398, 399.

187 D Friedmann, ‘Sinking the Safe Harbour with the Legal Certainty of Strict Liability in Sight’ (2014) 9 *Journal of Intellectual Property Law & Practice* 148; Gavin Sutter, “Don’t Shoot the Messenger?” *The UK and Online Intermediary Liability*’ (2003) 17 *International Review of Law, Computers & Technology* 73; Q Tao, ‘The Knowledge Standard for the Internet Intermediary Liability in China’ (2012) 20 *International Journal of Law and Information Technology* 1.

188 Sethia (n 186) 399.

189 Friedmann (n 187).

190 Sutter (n 187) 75–76.

191 *Intermediary Guidelines 2011* r. 3(4).

192 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121]-[123].

193 See Richard Arnold, ‘Intermediary Liability and Trade Mark Infringement: A Common Law Perspective’ in Giancarlo Frosio (ed), Richard Arnold, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 416. Noting that requiring intermediaries to block content without actual knowledge of the unlawful content amounts to a general monitoring obligation.

194 *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi, 21 January 2020); *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382; *R K Productions Pvt Ltd v Bharat Sanchar Nigam Limited* 2012 SCC OnLine Mad 4184.

195 Arun and Singh (n 68); Rishabh Dara, ‘Intermediary Liability in India: Chilling Effects on Free Expression on the Internet’ [2011] SSRN Electronic Journal <<http://www.ssrn.com/abstract=2038214>> accessed 18 February 2021.

Notice and takedown under the 2011 Guidelines

Under Rule 3(4) of the Intermediary Guidelines 2011, once an intermediary had “actual knowledge” of ‘prohibited’ third-party content on its platform (based on a written complaint), it was required to remove or disable access to such content within thirty-six hours.¹⁹⁶ The Rule effectively created a ‘notice and takedown’ regime, where intermediaries were required to take down content upon receipt of a private complaint to enjoy the qualified immunity under Section 79.

Notice and takedown regimes are driven by the practical concerns of ensuring fast and effective relief to parties potentially injured by online content, without imposing the time and costs associated with the judicial process.¹⁹⁷ However, absent strong safeguards to protect free expression, notice and takedown regimes may result in the stifling of free speech.¹⁹⁸ Intermediaries are not compelled to evaluate the legality of speech they take down pursuant to a private complaint, and this could lead to lawful and constitutionally protected speech being taken down merely because it offended the sensibilities of a single internet user.¹⁹⁹

If there are a large volume of frivolous requests, and intermediaries do begin evaluating complaints by deciding upon competing rights, they effectively engage in a public censorship function; a task they may lack the specialised skills and the legitimacy to carry out.²⁰⁰ Because content is taken down by communications between the intermediary and a private complainant, an opaque process is created where content originators and third parties (who have rights to access information) have limited legal remedies to enforce their freedom of expression claims and reinstate content.²⁰¹ To make matters worse, conditioning immunity on the take down of content within a short period of time, fundamentally incentivises intermediaries to over comply, leading to constitutionally protected content being taken down.²⁰² Safeguards can include some verification for complaints and punishments for sending abusive complaints, or automatic reinstatement of content after a brief period if the complainant is unable to secure a court order.

Research was able to demonstrate that under the 2011 Guidelines, the thirty-six hour timeframe granted to intermediaries to take down content caused them to over-comply with user takedown requests and restrict constitutionally protected speech.²⁰³

196 Intermediary Guidelines 2011, r.3(4). The Union Government has released a clarification on 18 March 2013 that an intermediary was only required to “respond or acknowledge” the complaint within thirty-six hours and “redress” the complaint within one month.

197 See Aleksandra Kuczerawy, ‘From “Notice and Takedown” to “Notice and Stay Down”’: Risks and Safeguards for Freedom of Expression’ in Giancarlo Frosio (ed), Aleksandra Kuczerawy, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 527.

198 Kuczerawy (n 197).

199 *ibid*; Christophe Geiger, Giancarlo Frosio and Elena Izyumenko, ‘Intermediary Liability and Fundamental Rights’ in Giancarlo Frosio (ed), Christophe Geiger, Giancarlo Frosio and Elena Izyumenko, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 145.

200 Kuczerawy (n 197) 527.

201 The Intermediary Guidelines 2011 did not offer a hearing to originators, nor did it require a notice informing originators or other internet users that the content had been taken down pursuant to a takedown request.

202 Kuczerawy (n 197).

203 Dara (n 195).

The 2011 Guidelines were criticised for permitting a regime of horizontal censorship by allowing content to be taken down at the behest of private user complaints, compelling intermediaries to make quick-fire decisions on the legality of content; and promoting a regime that lacked transparency and accountability between other internet users and intermediaries.²⁰⁴ Although the Union Government never repealed or amended the Intermediary Guidelines 2011, the notice and takedown regime was radically altered by the decision of the Supreme Court of India in *Shreya Singhal vs. Union of India*.²⁰⁵

204 Arun and Singh (n 68) 27.

205 2015 (5) SCC 1.

4.2. *Shreya Singhal vs. Union of India* and its aftermath

The decision in *Shreya Singhal* primarily concerned the constitutional validity of Section 66A of the IT Act (punishing the sending of ‘grossly offensive’ content over computer networks). The petitioners in the case also challenged Section 69A (the government’s power to block websites or content) and Section 79 (safe harbour) along with certain provisions of the Intermediary Guidelines 2011. With respect to Section 79, the petitioners contended that the 2011 Guidelines effectively required intermediaries to determine the legality of content upon receipt of a private complaint, which was contrary to their role as neutral entities.²⁰⁶ Further, the petitioners argued that the broad definition of ‘prohibited’ third-party content in Rule 3(2) of the Intermediary Guidelines 2011 allowed more speech to be restricted than permitted by Article 19(2) of the Indian Constitution.²⁰⁷

(i) The decision of the Supreme Court

On March 24, 2015, the Supreme Court of India ruled largely in favour of the petitioners. Although the judgement predominantly focussed on the unconstitutionality of Section 66A, after a limited discussion, the Supreme Court accepted the petitioner’s arguments on safe harbour. The Court began its analysis by observing that under Section 69A of the IT Act, access to content could only be blocked by a reasoned order of the Union Government and compliance with several procedural safeguards.²⁰⁸ It observed that Section 69A did not contemplate an intermediary making its own determination as to the legality of content.²⁰⁹ Extrapolating to Section 79 this legislative conception of intermediaries as neutral entities who do not interfere with content, the Supreme Court ruled that the ‘actual knowledge’ requirement in Section 79(3)(b) of the IT Act and Rule 3 of the Intermediary Guidelines 2011 must be interpreted as the intermediary receiving a court order to take down content (the possibility of a government notification requiring removal at the risk of losing safe harbour was left untouched).²¹⁰ The Court noted that the “*millions of requests*” submitted to large intermediaries would mean that in reality, intermediaries would have to judge which requests were legitimate.²¹¹

206 Alternatively, if intermediaries do *not* apply their mind, a significant amount of lawful speech will be restricted at the behest of private complainants.

207 Under Article 19(2) of the Constitution of India, reasonable restrictions may be placed on speech only in the interests of: “the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.”

208 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121]. *See also* The Information Technology Act, 2000 s. 69A.

209 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121].

210 *ibid* [122].

211 *ibid* [122].

As a result of the decision, an intermediary was no longer obligated to take down content upon receipt of a private complaint to retain safe harbour. Under *Shreya Singhal*, an intermediary would only lose safe harbour if it failed to take down content pursuant to a court or government order. An intermediary could in principle refuse to take down content (until it received a court or government order) and continue to be eligible for safe harbour. This significantly increased the knowledge threshold by interpreting the phrase “actual knowledge” under the Intermediary Guidelines 2011 and Section 79(3)(b) of the IT Act.²¹² Prior to *Shreya Singhal*, actual knowledge had meant a written complaint by an aggrieved private party. After the judgement, it meant an order by a court, while Section 79(3)(b) continued to state that intermediaries would lose safe harbour for failing to comply with a government notification directing the removal of online content. Lastly, the Supreme Court also held that any court order or government notification must “*strictly conform to*” constitutionally permissible restrictions on the freedom of speech under the Indian Constitution.²¹³

212 Sethia (n 186) 404.

213 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [122].

(ii) Impact of the Supreme Court's decision

The decision in *Shreya Singhal* is best understood contextually, in light of the law prior to 2015 and how courts have subsequently applied its rationale. Issues of safe harbour typically attempt to balance the harm arising from speech against protecting free speech online. First, the decision in *Shreya Singhal* did not concern copyright infringement. Within a year of the decision in *Shreya Singhal*, the High Court of Delhi ruled that a judicial order was not necessary in cases of alleged copyright infringement, and an intermediary would be obligated (at the risk of losing safe harbour) to take down content upon receipt of a complaint by a copyright owner asserting infringement.²¹⁴ This is in line with the approach under the Copyright Act and the relevant regulations.²¹⁵ Therefore, the judicially-authorized takedown requests required by *Shreya Singhal* must be understood in the context of other classes of unlawful content, such as hate speech, child sex abuse material, and defamatory content.

Notice and takedown regimes offer higher protection to a party potentially injured by online speech due to the speed of content removal. *Shreya Singhal's* requirement of a court order prior to takedown is diametrically opposed to this approach. Park argues that the decision in *Shreya Singhal* does not align with Section 79's 'liability exempting' nature, noting that intermediaries did not actually have to decide the legality of content under Section 79 correctly to be exempt from liability, but merely had to comply with takedown notices to avail of safe harbour.²¹⁶ However, given that take-down requests are completely unverified, this approach leads to one of two real-world outcomes: (i) intermediaries taking down vast swathes of content at the behest of complainants to preserve safe harbour; or (ii) intermediaries applying their own judgement to determine which requests were legitimate or not at the risk of losing safe harbour.

As Park also acknowledges, the architecture of the IT Act and the Intermediary Guidelines only incentivise the taking down of content and not its reinstatement if the content is subsequently found to be legal.²¹⁷ When this architecture is paired with empirical evidence of over-compliance by intermediaries,²¹⁸ it becomes evident that by removing content at the behest of a private party, India's notice and takedown regime skewed towards protecting injured parties and failed to sufficiently protect free expression and access to information.²¹⁹ Thus, the decision in *Shreya Singhal*

214 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [54]. For a detailed analysis of the High Court's reasoning, refer to Section 5.2 of this report.

215 The Copyright Act, 1957 s. 52(1)(c); The Copyright Rules, 2013 G.S.R. 172(E) dated 14 March 2013 r. 75(3). For a detailed analysis of the safe harbour offered to intermediaries in the case of copyright actions, refer to Section 5.1 of this report.

216 Park (n 109) 262–263.

217 *ibid.*

218 Dara (n 195).

219 Yogesh Pai and Nitesh Daryanani, 'Online Intermediary Liability and Privacy in India' [2016] SSRN Electronic Journal <<https://www.ssrn.com/abstract=2856527>> accessed 11 February 2021.

may be viewed as judicially installing certain free speech safeguards. The specific safeguard adopted by the Supreme Court was a judicial balancing of rights prior to the removal of content.

Reddy has criticised the Supreme Court's reliance on the 'millions of requests intermediaries receive' to strike down the notice and takedown regime; also noting that the resulting regime is too protective of intermediaries and has increased the costs for injured parties who want to take down content.²²⁰ For example, an individual against whom defamatory content has been uploaded to the internet would have to undertake the expensive and time consuming task of securing a court order to get the content taken down. However, when evaluating this criticism, it must be recognised that the decision in *Shreya Singhal* does not prevent intermediaries from removing content pursuant to a complaint, it merely states that they shall not lose safe harbour for failing to do so (the complications posed by Section 79(2)(b) of the IT Act are discussed separately at section 4.1(ii) of this report). Large platforms for example may take down such content without a court order for violating their terms of service or where the content is ex-facie illegal. Nonetheless, certain online intermediaries may decline to do so or merely be unresponsive to complaints. The risk of such online harms is aggravated where intermediaries derive monetary benefits from keeping the content up, and the requirement to secure a court order may disproportionately impact the already socially and economically marginalised.

220 Reddy (n 171) 49–50.

The Supreme Court's discussion of safe harbour in *Shreya Singhal* is admittedly brief, spanning just two paragraphs. However, the court's choice of solution comes into clearer view upon an examination of the options facing the court. Briefly summarised, the Court could have: (i) ruled that intermediaries risk losing safe harbour for failure to take down content pursuant to a private notice, despite knowing that many requests were not legitimate – harming free speech; (ii) allowed intermediaries to deal with requests as they saw fit, knowing that this permitted private intermediaries to ultimately determine the legality of speech (this also contradicted the grammar of the IT Act, which viewed intermediaries as neutral); or (iii) ruled that an intermediary only risked losing safe harbour if they failed to comply with a judicial or government order directing takedown. This third option was ultimately viewed by the Court as an appropriate balance between the rights of potentially injured parties and free speech while still adhering to the neutral conception of intermediaries and not

vesting them with too much power over speech. It preserved the intermediaries' ability to voluntarily remove content, ensured that users have recourse against unresponsive intermediaries, and reduced the incentive of intermediaries to over-remove, thus protecting the free flow of information.

Viewed from this perspective, a close reading suggests that the Court's reference to the volume of requests received by intermediaries (criticised by Reddy) has less to do with alleviating operational burdens of intermediaries and more to do with the large number of requests leading to intermediaries *ipso facto* determining which requests were legitimate, and consequently, what speech is legal. The Supreme Court expressly stated, "*it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. (emphasis supplied)*"²²¹ This is an acknowledgement that although intermediaries were not required to determine the legality of content disputed in a private complaint, the volume and potentially abusive nature of such notices risked intermediaries doing exactly that or simply removing everything that was complained against. The Court's approach prevented intermediaries from having to make this choice. Under *Shreya Singhal*, intermediaries could continue to enforce their terms of service, and if an intermediary refused to remove content, a user could secure a court order, and the content would be kept up or taken down pursuant to a judicial determination instead of an intermediary's.

²²¹ *Shreya Singhal v Union of India* 2015 (5) SCC 1 [122].

The Supreme Court was also unwilling to grant intermediaries *carte blanche* in making determinations of whether content stayed online (this would have resulted in a blanket immunity where users have very limited or no recourse against an intermediary hosting unlawful content). Such an approach was always unlikely given Section 79(3) of the IT Act required intermediaries to remove content upon receiving actual knowledge or risk losing safe harbour. However, the Court attempted to craft a procedure that preserved user's recourse against harmful content without incentivising intermediaries to over-remove content due to the risk of losing safe harbour. Earlier in the judgement, the Court distinguished the procedure for the Union Government taking down content under Section 69A (power to block websites) and the private notice and takedown regime. The Court observed that Section 69A provided numerous safeguards against taking down

content, such as hearings for the content originator, ultimately noting that “*The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69-A*”.²²² This would suggest that the Supreme Court was seeking to avoid granting private intermediaries absolute control over the taking down of content. This would also explain why the Court did not impose the judicial order requirement only on some large intermediaries (which it could have done if it was solely concerned with reducing the operational difficulties arising from the large number of requests). The Court ultimately sought to balance user recourse against harmful content with the need to ensure intermediaries did not over-remove content due to a risk of losing safe harbour.

222 *ibid* [121].

Fallout of *Shreya Singhal*

Since the decision in *Shreya Singhal*, arguments have been raised that the requirement of a court order to compel an intermediary to remove content or risk losing safe harbour should not be applicable to all situations; and that in certain situations, intermediaries should lose safe harbour if they are unresponsive to complaints. For example, the Delhi High Court distinguished *Shreya Singhal's* reasoning and judicial order requirement in the context of copyright actions.²²³ This argument has primarily centred on how different types of content ought to be treated differently, based on the ease of determining its legality. For example, the illegality of child sex abuse material is comparatively easy to determine and may not require judicial determinations – clear cases potentially being amenable to voluntary content moderation and a notice and take down regime. However, content involving allegedly defamatory statements or political hate speech may require careful judicial consideration, of the kind intermediaries are both ill-suited and lack the legitimacy to make.²²⁴

223 For a detailed analysis on the reasoning employed by the High Court of Delhi when distinguishing *Shreya Singhal*, refer to Section 5.2 of this report.

224 Kuczerawy (n 197) 527.

Distinguishing the responses intermediaries are required to make based on how hard it is to determine the legality of content may have certain advantages.

- (1) The speech interests in content being taken down may not be universally high enough to warrant a judicial balancing of rights. For example, where the Supreme Court of Argentina imposed the requirement of a judicial order prior to takedown, it expressly exempted ‘ostensibly or manifestly’ – unlawful content such as child sex abuse material, content inciting violence, crime or promoting genocide, or content seriously invading a person’s privacy – from prior judicial scrutiny.²²⁵ Thus, for the most obvious of notices, intermediaries were suited to take down content. Similarly, Austria’s proposed Communication Platforms Act distinguished between content where the “*illegality is already evident to a legal layperson without further investigation,*” and content where the “*illegality becomes apparent only after a detailed examination.*”²²⁶
- (2) *Shreya Singhal* imposes certain burdens on persons potentially injured by online content, requiring them to approach a court and incur legal costs where an intermediary is unresponsive to their complaints.²²⁷ Given the rapid pace of the internet and the time required to obtain a court order in India, content may cause significant damage to a person long before it is taken down.
- (3) In more borderline cases where interests may need to be balanced (e.g., defamation or hate speech), intermediaries can safely keep the content online without risking the loss of safe harbour. In hotly contested cases (e.g., involving political leaders), the role of private intermediaries in shaping public discourse is reduced as intermediaries can wait for a court or government order.

However, distinguishing between clear and borderline cases, and preventing the abuse of such a distinction, may pose serious, potentially insurmountable, challenges. It is also important to note that the requirement for a court order does not bar an intermediary from removing ex-facie illegal content, or content that violates their terms of service voluntarily pursuant to a private complaint; intermediaries are merely not at risk of losing safe harbour for failing to remove content. Thus, arguments that

225 Giancarlo Frosio and Paula Vargas, ‘Argentine Supreme Court Decides Landmark Intermediary Liability Case’ (*The Centre for Internet and Society (Stanford Law School)*, 5 November 2014) </blog/2014/11/argentine-supreme-court-decides-landmark-intermediary-liability-case> accessed 9 March 2021; Giancarlo Frosio and Sunimal Mendis, ‘Monitoring and Filtering: European Reform or Global Trend?’ in Giancarlo Frosio (ed), Giancarlo Frosio and Sunimal Mendis, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 549.

226 Draft Federal Act on measures to protect users on communication platforms (Communication Platforms Act), Federal Law Gazette of the Republic of Austria dated 23 December 2020, s. 3.

227 Reddy (n 171) 49–50.

Shreya Singhal imposes burdens on victims of online harms are most applicable to situations where intermediaries are unresponsive to complaints for ex-facie illegal content; with the behaviour of such ‘rogue’ intermediaries unlikely to improve by a threat of losing safe harbour in the absence of meaningful prosecution or civil suits. Arguments that a court or government order requirement raises the risk of online harms, or systemic bad or unresponsive intermediaries must also demonstrate the eventual loss of safe harbour under a notice and takedown regime will result in lawsuits or prosecutions of such ‘rogue’ intermediaries so as to serve as a meaningful deterrent (as opposed to only lawsuits against intermediaries that are generally responsive and seek to preserve safe harbour but have erred in a single instance).

Lastly, the Supreme Court’s observation that court and government-ordered takedowns should strictly conform to constitutionally permissible restrictions is made in the context of a traditional State-citizen relationship. While Article 19(2) of the Indian Constitution provides limited grounds on which the State may interfere with free speech,²²⁸ it may be desirable for platforms to restrict speech beyond these interests.²²⁹ For example, fraud, consumer harm, or copyright infringement are not constitutionally-sanctioned grounds on which to restrict free speech, but their removal is essential to the functioning of online information eco-systems. This tension is reflected in the broad categories of speech that the Intermediary Guidelines 2011 and 2021 proscribe.²³⁰

228 The permissible restrictions on free speech under the Indian Constitution are set out in Article 19(2) and are “the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.”

229 Daphne Keller, ‘Lawful but Awful? Control over Legal Speech by Platforms, Governments, and Internet Users’ (*The University of Chicago Law Review Online*, 28 June 2022) <<https://lawreviewblog.uchicago.edu/2022/06/28/keller-control-over-speech/>> accessed 30 July 2022.

230 See Section 4.3(ii) of this report.

(iii) Public interest litigation post-*Shreya Singhal*

The criticisms of *Shreya Singhal* are representative of the broader trend of governments across the world seeking to impose greater responsibility and accountability on intermediaries to remove unlawful content.²³¹ In India, this trend is reflected in public interest litigation that asked for large technology companies to provide technical solutions to restrict unlawful content online, ultimately contributing to a revision of the Intermediary Guidelines 2011.

231 Frosio and Mendis (n 225).

Litigation around pre-filtering tools

In 2015, the Supreme Court of India began hearing a public interest litigation concerning the circulation of videos depicting rape and websites that hosted such content.²³² In 2017, the Supreme Court appointed an *amicus curiae*, who suggested that unlawful content such as explicit videos and photographs could be pre-emptively blocked through the use of technological solutions.²³³ The Supreme Court set up a committee of civil servants and representatives from Facebook, Google, Yahoo, and Microsoft to examine the “feasibility of ensuring that videos depicting gang rape, child pornography and rape should not be made available to the general public”.²³⁴ Although the committee’s recommendations were not unanimous, the recommendations recorded by the Supreme Court included:

232 *In re: Prajwala Letter dated 18.2.2015* SMW (Cri) 3 of 2015 (Supreme Court of India, 27 February 2015).

233 *ibid* (1 February 2017).

234 *ibid* (22 March 2017).

- The Union Government should create a hash bank of content depicting rape, and formulate specific parameters for identifying such content and ensuring its expeditious removal;
- Content hosting platforms and search engines shall work with the Union Government to create processes for the proactive verifying, identification, and take down of child sex abuse material and content depicting rape, including research and development on artificial intelligence systems capable of real-time filtering;
- The Ministry of Home Affairs, Department of Telecommunications, and law enforcement agencies should directly order ISPs to prevent the circulation of child sex abuse material and content depicting rape;

- Proprietary tools such as PhotoDNA and VideoHash should be implemented on the WhatsApp messaging client that match content against central databases of child sex abuse material and content depicting rape while maintaining the integrity of the contents of the message and metadata; and
- Content hosting platforms retain the information of originators and assist law enforcement agencies.²³⁵

235 *ibid* (23 October 2017).

In November 2018, the Union Government informed the Supreme Court that certain steps were required to be taken by intermediaries to achieve satisfaction with the committee's recommendations, including:

- The setting up of “*proactive monitoring tools for auto deletion of unlawful content by deploying Artificial intelligence tools*”;
- The deploying of moderators for identifying and deletion of unlawful content;
- Appointment of officers and escalation officers in India and the setting up a round-the-clock mechanism for prompt compliance with the takedown orders issued by law enforcement agencies and the government.²³⁶

236 *ibid* (28 November 2018).

The technology companies that were parties to the court proceedings had varied responses to the Union Government's observations on the next steps to be taken and proposed sharing 'standard operating procedures' to implement the committee's recommendations.²³⁷

237 *ibid* (6 December 2018).

Litigation around 'traceability' obligations

In a separate dispute beginning in 2018, two petitions were filed in the High Court of Madras by victims of alleged cyber-bullying.²³⁸ The petitions contended that it was impossible to identify the originator of the alleged bullying on social media platforms and asked the High Court to direct that an individual's social media account be linked to their Aadhar number (a unique identification number possessed by a majority of Indian citizens and linked to a citizen's biometric and demographic data). This plea was subsequently withdrawn; however, the High Court deemed it appropriate to implead Facebook, Twitter, YouTube, Google, and WhatsApp as respondents and investigate the extent to which

238 *See Antony Clement Rubin v Union of India* WP 20774 of 2018 (High Court of Madras); *Janani Krishnamurthy v Union of India* WP 20214 of 2018 (High Court of Madras).

intermediaries provide information to law enforcement agencies.

Before the High Court, a key issue was whether it was sufficient for intermediaries to provide law enforcement agencies with ‘Basic Subscriber Information’ (BSI) that they possessed, or whether the intermediaries were obligated to provide additional information. The respondent intermediaries argued that they could only provide information to the extent that it existed on their platforms and was reasonably accessible.²³⁹ WhatsApp specifically argued that it could not comply with requests for content removal, sharing of originator identities, and call logs, as it provided an end-to-end encrypted platform wherein WhatsApp itself did not record and store this information, and to the extent the information did exist, WhatsApp was not in possession of the requisite decryption key.²⁴⁰

239 *Antony Clement Rubin v Union of India* WP 20774 of 2018 (High Court of Madras, 25 April 2019).

240 *ibid.*

During the pendency of the dispute before the High Court of Madras, Facebook approached the Supreme Court of India and sought to have the dispute (along with analogous disputes in the country) transferred to the Supreme Court. The Supreme Court noted that the key issue was how and in what manner intermediaries should provide information (including the names of originators) to law enforcement agencies.²⁴¹ In October 2019, the Supreme Court transferred the dispute to itself.²⁴² At the time of writing this report, the Supreme Court last heard the dispute on January 30, 2020²⁴³ and has yet to issue a final judgement in the matter.

241 *Facebook Inc v Union of India* TP (C) 1943-46 of 2019 (Supreme Court of India, 24 September 2019).

242 *ibid.* (22 October 2019).

As both these cases worked their way through the courts, MEITY released draft amendments to the Intermediary Guidelines 2011,²⁴⁴ and eventually replaced the Intermediary Guidelines 2011 with the Intermediary Guidelines 2021.

243 *Sagar Rajbhau Suryavanshi v Union of India* TC (C) 5 of 2020 (Supreme Court of India, 30 January 2020). Diary No 986 of 2020.

244 Ministry of Electronics and Information Technology, The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018, December 24, 2018, <https://prsindia.org/files/bills_acts/bills_parliament/Draft_Intermediary_Amendment_2018.pdf> (draft rules) accessed on 13 September 2021.

4.3. Intermediary Guidelines 2021: Rule 3

The Intermediary Guidelines 2021 constitute delegated legislation under the IT Act and, like the Intermediary Guidelines 2011 that they replace, detail the conditions intermediaries must observe to satisfy their due diligence obligations under Section 79(2)(c). As discussed in Section 2 of this report, since 2015 the Union Government had made several statements on the need for large social media platforms to be accountable to Indian authorities for content they host, and to assist law enforcement agencies in investigating crimes.²⁴⁵ To further these goals, in 2018 MEITY released draft revisions to the Intermediary Guidelines 2011 and began a public consultation process.

The draft guidelines attempted to codify the ‘judicial order and takedown’ regime set out in *Shreya Singhal* but also inter alia: (i) imposed obligations on intermediaries to proactively remove ‘prohibited’ third-party content from their platforms; (ii) required intermediaries to trace the ‘originator’ of individual pieces of content at the behest of law enforcement agencies; and (iii) required intermediaries with more than 5 million ‘Indian users’ to incorporate themselves under Indian company law.²⁴⁶ The draft guidelines were widely criticised; the use of proactive filters and the identification of ‘originators’ were believed to violate the constitutional guarantees of free speech and privacy, and concerns were raised that local incorporation requirements would hamper innovation.²⁴⁷

These draft guidelines were never promulgated. Rather, in February of 2021, without any further public consultations, the Union Government notified a revised and expanded set of regulations titled the “Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021” (or Intermediary Guidelines 2021). These Guidelines were themselves subsequently amended in October 2022 by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 (‘October 2022 Amendment’).²⁴⁸ As the name suggests, the Intermediary Guidelines 2021 regulate both intermediaries as well as publishers of digital news media²⁴⁹ and curated audio-visual content.²⁵⁰ Although this report does not cover the obligations imposed on digital media outlets by the Intermediary Guidelines 2021, it is important to note that under Rule 5, all intermediaries must inform publishers of news and current affairs content on their platform to furnish their user accounts to the Ministry of

245 Ahmad (n 61).

246 Ministry of Electronics and Information Technology, ‘Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018’ (24 December 2018) <https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf> accessed 15 October 2021.

247 See ‘Comments to the Information Technology [Intermediary Guidelines (Amendment) Rules] 2018’ (Comments invited on Draft of Intermediary Guidelines 2018, 31 January 2019) <<https://www.meity.gov.in/comments-invited-draft-intermediary-rules>> accessed 13 September 2021; Centre for Communication Governance, ‘Submission of Comments on the Draft Information Technology Intermediary Guidelines (Amendment) Rules, 2018’ <<https://ccgdelhi.org/wp-content/uploads/2019/02/CCG-NLU-Comments-to-Meity-on-Draft-IL-Guidelines-Amendment-Rules.pdf>>; Software Freedom Law Centre, ‘The Future of Intermediary Liability in India’ (2020) <https://sflc.in/sites/default/files/2020-01/SFLC.in%20-%20Intermediary_Liability_Report_%282020%29_1.pdf> accessed 13 July 2021.

248 G.S.R. 794(E) dated 28 October 2022.

249 Intermediary Guidelines 2021 r. 2(t) (defining ‘publisher of news and current affairs content’ as an online newspaper, news portal, news aggregator, news agency, or other functionally similar entities but not newspapers, replica e-papers, or individuals transmitting content outside the course of a systematic commercial activity).

250 Intermediary Guidelines 2021 r. 2(q) (defining ‘online curated content’ as any curated catalogue of audio-visual content made available through computer networks, and includes films, audio-visual programmes, documentaries, television programmes, serials, and podcasts but does not include news and current affairs content); Intermediary Guidelines 2021 r. 2(u) (defining ‘publisher of online curated content’ to be a publisher who plays a significant role in making available online curated content but excludes individual users who are transmitting content outside the course of a systematic commercial activity).

Information and Broadcasting ('MIB').²⁵¹ Intermediaries may also provide publishers who have furnished their user accounts to the Ministry with a “demonstrable and visible mark of verification” on their platforms.²⁵² The MEITY has acknowledged that certain entities’ functionality may be akin to both an ‘intermediary’ and a ‘news aggregator’ or ‘news publisher’, and has stated that such entities may seek clarifications from the MIB to ensure they are in compliance with the Intermediary Guidelines 2021.²⁵³

A new paradigm

The Intermediary Guidelines 2021 represent a new paradigm in India’s regulation of online intermediaries. Post the adoption of the Intermediary Guidelines in 2011 and the decision in *Shreya Singhal* in 2015, there has been widespread recognition of the key role online intermediaries play in facilitating speech, the ongoing ‘platformization of public debate’,²⁵⁴ the sophisticated ways in which social media platforms curate third-party content, and the real-world consequences of online speech. The Intermediary Guidelines 2021 are a response to this new reality. The Guidelines aim to leverage the pre-requisites of safe harbour under Section 79 to modify intermediary behaviour, particularly that of social media intermediaries, to achieve greater accountability to both internet users and the Indian government.

The Intermediary Guidelines 2021 can thus be understood as acting along two axes. The first is the internet user-intermediary axis, and the second is the government-intermediary axis. The former tracks the relationship internet users have with online intermediaries, including questions of access to content, the accountability and transparency of moderation. The government-intermediary axis tracks the regulatory, investigative, and censorial powers government authorities have over intermediaries, and consequently over online speech. The government-intermediary axis results in government decisions on online content impacting users through intermediaries.

These dual axes are a recognition of speech regulation shifting from a ‘dyadic to a triadic model’, where intermediaries sit between governments and speakers.²⁵⁵ The Indian government is concerned with the accountability of platforms to users (insisting that platforms grant users hearings for moderation decisions and allowing users to appeal to a government committee against platform moderation decisions). However, it also recognises that

251 Intermediary Guidelines 2021 r. 5.

252 Intermediary Guidelines 2021 r. 5.

253 Ministry of Electronics and Information Technology (n 62). FAQ 9.

254 Tarlach McGonagle, ‘Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation’ in Giancarlo Frosio (ed), Tarlach McGonagle, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 479–485.

255 Kate Klonick, ‘The New Governors: The People, Rules, and Processes Governing Online Speech’ (2018) 131 *Harvard Law Review* 1598, 1664.

any speech regulation, censorship, or surveillance it wishes to carry out must be operationalised through intermediaries.

Still only conditions for safe harbour

As expected of guidelines setting out the due diligence obligations of intermediaries under Section 79(2)(c) of the IT Act, the Intermediary Guidelines 2021 (Rule 7) states that a failure to comply with the Guidelines disentitles an intermediary from seeking safe harbour under Section 79(1).²⁵⁶ Rule 7 of the 2021 Guidelines also states that failure to observe the Guidelines shall result in the intermediary being liable for punishment under any law in force, including the Indian Penal Code, 1860.²⁵⁷ The IT Act does contain a residuary provision which punishes non-compliance with any provision of the statute or regulations under the statute with a fine of ₹25,000.²⁵⁸ However, given that the Intermediary Guidelines constitute conditions precedent for availing of safe harbour, the consequence of a breach of the Intermediary Guidelines/Section 79(2)(c) would merely be non-applicability of safe harbour.

256 Intermediary Guidelines 2021 r. 7.

257 Intermediary Guidelines 2021 r. 7.

258 The Information Technology Act, 2000 s. 45.

Thus, Rule 7 may be read as: failure to observe the Guidelines shall result in the possibility of an intermediary being secondarily liable for unlawful content it hosts or makes available on its platform due to the non-applicability of safe harbour under Section 79. However, as discussed earlier in this report, such liability would be subject to an ascertainment of the intermediary's role and the illegality of the content.²⁵⁹ This understanding is supported by the MEITY's own documentation, which states that non-compliance with the Intermediary Guidelines 2021 will lead to a loss of the exemption under Section 79 "with respect to the extant law violated."²⁶⁰ This highlights how intermediary liability is determined on a case by case basis with respect to the specific unlawful content an intermediary is being sued or prosecuted for and the specific laws such content may violate.

259 See Section 4 of this report.

260 Ministry of Electronics and Information Technology (n 62). FAQ 27.

This section of the report documents and analyses the content of Rule 3 of the Intermediary Guidelines 2021, while section 4.4 of the report examines Rule 4 of the Guidelines applicable to SSM Intermediaries. Finally, the October 2022 Amendment is discussed in section 4.5(ii).

(i) Staggered due diligence obligations for different intermediaries

The Intermediary Guidelines 2021 create two tiers of due diligence obligations, one for ‘intermediaries’ simpliciter, and another for ‘significant social media intermediaries’ (‘SSM Intermediaries’).²⁶¹ The Intermediary Guidelines 2021 defines a “significant social media intermediary” as an intermediary that: (i) primarily “enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify, or access information” using the intermediary’s services and; (ii) has more “users in India”²⁶² than a threshold specified by the Union Government.²⁶³ In February 2021, the Union Government set the threshold for SSM Intermediaries at 5 million users in India.²⁶⁴ In a non-legal clarificatory document, the MEITY listed three factors that may be indicative of significant social media functionality: (i) facilitating users to increase their ‘reach and following’; (ii) facilitating interactions with unknown users; and (iii) the ability of content to go ‘viral’ through user-sharing.²⁶⁵ The Intermediary Guidelines 2021 clarify that intermediaries that primarily enable commercial transactions, provide access to the internet, are search engines, online encyclopaedias or directories, online storage services, or email services are not SSM Intermediaries.²⁶⁶

Rule 3 of the Guidelines sets out the due diligence obligations to be observed by all intermediaries, including SSM Intermediaries.²⁶⁷ Rule 4 sets out certain additional due diligence obligations that apply solely to SSM Intermediaries.²⁶⁸ The Intermediary Guidelines 2021 thus creates a two-tiered system of due diligence obligations, with additional requirements placed on SSM Intermediaries. Rule 6 also empowers the Union Government to require any intermediary to observe the additional due diligence obligations set for SSM Intermediaries where “the services of that intermediary permits the publication or transmission of information in a manner that may create a material risk of harm to” the sovereignty, integrity or security of India, its relations with foreign States, or public order.²⁶⁹ The reasons for determining that an intermediary’s services pose a material risk shall be recorded in writing²⁷⁰ and shall be based on whether the intermediary’s platform allows interaction between users and the publication or transmission of content to a significant number of users.²⁷¹

261 Intermediary Guidelines 2021 r. 3, r. 4.

262 Intermediary Guidelines 2021 r. 2(1)(x) (defining ‘user’ as a person who accesses any computer resource of an intermediary or publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading, or uploading information and includes addresses, originators, and other persons jointly using the computer resource).

263 Intermediary Guidelines 2021 r. 2(1)(v).

264 Ministry of Electronics and Information Technology, Notification S.O. 942(E) dated 25 February 2021 <<https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf>> accessed 15 October 2021.

265 Ministry of Electronics and Information Technology (n 62). FAQ 12.

266 Intermediary Guidelines 2021 r. 2(1)(w).

267 Intermediary Guidelines 2021 r. 3(1).

268 Intermediary Guidelines 2021 r. 4(1).

269 Intermediary Guidelines 2021 r. 6(1).

270 Intermediary Guidelines 2021 r. 6(1).

271 Intermediary Guidelines 2021 r. 6(2).

Thus, the Union Government has created a new class of intermediaries (SSM Intermediaries), imposed additional obligations on this new class of intermediaries, and empowered itself to designate any intermediary as an SSM Intermediary through delegated legislation. The question of whether these measures are ultra vires the IT Act and its rule-making powers is subject to the earlier discussion on delegated legislation.²⁷²

272 See Section 4.1(ii) of this report.

(ii) Obligations vis-à-vis ‘prohibited content’

The Intermediary Guidelines 2021 require all intermediaries (including SSM Intermediaries) to put in place user agreements, rules, regulations, and privacy policies that inform their users not to “upload, display, modify, publish, store, share, or transmit” certain broad categories of content on the intermediary’s network.²⁷³ The October 2022 Amendment modifies this obligation, requiring intermediaries to “make reasonable efforts to cause the user” not to upload, transmit or store such content,²⁷⁴ and is discussed in section 4.5(ii) of this report. Under the Intermediary Guidelines 2021 the categories of ‘prohibited’ third-party content include:²⁷⁵

273 Intermediary Guidelines 2021 r. 3(1)(a), r.3(1)(b).

274 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, G.S.R. 794(E) dated 28 October 2022 [October 2022 Amendment], amendment to r. 3(1)(b).

275 Intermediary Guidelines 2021 r. 3(b).

- Content that belongs to another person and the uploader has no rights to;
- Content that contains a software virus or code that is designed to interrupt, destroy, or limit the functionality of a computer resource;
- Content that impersonates another person;
- Content that deceives or misleads the recipient about the origin of the message or knowingly communicates information which is patently false or misleading but may be reasonably be perceived as a fact (the October 2022 Amendment expressly uses the term “misinformation”²⁷⁶);
- Content that is patently false and untrue, and published with the intent to mislead the recipient for financial gain or to cause injury;
- Content that encourages money laundering or gambling;
- Content that infringes on any trademark, patent, copyright or other proprietary rights;

276 October 2022 Amendment, amendment to r. 3(1)(b).

- Content that is obscene, pornographic, paedophilic, invasive of another user’s privacy (including bodily privacy), insulting of other users on the basis of gender, racially or ethnically objectionable (‘defamatory and libellous’ content was part of the categories ‘prohibited’ content under the Intermediary Guidelines 2021, but has been removed by the October 2022 Amendment ²⁷⁷);
- Content that is harmful to children;
- Content that threatens the unity, integrity, defence, security, or sovereignty of India, friendly relations with foreign States, or public order, or insults any other nation, or causes the incitement of a serious offence or prevents the investigation of an offence; and
- Content that violates any Indian law.

277 October 2022 Amendment, amendment to r. 3(1)(b).

At least once a year, all intermediaries must inform their users of the relevant user agreements and policies, including changes to those agreements or policies,²⁷⁸ and that breach of the agreements and policies may result in the termination of a user’s access to the intermediary’s services.²⁷⁹ Under the current Guidelines, intermediaries are not compulsorily required to terminate users for a breach of the relevant user agreements.

278 Intermediary Guidelines 2021 r. 3(1)(f).

279 Intermediary Guidelines 2021 r. 3(1)(c).

The requirement to publish platform rules, privacy policies, and/or terms of use agreements informing users not to share unlawful content on the intermediary’s network existed under the Intermediary Guidelines 2011 as well.²⁸⁰ The requirement was largely enforced through self-regulation and neither the Intermediary Guidelines 2011 nor the 2021 Guidelines specify the exact form the user agreements should take. Courts have verified whether an online intermediary’s terms of service informed users not to upload unlawful content but have not provided a legal standard against which to evaluate the agreements,²⁸¹ indicating that the existence on record of such agreements is sufficient to satisfy the requirement under the Guidelines. However, merely because a user accepted an intermediary’s terms of use to not upload unlawful content does not itself absolve an intermediary of liability with respect to the unlawful content.²⁸²

280 Intermediary Guidelines 2011 r. 3(1), r. 3(2).

281 *Kunal Bahl v State of Karnataka* Cri (P) 4676 of 2020 (High Court of Karnataka, 7 January 2021) [12.7]; *Jitendra Singh Yadva v Union of India* WP (PIL) 4682 of 2015 (High Court of Madhya Pradesh, 16 February 2017) [26]; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [45]-[47]; *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201 [28]; *Flipkart Internet Pvt Ltd v State of NCT of Delhi* Writ Petition (Cri) 1376 of 2020 (High Court of Delhi, 17 August 2022) [26].

282 *Snapdeal Pvt Ltd v GoDaddy LLC* CS (Comm) 176 of 2021 (High Court of Delhi, 18 April 2022) [87].

Actual knowledge and judicial orders

The Intermediary Guidelines 2011 required an intermediary to take down ‘prohibited’ third-party content upon receiving a private complaint or risk losing safe harbour, creating the risks of horizontal censorship discussed previously.²⁸³ The Intermediary Guidelines 2021 codify the ‘judicial order and takedown’ regime set out in *Shreya Singhal*. Rule 3(1)(d) of the 2021 Guidelines requires an intermediary to take down content “*upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency*” under Section 79(3)(b) of the IT Act,²⁸⁴ failing which an intermediary loses its safe harbour. To preserve safe harbour, an intermediary must remove or disable access to the content within thirty-six hours of the court order or government notification.²⁸⁵ Thus, the Intermediary Guidelines 2021 formally bring regulation in line with the position laid down in *Shreya Singhal*, that an intermediary only risks losing safe harbour if it fails to take down content upon receipt of a court or government order. However, as discussed in section 4.5(ii), the October 2022 Amendment further modifies the ‘actual knowledge’ standard.

283 Section 4.1(iv) of this report.

284 Intermediary Guidelines 2021 r. 3(1)(d) (emphasis supplied).

285 Intermediary Guidelines 2021 r. 3(1)(d) (second proviso).

Complaints and notices to intermediaries

Rule 3(2) of the Intermediary Guidelines 2021 requires all intermediaries to set up a complaints mechanism²⁸⁶ and publish the contact details of a Grievance Officer.²⁸⁷ A user may also make a complaint regarding any other issue relating to the intermediary’s services, in which case the Grievance Officer shall acknowledge the complaint within twenty-four hours and dispose of the complaint within fifteen days of receipt.²⁸⁸ Finally, the Grievance Officer under Rule 3(2) is also tasked with receiving and acknowledging orders and directions from the government and courts.²⁸⁹

286 Intermediary Guidelines 2021 r. 3(2)(c).

287 Intermediary Guidelines 2021 r. 3(2)(a).

288 Intermediary Guidelines 2021 r. 3(2)(a)(i).

289 Intermediary Guidelines 2021 r. 3(2)(a)(ii).

Under the October 2022 Amendment to the Intermediary Guidelines 2021, intermediaries are legally required to ‘act on’ certain classes of content within seventy-two hours upon receipt of a complaint under Rule 3(2),²⁹⁰ and decisions of the Grievance Officer may be appealed to a government Grievance Appellate Committee.²⁹¹ This Amendment is discussed in detail in section 4.5(ii) of the report.

290 October 2022 Amendment, amendment to r. 3(2).

291 October 2022 Amendment, addition of r. 3A.

Data retention and cooperation

Under the Intermediary Guidelines 2021, where an intermediary collects any user information pursuant to a user’s registration on the intermediary’s platform, the intermediary must retain this information²⁹² for 180 days after the user withdraws or cancels their registration.²⁹³ Similarly, where an intermediary takes down content pursuant to a court order or government notification, a violation of its user agreements, or pursuant to a grievance raised by a user, the intermediary must preserve such content and associated records for investigative purposes for 180 days or as required by a government agency.²⁹⁴ Intermediaries must also render assistance to government agencies within seventy-two hours of receiving an order to cooperate, on the condition that the order clearly states why the government is seeking assistance or information.²⁹⁵ Assistance includes the sharing of information with government agencies for the verification of an identity, or the prevention, detection, investigation, or prosecution of an offence or cyber security incident.²⁹⁶

(iii) Uncertainty over Government’s power to block content

In addition to court orders, intermediaries are also required to remove content upon the issuance of a government notification, failing which they lose safe harbour.²⁹⁷ Section 79(3)(b) of the IT Act itself states that an intermediary is required to take down content if “*notified by the appropriate Government or its agency*” that its computer resource is being used to commit an unlawful act.²⁹⁸ In a non-legal response to ‘Frequently Asked Questions’ regarding the Intermediary Guidelines 2021, the MEITY stated that the order from the appropriate government would include: (i) specific URL(s) that needed to be taken down; (ii) the specific legal provision that the content violated; and (iii) the justification and evidence for the violation.²⁹⁹

Once an intermediary receives notice from the government or its agencies, it must take down the content within thirty-six hours or risk losing safe harbour protection.³⁰⁰ Neither the Intermediary Guidelines 2021 nor the decision in *Shreya Singhal* curtail the possibility that the government or its agencies may directly put intermediaries on notice under Section 79(3)(b) regarding potentially unlawful content, resulting in the content’s removal without judicial scrutiny.

292 Ministry of Electronics and Information Technology (n 62). FAQ 15. The MEITY has clarified that under the Intermediary Guidelines 2021, the intermediary is only required to retain the data collected at the time of registration, namely the location, time, and date stamp when the account was created.

293 Intermediary Guidelines 2021 r. 3(1)(h).

294 Intermediary Guidelines 2021 r. 3(1)(g).

295 Intermediary Guidelines 2021 r. 3(1)(j).

296 Intermediary Guidelines 2021 r. 3(1)(j).

297 Intermediary Guidelines 2021 r. 3(1)(d).

298 The Information Technology Act, 2000 s. 79(3)(b).

299 Ministry of Electronics and Information Technology (n 62). FAQ 14.

300 The Information Technology Act, 2000 s. 79(3)(b); Intermediary Guidelines 2021 r. 3(1)(d).

Section 79(3)(b) of the IT Act and Rule 3(1)(d) Intermediary Guidelines 2021 leave open the possibility that the government or law enforcement agencies may directly issue a notice to intermediaries with respect to potentially unlawful content, resulting in intermediaries either taking down the content or losing safe harbour protection. Noting that identical language existed under the Intermediary Guidelines 2011, the MEITY has even stated that there is “*a clear and existing practice in relation to orders of law enforcement or Appropriate Government authorities*” when discussing Section 79(3)(b) and Rule 3(1)(d).³⁰¹

Separately, Section 69A of the IT Act also grants the Union Government the power to ‘block’ content on the internet in specific situations.³⁰² Section 69A may only be invoked where the Union Government is satisfied that it is necessary to block content in the interests of public order, the sovereignty, integrity, defence or security of India, to maintain friendly relations with foreign States, or to prevent the incitement of a serious offence.³⁰³ Additionally, when the Union Government issues an order to block content under Section 69A, it is obligated to notify and give a hearing to the intermediary or originator³⁰⁴ (although it may circumvent this requirement in emergencies,³⁰⁵ and evidence suggests hearings do not occur in practice³⁰⁶). The power and practice of website blocking by the Union Government under Section 69A is analysed more thoroughly in section 8 of this report.

In the past, the Union Government has referred to both Section 69A and 79(3)(b) of the IT Act as the source of its power to restrict content. For example, in a Union Government order from 2015, the Department of Telecommunications expressly cited Section 79(3)(b) when directing ISPs to disable access to 857 websites allegedly hosting pornography.³⁰⁷ But other orders of the Union Government refer to Section 69A of the IT Act as the source of its power to restrict content.³⁰⁸

As a result of this, there remains a lack of clarity as to the exact legal basis the government relies on to block content under the IT Act. It remains unclear whether Section 79(3)(b) constitutes an avenue independent of Section 69A for the government to restrict content.³⁰⁹ This is relevant as Section 69A imposes some restraints on the Union Government’s power to block content. Section 69A has certain threshold criteria (e.g., defence of India or public order) and requires the originator or intermediary be heard prior to content being restricted. The Supreme Court in *Shreya Singhal* stated that

301 Ministry of Electronics and Information Technology (n 62), FAQ 14. It is relevant to note that these statements make no reference to Section 69A of the IT Act.

302 The Information Technology Act, 2000 s. 69A.

303 *ibid* s. 69A(1).

304 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 G.S.R. 781(E) dated 27 October 2009 r. 8(1).

305 *ibid* r. 9.

306 Apar Gupta, ‘But What about Section 69A?’ *The Indian Express* (27 March 2015) <<https://indianexpress.com/article/opinion/columns/but-what-about-section-69a/>> accessed 3 March 2021.

307 Department of Telecommunications, No. 813-7/25/2011-DS (Vol.V), Communication dated 31 July 2015 <https://cis-india.org/internet-governance/resources/dot-morality-block-order-2015-07-31/at_download/file> accessed on 15 October 2021.

308 Anuj Srivas, ‘Understanding the Nuances to Twitter’s Standoff With the Modi Government’ *The Wire* (12 February 2021) <<https://thewire.in/tech/twitter-modi-government-block-section-69-a>> accessed 11 July 2021.

309 The decision in *Shreya Singha* treats Section 69A and Section 79 of the IT Act as operating independently but does not discuss the requirements a government notification would have to satisfy under Section 79 of the IT Act under than having to conform to Article 19(2) of the Constitution. The primary issue before the Court was whether the take down of content pursuant to a private complaint was permissible.

government orders must strictly conform to Article 19(2) of the Indian Constitution.³¹⁰ Unlike Section 69A,³¹¹ neither Section 79(3) of the IT Act or Rule 3(1)(d) of the Intermediary Guidelines 2021 provide any process to review or contest the government order, compelling individuals to approach courts after content has been taken down, by which time the value of the content may be significantly reduced. However, it is important to note that non-compliance with Section 69A can result in penal consequences for intermediaries,³¹² while non-compliance with a notification under Section 79(3) would only result in the loss of safe harbour.

Section 69A of the IT Act only allows the Union Government to block content.³¹³ However, under Section 79(3)(b), a takedown notification may be issued by the “*appropriate Government or its agency*”.³¹⁴ Section 2(1)(c) of the IT Act defines the “*appropriate Government*” as the Union Government, but also a State Government in respect to (i) anything set out in List II (State List) of the Seventh Schedule of the Constitution; or (ii) anything concerning a State law passed under List III (Concurrent List) of the Seventh Schedule of the Constitution.³¹⁵ List II contains several items that may cause a State Government to claim it is the appropriate government and request the removal of content, including public order,³¹⁶ elections to the state legislature,³¹⁷ and cinemas.³¹⁸ Examining select government requests disclosed by Google reveals that in addition to the Union Government, police authorities from various Indian States also send removal requests, and Google complies with at least some of these requests.³¹⁹ Thus, if Section 79(3)(b) of the IT Act represents an avenue independent of Section 69A to remove content, the power to censor content online may be extended to State Governments and their agencies in certain situations.

Recently, the text of the government orders has also not proved instructive. For example, prior to 2020, disclosures of government requests to Twitter uploaded on the Lumen transparency database indicated that content was taken down pursuant to Section 69A of the IT Act. However, since 2020, Lumen disclosures merely state that content had been ‘removed pursuant to the provisions of the IT Act’.³²⁰ This concern is accentuated as the limited disclosures by intermediaries’ evidence that the government blocks content more than courts. For example, in 2018 Google received 2,474 requests to restrict access to content, of which only 153 were from the judiciary.³²¹

310 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [122].

311 For an overview of the procedures for blocking content, refer to Section 8.1 of this report.

312 The Information Technology Act, 2000 s. 69A(3).

313 The Information Technology Act, 2000 s. 69A(1).

314 *ibid* s. 79(3)(b).

315 *ibid* s. 2(1)(e).

316 Constitution of India, 1950 sch. 7 list II Item 1.

317 *ibid* sch. 7 list II Item 37.

318 *ibid* sch. 7 list II Item 33.

319 Google India, ‘Government Requests to Remove Content – Google Transparency Report’ <https://transparencyreport.google.com/government-removals/government-requests/IN?hl=en&lu=country_request_explore&country_request_explore=p:3> accessed 3 May 2022.

320 Srivas (n 308).

321 Google India (n 319).

Once an intermediary receives notice from the government or its law enforcement agencies under Section 79(3)(b), it has thirty-six hours to either take down the content or find itself in breach of the Intermediary Guidelines. The possibility that the government and law enforcement agencies can compel intermediaries to take down content, with the threat of stripping intermediaries of safe harbour without any safeguards, significantly skews the government-intermediary axis in favour of government control over intermediaries, and consequently over online speech. This is particularly relevant given the number of criminal speech offences in India,³²² raising the risk of criminal speech prosecutions as a result of hosting unlawful speech initiated and conducted by State authorities. As discussed above, the lack of transparency surrounding government blocking is a significant challenge to a thorough analysis of both Section 69A and 79(3)(b) of the IT Act.

(iv) Express recognition of content moderation

The Intermediary Guidelines 2021 expressly note that if an intermediary removes ‘prohibited’ third-party content from its network “*on a voluntary basis*”, it shall not amount to a breach of the conditions of Sections 79(2)(a) and 79(2)(b) of the IT Act.³²³ Given the broad definition of ‘prohibited’ third-party content,³²⁴ intermediaries have substantial discretion to remove a wide range of content on their platforms while continuing to satisfy the requirements of Sections 79(2)(a) and 79(2)(b).

This is akin to the ‘Good Samaritan’ protections provided under Section 230 of the Communications Decency Act in the United States,³²⁵ which ensures that intermediaries retain their safe harbour when they voluntarily moderate content in good faith on their platform. However, unlike Section 230, the Intermediary Guidelines 2021 do not require that voluntary takedowns be done in good faith, rather Rule 3(1)(b) of the Intermediary Guidelines prescribes broad categories of ‘prohibited’ content that intermediaries may voluntarily remove. This is relevant, as the Union Government has itself prescribed certain speech rules; and incentivising intermediaries to moderate *more* does not necessarily ensure that they will moderate *better*.³²⁶ While the freedom to moderate content is essential to the functioning of most modern intermediaries, certain safeguards may need to be placed to ensure the quality and accountability of the moderation.

In India, it can be argued that both Section 79(2)(b) and the

322 Section 4 of this report.

323 Intermediary Guidelines 2021 r. 3(1)(d) (third proviso). See also Section 4.1(ii) of this report on ‘neutrality’ under Section 79(2).

324 For the definition of ‘prohibited third-party content’ see Section 4.3(ii) of this report.

325 Communications Decency Act 47 U.S.C. s. 230(c) (1996). (“No provider or user of an interactive computer service shall be held liable on account of – (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected”).

326 See Aleksandra Kuczerawy, ‘The Good Samaritan That Wasn’t: Voluntary Monitoring under the (Draft) Digital Services Act’ (*CITIP blog (KU Leuven)*, 14 January 2021) <<https://www.law.kuleuven.be/citip/blog/the-good-samaritan-that-wasnt/>> accessed 20 October 2021.

2011 Guidelines created a situation where intermediaries were disincentivised from voluntary content moderation, as any exercise of control of content may be interpreted as them breaching the neutrality requirements of Section 79(2)(b) and losing safe harbour.³²⁷

Furthermore, prior to *Shreya Singhal*, exercising editorial control may be construed as having ‘knowledge’ of specific unlawful content, and thus intermediaries risked liability by breaching Section 79(3)(b) of the IT Act if they *failed* to take down the specific unlawful content. In other words, by not protecting voluntary takedown of content by intermediaries, Section 79 and the

2011 Guidelines could be construed as created a regime where intermediaries must either exercise no editorial control or exercise editorial control perfectly to the point where no unlawful content was on their platform.³²⁸ However, content moderation is central to the business and experience of large social media companies and there is no evidence that online platforms stopped moderating content in India despite these legal uncertainties.³²⁹ Additionally, at the time of writing this report, no court has ruled that the content moderation activities of an intermediary violated the neutrality required of Section 79(2)(b).

This issue of content moderation was largely mitigated by the decision in *Shreya Singhal*. By ruling that intermediaries only had “*actual knowledge*” of unlawful content when served with a court order, the Supreme Court opened the door for intermediaries to engage in voluntary content moderation without the associated risk of being deemed to ‘know’, for the purposes of Section 79(3)(b), of unlawful content. However, the ambiguity between voluntary content moderation and the satisfaction of conditions set out under Section 79(2)(b) remained until the adoption of the express protections in Rule 3(1)(d) of the Intermediary Guidelines 2021. As noted earlier, this is partly a result of Section 79 not clearly distinguishing between ‘mere conduits’ and ‘hosting’ providers.³³⁰

327 Under Section 79(2)(b) of the IT Act, an intermediary other than a mere conduit cannot claim safe harbour if it has: (i) initiated the transmission; (ii) selected the receiver of the transmission; and (iii) selected or modified the information contained in the transmission. Content moderation would breach this third requirement.

328 See Rahul Matthan, ‘Opinion | Shield Online Platforms for Content Moderation to Work’ (*mint*, 2 June 2020) <<https://www.livemint.com/opinion/columns/shield-online-platforms-for-content-moderation-to-work-11591116270685.html>> accessed 13 September 2021.

329 See Prasad Banerjee, ‘Inside the Secretive World of India’s Social Media Content Moderators’ (*mint*, 18 March 2020) <<https://www.livemint.com/news/india/inside-the-world-of-india-s-content-mods-11584543074609.html>> accessed 5 October 2021.

330 Section 4.1(ii) of this report.

The issue of neutrality under Section 79(2)(b) is exacerbated by the fact that the requirements for safe harbour under Sections 79(2) and 79(3) of the IT Act are conjunctive. If a judge opined that content moderation activities constituted ‘modifying or interfering with content’, a court could have ruled that irrespective of the question of a court order/actual knowledge, a platform’s content moderation violated Section 79(2) and disqualified it from safe harbour. However, courts in India have not taken this view, suggesting that either they do not view content moderation as violating Section 79(2)(b) or they are yet to substantively engage with the tension between the modern-day reality of moderation and the requirements of Section 79(2) of the IT Act. One reason for the lack of judicial commentary on the subject may be that the primary focus of plaintiffs approaching courts in India is to take down or injunct content, with the actual imposition of liability and securing damages from the intermediary a distant secondary consideration to be determined after a full trial. These interim hearings primarily centre on speech harm vs. free speech, and full trials with exhaustive examinations of an intermediary’s functionality are yet to be concluded.

Transparency in content moderation

Unaccountable private moderation may also give rise to private censorship to the extent that intermediaries restrict the speech of internet users.³³¹ As noted in section 4.2(ii) of this report, content moderation may set up systems of “*private governance*” where social media companies struggle to consistently and transparently moderate content.³³² Private systems of content moderation raise rule of law concerns as they mix elements of norm setting, law enforcement, and adjudication, and may result in the censoring of lawful speech, potentially impacting certain groups disproportionately.³³³ Thus, as noted in section 4.2(ii), it is desirable to ensure that users are provided safeguards along the user-intermediary axis to guard against arbitrary or even discriminatory conduct by platforms.

Early reports from Facebook, Instagram, and Google under Rule 4(1)(d) of the Intermediary Guidelines 2021 indicate that all three platforms take down substantially more content voluntarily and proactively as compared to takedowns pursuant to user complaints.³³⁴ For example, in July 2021, Google removed 95,680 pieces of content pursuant to user complaints and removed 576,982 pieces voluntarily as part of its proactive detection

331 Klonick (n 255).

332 Section 4.1(ii) of this report.

333 Niva Elkin-Koren and Maayan Perel, ‘Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law’ in Giancarlo Frosio (ed), Niva Elkin-Koren and Maayan Perel, Oxford Handbook of Online Intermediary Liability (Oxford University Press 2020) 672.

334 Google India, ‘Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Monthly Transparency Report’ (2021) <https://storage.googleapis.com/transparencyreport/report-downloads/india-intermediary-guidelines_2021-7-1_2021-7-31_en_v1.pdf> accessed 18 October 2021; Facebook, ‘Facebook India Monthly Report August 31 2021’ (2021) <<https://transparency.fb.com/sr/india-monthly-report-august-2021/>>.

processes.³³⁵ Facebook’s report differs slightly, by providing a “Proactive Rate” for different classes of content to indicate the percentage of content that was ‘acted on’ (either removed or qualified by a warning) before a user complaint.³³⁶ According to Facebook’s report, around 33.3 million pieces of content were ‘actioned against’ between June 16 and July 31, 2021.³³⁷ In cases of bullying and harassment, only 42% of content was proactively acted on by Facebook before user reports, while in the cases of Nudity, Violent and Graphic Content, and Spam, the ‘Proactive Rate’ was above 99%.³³⁸

While these reports provide evidence of the scale of content moderation in India, they do not provide insight into the quality of moderation being undertaken.³³⁹ This problem has been aggravated by the MEITY’s (albeit non-legal) clarificatory statements that reports by SSM Intermediaries need not adhere to a prescribed format and need only provide: (i) the subject area of complaints received, and action taken; and (ii) the number of links removed voluntarily.³⁴⁰ Reporting on removal volumes cannot determine whether lawful content was taken down pursuant to proactive tools.³⁴¹ Further, the reports do not disclose situations where users have sought content reinstatement.³⁴² Some scholars have suggested ‘tinkering’ as providing a more accurate assessment of content moderation systems, whereby researchers upload samples of content and evaluate how platforms’ algorithmic and human moderation systems respond to it.³⁴³

Granting online intermediaries increased power to take down content voluntarily may also lead to increased government interference in online speech. Research shows that governments often ‘informally collaborate’ with intermediaries,³⁴⁴ subtly lobbying platforms to take down content.³⁴⁵ The Indian government regularly applies extra-legal pressure to print and broadcast journalists,³⁴⁶ and close ties between senior Facebook employees and India’s Prime Minister have led to accusations that the platform acted in a partisan manner by failing to ban members of the ruling party.³⁴⁷ In a similar vein, Google officials suggested to the Indian Government that it keep take down requests confidential to avoid the negative publicity associated with speech restrictions.³⁴⁸ While State authorities are subject to constitutional constraints, informal pressure (through threats of fines, bans, or adverse policy decisions) on unaccountable and unconstrained private platforms can lead to significant censorship outside the rule of law.³⁴⁹

335 Google India (n 334).

336 Facebook (n 334).

337 *ibid.*

338 *ibid.*

339 Vasudev Devadasan, ‘Compliance Reports by Social Media Platforms Are Unhelpful’ *MediaNama* (18 April 2022) <<https://www.medianama.com/2022/04/223-transparency-reports-social-media-platforms-unhelpful/>> accessed 27 April 2022.

340 Ministry of Electronics and Information Technology (n 62). FAQ 20.

341 *See* McGonagle (n 254) 483.

342 Devadasan (n 339).

343 Elkin-Koren and Perel (n 333) 676.

344 *ibid* 673.

345 Klonick (n 255) 1650.

346 Vindu Goel and Jeffrey Gettleman, ‘Under Modi, India’s Press Is Not So Free Anymore’ *The New York Times* (2 April 2020) <<https://www.nytimes.com/2020/04/02/world/asia/modi-india-press-media.html>> accessed 20 October 2021; Hartosh Singh Bal, ‘How the Media Becomes an Arm of the Government’ [2020] *The Caravan* <<https://caravanmagazine.in/media/media-becomes-government-modi-indian-express-republic>> accessed 12 October 2021.

347 Jeff Horwitz and Newley Purnell, ‘Facebook Executive Supported India’s Modi, Disparaged Opposition in Internal Messages’ *Wall Street Journal* (30 August 2020) <<https://www.wsj.com/articles/facebook-executive-supported-indias-modi-disparaged-opposition-in-internal-messages-11598809348>> accessed 12 October 2021; Newley Purnell and Jeff Horwitz, ‘Facebook’s Hate-Speech Rules Collide With Indian Politics’ *Wall Street Journal* (14 August 2020) <<https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346>> accessed 12 October 2021.

348 Sarvesh Mathi, ‘Is the Government as Open about Content Takedown Orders as It Claims?’ *MediaNama* (3 February 2022) <<https://www.medianama.com/2022/02/223-government-content-takedown-fake-news/>> accessed 27 April 2022.

349 *See* Elkin-Koren and Perel (n 333) 671.

(v) Takedown of intimate images

Rule 3(1)(d) of the Intermediary Guidelines 2021 codifies the ‘judicial order and takedown’ regime laid down in *Shreya Singhal*. But where a user complains of sexually explicit content that depicts the user in a state of nudity or engaged in a sexual act, Rule 3(2)(b) sets up a more traditional ‘notice and takedown’ regime. Intermediaries will lose their safe harbour if they fail to remove (on a best efforts-basis) such content once a user complains against it, contrary to the approach stipulated in *Shreya Singhal*.

A user may utilise an intermediary’s complaint mechanism under Rule 3(2)(b) to lodge a complaint against any content which *prima facie* depicts the private area of the complainant, shows the complainant in a state of partial or complete nudity, or depicts the complainant engaging in a sexual act or conduct, including where such content impersonates the complainant using morphed images.³⁵⁰ The MEITY characterised the content targeted by this rule as “*revenge porn and similar content breaching physical privacy*”.³⁵¹ Upon receipt of a complaint, the intermediary shall take “*all reasonable and practicable measures*” to disable access to such content within twenty four hours.³⁵²

One possible rationale is that the intimate and potentially non-consensual nature of the content/upload may necessitate a speedier removal procedure,³⁵³ and the speech value of such content may also be limited. When announcing the Intermediary Guidelines 2021, the Union Government’s Press Information Bureau stated that the “*Rampant abuse of social media to share morphed images of women and contents related to revenge porn have often threatened the dignity of women.*”³⁵⁴ Another aspect is costs. Reddy criticised the decision in *Shreya Singhal* as transferring the costs of taking down content from intermediaries to potentially injured parties,³⁵⁵ as these parties would have to incur the costs of obtaining a judicial takedown order. In the case of intimate images and nudity, Rule 3(2)(b) removes the costs and time of having to get a court order.

Historically, notice and takedown regimes without any safeguards have been open to abuse and resulted in over-compliance by intermediaries.³⁵⁶ Rule 3(2)(b) raises similar concerns as there exists no process for verifying that the content depicts the same individual making the complaint. This creates a risk of abuse by third-party internet users who may merely find sexually explicit

350 Intermediary Guidelines 2021 r. 3(2)(b).

351 Ministry of Electronics and Information Technology (n 62). FAQ 5.

352 Intermediary Guidelines 2021 r. 3(2)(b).

353 Kuczerawy (n 197) 527–528. Noting that a key advantage of a notice and takedown procedure is its speed.

354 ‘Government Notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021’ (25 February 2021) <<https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1700749>> accessed 14 September 2021.

355 Reddy (n 171) 50.

356 Dara (n 195).

content offensive. For example, to counter this risk, under the Digital Millennium Copyright Act in the United States complainants are required to state that the contents of the notification to an intermediary are accurate under a penalty of perjury.³⁵⁷ In fact, the Supreme Court in *Shreya Singhal* tied the potential abuse of private complaints to intermediaries being compelled to make private censorial decisions as to which complaints were legitimate.³⁵⁸

357 Digital Millennium Copyright Act 17 U.S.C. s. 512(c)(3)(vi) (1998).

358 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [122].

Rule 3(2)(b) is not narrowly tailored to the removal of non-consensual intimate images. Unlike Section 66E of the IT Act, Rule 3(2)(b) does not use the term ‘without consent’ or ‘in circumstances violating privacy’ (essential to any definition of non-consensual intimate images). Thus, Rule 3(2)(b) could be utilised to force intermediaries to remove (at the risk of losing safe harbour) mere nudity or sexual content that deviates from traditional societal mores without any judicial oversight. The lack of a clear definition of non-consensual intimate images and videos also raises the scope for disagreement and litigation. In a recent case before the High Court of Delhi, a complainant consented to be recorded in a state of nudity during an acting audition, but the video was eventually uploaded against their will.³⁵⁹ Resisting the takedown of the video, certain respondent intermediaries argued that the IT Act permitted the dissemination of content in the interests of art and literature, and as the disputed video was taken for artistic purposes, it was excluded from the application of Rule 3(2)(b).³⁶⁰ The High Court rejected this reasoning, noting that the existence of sexually explicit material concerning the complainant was sufficient to invoke the applicability of Rule 3(2)(b).³⁶¹ While the content in this case warranted being taken down, this dispute highlights the tensions raised by Rule 3(2)(b). Finally, even where a complaint is initiated by the person depicted in the content, there may exist free speech interests in keeping the content online (e.g., where the individual depicted is a public figure, or where the content depicts a second person who wishes to keep the content online). These risks to lawful content being taken down may also be heightened due to the short timeline provided to take down content (twenty-four hours)³⁶² and, in the case of SSM Intermediaries, the personal liability imposed on officers for violations of the Guidelines.³⁶³

359 *X v YouTube* CS (OS) 392 of 2021 (High Court of Delhi, 23 August 2021) [7].

360 *ibid* [13].

361 *ibid* [14].

362 Intermediary Guidelines 2021 r. 3(2)(b).

363 Intermediary Guidelines 2021 r. 4(1)(a).

Crucially, Rule 3(2)(b) has no procedure under which content may be reinstated or an intermediary can insist on a court order. For example, under the Copyright Act, content must also be taken down pursuant to a complaint (at the risk of losing safe harbour).

However, crucial safeguards exist. First, the complainant must demonstrate they are the owner of the content³⁶⁴ and that the content infringes their copyright.³⁶⁵ Second, while the intermediary must take down the content expeditiously, the complainant must approach a court and secure a favourable order within twenty-one days.³⁶⁶ If the complainant fails to secure a court order within this timeframe, the intermediary may reinstate the content.³⁶⁷ Similar safeguards are absent in Rule 3(2)(b) of the Intermediary Guidelines 2021. However, admittedly, ultimately requiring a court order does not solve the issue of costs.

Rule 3(2)(b) of the Intermediary Guidelines 2021 operates on the internet user-intermediary axis, offering users a speedy out-of-court process to take down intimate images of themselves on the internet. However, in its current iteration, the Rule is contrary to the decision in *Shreya Singhal*, and creates the risks to free speech ordinarily associated with notice and takedown regimes, most notably, a regime of horizontal censorship operationalised by over-compliant intermediaries that zealously take down content under the threat of liability. While most of the content complained against may be *ex-facie* illegal, the existence of borderline cases and abusive complaints under Rule 3(2)(b) may result in the suppression of some protected speech. The operation of Rule 3(2)(b), especially in cases raising competing interests, will have to be monitored closely to understand the need for additional safeguards.

364 The Copyright Act, 1957 s. 52(1)(c); The Copyright Rules, 2013 G.S.R. 172(E) dated 14 March 2013 [Copyright Rules] r. 75(2)(b).

365 Copyright Rules r. 75(2)(c).

366 The Copyright Act, 1957 s. 52(1)(c).

367 *ibid.*

4.4. Intermediary Guidelines 2021: Rule 4

In addition to the due diligence obligations imposed on all intermediaries under Rule 3, SSM Intermediaries must satisfy ‘additional due diligence’ obligations under Rule 4 of the Intermediary Guidelines 2021.³⁶⁸ SSM Intermediaries must have a physical contact address in India.³⁶⁹ They must also appoint a Chief Compliance Officer, a Resident Grievance Officer, and a nodal contact person.³⁷⁰ The Chief Compliance Officer is responsible for ensuring the intermediary is in compliance with the IT Act and its subsidiary regulation (including the Intermediary Guidelines 2021), and shall be liable for any ‘prohibited’ third-party information hosted or made available by the intermediary.³⁷¹ However, no liability shall be imposed without the SSM Intermediary being given a hearing.³⁷² In a non-legal response to queries, the MEITY clarified that an SSM Intermediary offering multiple services in India (e.g., Facebook offers Facebook, Messenger, WhatsApp, and Instagram) may appoint one common officer across services.³⁷³ SSM Intermediaries are also required to ‘monthly compliance reports’ documenting the number of complaints received and actions taken in response, and the volume of content removed pursuant to any ‘proactive monitoring conducted using automated tools’.³⁷⁴ These reports are discussed in section 4.3(iv) of this report under the sub-heading ‘Transparency of Content Moderation’.

A SSM Intermediary is required to clearly identify and distinguish content on its platform as ‘advertised, marketed, sponsored, owned, or exclusively owned’, where: (i) the SSM Intermediary derives a direct financial benefit from the increase in the visibility or targeting of receivers of the content on its platform; or (ii) the SSM Intermediary owns a copyright or exclusive license or has exclusive control over the dissemination of content.³⁷⁵ SSM Intermediaries shall also provide Indian users who voluntarily verify their accounts with a “*demonstrable and visible mark of verification*” that all other users on the platform can see,³⁷⁶ allowing users to distinguish ‘verified’ accounts from ‘unverified’ accounts. Users can ‘verify’ themselves using any “*appropriate mechanism, including the active Indian mobile number of such users*”.³⁷⁷

(i) Proactive filtering

Rule 4(4) of the Intermediary Guidelines 2021 stipulates that SSM Intermediaries “*shall endeavour to deploy technology-based measures, including automated tools*” to proactively identify content that:

368 Intermediary Guidelines 2021 r. 4(1).

369 Intermediary Guidelines 2021 r. 4(5).

370 Intermediary Guidelines 2021 r. 4(1)(a), r. 4(1)(b), r. 4(1)(c).

371 Intermediary Guidelines 2021 r. 4(1)(a).

372 Intermediary Guidelines 2021 r. 4(1)(a).

373 Ministry of Electronics and Information Technology (n 62). FAQ 19.

374 Intermediary Guidelines 2021 r. 4(1)(d).

375 Intermediary Guidelines 2021 r. 4(3).

376 Intermediary Guidelines 2021 r. 4(7).

377 Intermediary Guidelines 2021 r. 4(7).

(i) implicitly or explicitly depicts rape or child sexual abuse; or (ii) is “exactly identical” to content that has been disabled pursuant to a court order or government notice under Rule 3(1)(d).³⁷⁸ Where such content is identified, SSM Intermediaries must display a notice to users attempting to access the content, stating that the content has been disabled and the reasons for the content being disabled.³⁷⁹

Rule 4(4)’s obligation to proactively filter is qualified by three conditions that aim to provide safeguards against lawful content being taken down. First, the measures taken by SSM Intermediaries “shall be proportionate having regard to the interests of free speech and expression” and the privacy of users.³⁸⁰ Second, SSM Intermediaries are required to implement “mechanisms for appropriate human oversight” including a periodic review of the intermediary’s use of automated tools.³⁸¹ Third, the automated tools are to be evaluated with respect to their “accuracy and fairness”, their “propensity for bias and discrimination”, and the impact on the privacy of users.³⁸² SSM Intermediaries are also required to publish a monthly compliance report detailing the complaints they have received and their responses, including the details of content taken down using ‘proactive automated tools’.³⁸³ These reports are discussed in section 4.3(iv) of this report under the sub-heading ‘Transparency of Content Moderation’.

Since the obligation to use automatic filtering is qualified by the terms “shall endeavour”, the steps to be taken by an intermediary to satisfy this obligation remain unclear. Further, Rule 4(4) does not set out a standard of efficacy required of these automated systems. Thus, it remains to be seen if an SSM Intermediary will be held liable for failing to implement an automated system; and, if such a system is implemented, when an intermediary may be liable for the ‘failure’ of such a system to identify unlawful content.

Requiring SSM Intermediaries to *proactively* identify and take down certain types of suspect content using automated systems undermines the requirement for an *ex-ante* judicial balancing of rights enshrined in Rule 3(1)(d) and the *Shreya Singhal* decision. In other words, by requiring SSM Intermediaries to engage in the identification and removal of unlawful content (at the risk of losing safe harbour), Rule 4(4) requires them to remove content prior to receiving a court or government order. Although Rule 4(4) does not expressly require SSM Intermediaries to screen and block content prior to its publication, the risk of losing safe harbour due to a failure to ‘proactively identify’ content may cause intermediaries

378 Intermediary Guidelines 2021 r. 4(4).

379 Intermediary Guidelines 2021 r. 4(4).

380 Intermediary Guidelines 2021 r. 4(4) (first proviso).

381 Intermediary Guidelines 2021 r. 4(4) (second proviso).

382 Intermediary Guidelines 2021 r. 4(4) (third proviso).

383 Intermediary Guidelines 2021 r. 4(1)(d).

to make both hasty and overly cautious decisions overlooking the informational value of the content. For example, Facebook’s filter against ‘nudity’ was responsible for taking down the image of Phan Thi Kim Phuc fleeing a Napalm attack during the Vietnam War, an iconic piece of war imagery that stimulated public debate over the conflict.³⁸⁴ However, it must also be acknowledged that most large platforms already employ proactive automated filters to remove certain classes of content. However, they do so voluntarily and there is no risk of losing safe harbour if such filters are found to not be effective enough.

Incentivising SSM Intermediaries to proactively identify depictions of rape and child sexual abuse are compelling governmental objectives. However, the inherent imprecision of these suspect classes and the contextual nature of content means that where liability is imposed for failure to *prevent* unlawful content being published, intermediaries may over-comply and take down lawful content.³⁸⁵ This is aggravated by the requirement that SSM Intermediaries also filter content identical to content which was *previously taken down* under Rule 3(1)(d). This creates an ever-expanding set of hyper-individualised suspect classes of content, which may be even more broadly defined than the already general ‘depictions of rape and child sexual abuse’.³⁸⁶ For similar reasons, the German NetzDG law – which originally required intermediaries to prevent future uploads of content that was similar to content which had been blocked once – dispensed with this requirement due to concerns of over-blocking by imprecise upload filters.³⁸⁷

The requirement that intermediaries display a notice to users indicating why the content has been restricted offers users a measure of transparency. However, requiring intermediaries to proactively identify unlawful user content requires intermediaries to monitor user posts and messages, which may also undermine user privacy.³⁸⁸ If imposed strictly, the net effect of the Rule will be to create a general monitoring obligation on intermediaries. A general monitoring obligation can be said to exist where intermediaries are required to install a system of filtering content: (i) stored by users on its platform; (ii) which is indiscriminately applicable to all users; (iii) as a preventive measure; (iv) exclusively at the intermediary’s expense; (v) for an unlimited period; (vi) to identify suspect classes of content.³⁸⁹ General monitoring obligations, as inherently disproportionate, are impermissible under the European E-Commerce Directive,³⁹⁰ as they require the screening of all content irrespective of the subject matter or

384 ‘Fury over Facebook “Napalm Girl” Censorship’ *BBC News* (9 September 2016) <<https://www.bbc.com/news/technology-37318031>> accessed 11 March 2021.

385 Medeiros and Singh, ‘Addressing Misinformation on Whatsapp in India Through Intermediary Liability Policy, Platform Design Modification, and Media Literacy’ (2020) 10 *Journal of Information Policy* 276; Balkin (n 165) 1176.

386 Courts also regularly pass broadly worded take down orders, often relying on lists of URLs provided by plaintiffs without any independent verification of the content on these webpages. For a detailed analysis of the content of court orders, refer to Section 7 of this report.

387 Wolfgang Schulz, ‘Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG’ [2018] *HIIG Discussion Paper Series* <<https://ssrn.com/abstract=3216572>>. The German law required intermediaries to take down ‘obviously illegal’ content. Schulz notes that the obligation to ensure that once content was taken down, similar content was not uploaded again was removed from the German law as it ‘triggered fears of over-blocking since the most effective way of doing this is by using upload filters, which – at their current state of development – fail to detect irony or critical references to content’.

388 Geiger, Frosio and Izyumenko (n 199) 148; Software Freedom Law Centre, ‘The Future of Intermediary Liability in India’ (n 247).

389 Frosio and Mendis (n 225) 561.

390 Directive 2000/31/EC of 8 June 2000 on electronic commerce, Art. 15.

user – effectively examining the content of all users to identify illegal activity amongst some users. Indian courts have also made observations critical of the imposition of such obligations.³⁹¹

Although the three provisos to Rule 4(4) contains language regulating the use of automated systems, from the perspective of the internet user-intermediary axis, the only opportunity a user has to contest the decision of such an automated system is under the Rule 4(8) dispute settlement mechanism, or an appeal to the government appointed Grievance Appellate Committee, the flaws of which have been discussed below.³⁹² Within the regulatory structure of the IT Act, it is unclear how the legality of such automated systems will be ensured or monitored on an ongoing basis. There remains uncertainty as to the extent to which algorithmic systems are capable of being effectively regulated,³⁹³ and under the Intermediary Guidelines 2021, there exists no regulatory body to whom this task is assigned. Reporting requirements that focus on the *amount* of content taken down (as required under Intermediary Guidelines 2021), but that do not disclose the process and criteria used to make such decisions are of limited value.³⁹⁴ These observations also apply to the requirement that SSM Intermediaries evaluate the ‘fairness’ and ‘bias’ of automated tools. Thus, while facially attractive, the three provisos to Rule 4(4) may not significantly alter the power imbalance between online platforms and internet users in the context of automated systems.

(ii) Accountability and dispute resolution

In addition to the complaints mechanisms for the sexual depictions of users that all intermediaries are obligated to set up under Rule 3(2)(b), SSM Intermediaries must allow such complainants to track the status of their complaints by assigning every complaint a unique ticket number.³⁹⁵ SSM Intermediaries shall also, “*to the extent reasonable*”, inform complainants of the reasons for any action taken or not taken in response to a complaint.³⁹⁶ The stated goal is for the complainant to understand how their complaint has been handled by the Intermediary’s Resident Grievance Officer, but according to the MEITY’s non-legal clarifications, SSM Intermediaries are permitted to devise their own systems of due process.³⁹⁷ These clarifications also note that in the case a of frivolous complaint, SSM Intermediaries may cite the nature of the complaint as a reason for dismissing it.³⁹⁸

391 *UTV Software Communications Ltd v 1337x CS* (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019); *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382; *Dept of Electronics and Information Technology v Star India Pvt Ltd* FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016).

392 See Section 4.5(ii) of this report.

393 See Ben Wagner, ‘Algorithmic Accountability: Towards Accountable Systems’ in Giancarlo Frosio (ed), Ben Wagner, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).

394 McGonagle (n 254) 483.

395 Intermediary Guidelines 2021 r. 4(6).

396 Intermediary Guidelines 2021 r. 4(6).

397 Ministry of Electronics and Information Technology (n 62). FAQ 21.

398 *ibid.*

Where an SSM Intermediary itself voluntarily restricts third-party content for violating its user agreements or policies, the SSM Intermediary shall: (i) provide the user who uploaded or shared the content a notification explaining why the content was disabled; and (ii) grant the concerned user an “adequate and reasonable opportunity to dispute the action” taken by the SSM Intermediary.³⁹⁹ The SSM Intermediary’s Resident Grievance Officer shall oversee the mechanism for dispute resolution.⁴⁰⁰ According to the MEITY’s non-legal clarifications, this obligation only applies to situations where an SSM Intermediary concludes the content violates a law or removes content pursuant to the established grievance redressal mechanism.⁴⁰¹ Crucially, the MEITY’s clarifications state that this due process obligation does not apply to cases where: (i) the SSM Intermediary removes content using automated filters; (ii) is of the opinion the content is blatantly illegal;⁴⁰² or (iii) where the intermediary believes it “prudent” not to provide due process, such as in cases of bots, malware, terrorism related content, or spam.⁴⁰³

These measures are intended to ensure transparency and accountability in content moderation, providing internet users a measure of recourse vis-à-vis online platforms. However, SSM Intermediaries may have limited incentive to meaningfully enforce this dispute settlement mechanism. To understand why, it is relevant to briefly discuss where Rule 4(8) is situated in the larger matrix of India’s intermediary regulation.

Rule 4(8) of the Intermediary Guidelines 2021 forms part of the “due diligence” obligations that intermediaries must satisfy under Section 79(2)(c) of the IT Act to enjoy safe harbour protections. Safe harbour is not a blanket immunity from civil and criminal liability, but rather a limited immunity for *hosting specific third party content*. From a regulatory perspective, this means that offering safe harbour will only alter intermediary behaviour in contexts where intermediaries are seeking immunity for content they are hosting. Additionally, an intermediary’s immunity is determined on a case-by-case basis, with respect to specific unlawful content, and is not a status that attaches to an intermediary for all content it hosts. Therefore, the breach of due diligence obligations vis-à-vis one piece of content does not disqualify intermediaries from safe harbour for all other content it is hosting.

Coming to Rule 4(8), the provision requires intermediaries to hear users prior to taking down, or *refusing to host*, the users’ content. A

399 Intermediary Guidelines 2021 r. 4(8) (a), 4(8)(b).

400 Intermediary Guidelines 2021 r. 4(8) (c).

401 Ministry of Electronics and Information Technology (n 62). FAQ 22.

402 *ibid.*

403 *ibid.* FAQ 23 The FAQs do not grant a blanket exemption from the due process requirements of Rule 4(8) but rather state that “intermediaries may undertake steps while handling a non-human user, to effectively counter bot activity.”

failure to provide this hearing will result in a loss of safe harbour for the SSM Intermediary. However, as the intermediary is *not hosting* the disputed content, the loss of safe harbour for hosting unlawful content is largely inconsequential, as an intermediary cannot be held liable for content it is not hosting. Indeed, the entire dispute between user and intermediary has arisen because the intermediary has refused to host the content. In other words, intermediaries may not be incentivised to provide this hearing to satisfy the requirements of “*due diligence*” and safe harbour, as they do not need safe harbour protections for content they are not hosting. This highlights the limits of trying to secure due process for content removals (i.e., recourse to users who want to keep content up) through the pre-conditions for safe harbour. One solution to this issue may have been to require SSM Intermediaries to provide due process by amending the IT Act rather than tying such a due process requirement to Section 79 immunity. Another process is the adoption of the Grievance Appellate Committee discussed in section 4.5(ii) of this report.

The incentives to provide users with hearings may be even weaker for large social media companies engaging in thousands of content moderation decisions daily. Further, Rule 4(8) does not prescribe the procedure for such dispute resolution. According to the MEITY’s non-legal clarifications, SSM Intermediaries are permitted to devise their own systems of due process.⁴⁰⁴ The scope of this obligation has also been narrowed to exclude situations where SSM Intermediaries remove content using automatic filters, where the content is blatantly illegal,⁴⁰⁵ and where the intermediary believes it “*prudent*” to not provide due process (e.g., in the case of bots or terrorism related content).⁴⁰⁶ While a user could in principle bring a contractual claim for the reinstatement of content, the clauses of platforms terms of service are exceedingly broad and confer platforms with almost unlimited discretion to take down content, making such a contractual claim unlikely to succeed.

Ultimately, several provisions of the Intermediary Guidelines 2021 may be better classified as regulatory legislation (as opposed to pre-conditions for safe harbour). However, unlike regulatory legislation which the government can directly enforce against intermediaries, intermediary liability and safe harbour as a regulatory tool relies on enforcement through individual lawsuits brought against intermediaries. It is crucial to recognise that safe harbour is evaluated on a case-by-case basis when an action

404 *ibid.* FAQ 21.

405 *ibid.* FAQ 22.

406 *ibid.* FAQ 23. The FAQs do not grant a blanket exemption from the due process requirements of Rule 4(8) but rather state that “intermediaries may undertake steps while handling a non-human user, to effectively counter bot activity.”

is brought against an intermediary for liability. While general standing conditions, such as the appointment of a local officer, can be tested by courts every time an action is initiated against an intermediary, ensuring compliance with Rule 4(8) in the context of safe harbour is more challenging. Even if SSM Intermediaries treat the Intermediary Guidelines 2021 as a regulatory scheme and set up a grievance mechanism, courts have no reason to examine the quality of *individual* adjudications under Rule 4(8) while adjudicating safe harbour cases where intermediaries are accused of hosting some *other* unlawful content. Thus, there may be little or no independent oversight of these processes. One structure to avoid this problem would have been to impose the notice and hearing requirements of Rule 4(8) as an independent and direct obligation on platforms by amending the IT Act instead of making it a pre-condition to safe harbour, as proposed by draft legislation in Europe.⁴⁰⁷

The adoption of the dispute settlement mechanism was intended to offer internet users a measure of recourse against the moderation decisions of large social media intermediaries. While its true impact on the internet user-intermediary axis is yet to be determined, the threat of stripping intermediaries of safe harbour in cases where they are not hosting content may apply limited regulatory pressure. It is relevant to note that with the October 2022 Amendment, users can now appeal content moderation decisions to a government appointed committee.⁴⁰⁸ This is discussed in section 4.5(ii) of the report. The October 2022 Amendment does not repeal Rule 4(8), thus the two continue to exist on paper concurrently. However, it is unclear the extent to which Rule 4(8) has been operationalised by SSM Intermediaries. Given that the transparency reporting under the Intermediary Guidelines 2021 does not require intermediaries to report (even in the aggregate) on the number of hearings conducted or volume of content reinstated under Rule 4(8), almost a year into the operation of Rule 4(8) compliance remains hard to assess.

(iii) Identifying first originators on messaging platforms

Rule 4(2) of the Intermediary Guidelines 2021 is applicable to SSM Intermediaries who provide services “primarily in the nature of messaging”.⁴⁰⁹ It requires such SSM Intermediaries to “enable the identification of the first originator” of content on its platform when directed by a court or an order passed under Section 69 of the IT Act (Power to issue directions for interception, monitoring,

⁴⁰⁷ European Commission, ‘Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC’ (15 December 2020) <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020P-C0825&from=en>> accessed 27 April 2022.

⁴⁰⁸ October 2022 Amendment, addition of r. 3A.

⁴⁰⁹ Intermediary Guidelines 2021 r. 4(2)

or decryption).⁴¹⁰ Where the first originator of unlawful content is located outside India, whomsoever is the first originator within India shall be deemed to be the first originator with respect to the content in question.⁴¹¹

Under Section 69, either the Union or State Government can direct the interception, monitoring, or decryption of information on a computer network if it is satisfied that it is “*necessary or expedient*” to do so in the interests of the sovereignty, integrity, or defence of India, relations with foreign States, public order, or the incitement of an offence related to these interests.⁴¹² In December 2018 the Union Ministry of Home Affairs authorised ten agencies to intercept, monitor, and decrypt information under Section 69 of the IT Act, including the Narcotics Control Bureau, the Central Board of Direct Taxes and Enforcement Directorate, and the Delhi Police Commissioner.⁴¹³ Directions under Section 69 are issued by senior civil servants of the home office without any judicial scrutiny (either *ex-ante* or *ex-post*).⁴¹⁴

Government statements indicate that the requirement is part of a strategy to curb real-world violence attributed to the distribution of inflammatory content on popular messaging platforms such as WhatsApp.⁴¹⁵ An order directing the identification of an originator under Rule 4(2) may be passed for the purposes of: (i) prevention, detection, investigation, prosecution or punishment of an offence;

410 Intermediary Guidelines 2021 r. 4(2).

411 Intermediary Guidelines 2021 r. 4(2) (fourth proviso).

412 The Information Technology Act, 2000 s. 69(1).

413 Ministry of Home Affairs (Cyber and Information Security Division) S.O. 6227(E) dated 20 December 2018 authorising security and intelligence agencies to intercept, monitor, and decrypt information under Section 69 of the IT Act.

414 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 G.S.R. 780(E) dated 27 October 2009 r. 2(d) (defining the ‘competent authority’ to issue directions as the Secretary in the Ministry of Home Affairs for the Central Government and the Secretary in charge of the Home Department in the case of the State Government).

415 Prasanto Roy, ‘Why India Wants to Track WhatsApp Messages’ *BBC News* (30 October 2019) <<https://www.bbc.com/news/world-asia-india-50167569>> accessed 21 May 2021.

and (ii) where such offence is related to the sovereignty, integrity, or security of the Indian State, its relation with foreign States, public order, or any offence relating to rape or sexually explicit material punishable by a prison term of five or more years.⁴¹⁶ Rule 4(2) further states that an identification order shall not be passed where a less intrusive means of identifying the first originator is effective,⁴¹⁷ and that the SSM Intermediary shall not be required to disclose the contents of any message or any other information regarding the content originator.⁴¹⁸

416 Intermediary Guidelines 2021 r. 4(2) (first proviso).

417 Intermediary Guidelines 2021 r. 4(2) (second proviso).

418 Intermediary Guidelines 2021 r. 4(2) (third proviso).

Issues with the idea of a ‘first originator’

Although the term “*first originator*” is not defined in the IT Act or the Intermediary Guidelines, the IT Act does define the term “*originator*” to mean a person who generates, stores, or transmits an electronic message or by their actions, causes a message to be generated, stored, or transmitted.⁴¹⁹ Thus, the term “*first originator*” may be construed to mean the first person to generate, store, or transmit a specific piece of content on a particular SSM Intermediary’s network. However, such an interpretation does not clarify if the first originator is chronologically the first person ever to transmit a specific piece of content on a particular network, or the first person in a single chain of forwarded content.⁴²⁰ For example, if User 1 shares content with User 2 on Day 1, and then User 3 independently accesses the same content on Day 2 and shares it with User 4, who forwards it to User 5, at which point it is disclosed to law enforcement and deemed to be unlawful. Is User 1 or User 3 the ‘first originator’? ⁴²¹ This is important because, as we shall see, one technical proposal to implement Rule 4(2) can trace the first time content ever appeared on a messaging platform while another can only trace the originator of a particular unbroken chain of forwarded content.

419 The Information Technology Act, 2000 s. 2(1)(za).

420 Greg Nojeim and Namrata Maheshwari, ‘Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth’ (2021) 17 Indian Journal of Law and Technology 1, 13.

421 *ibid.*

The text of Rule 4(2) requires the relevant SSM Intermediary to identify the originator itself, as opposed to a specific user account or device from which the content originated. However, a technological solution would only be able to identify the device, or alternatively, the email address or phone number of the individual, and not the actual person. Further, the obligation to identify is logically limited to the SSM Intermediary’s own network.

This raises three issues. First, even if the SSM Intermediary is able to trace content to a particular device or account, the use of the device or account by a particular person will need to be

independently verified. Indeed, Section 88 of the Indian Evidence Act prohibits courts from making assumptions about the real-world sender of an electronic message based on who the purported sender and addressee of a message are; an implicit acknowledgement that a single device or identifier may be used by multiple people (with or without permission).⁴²² Thus, the identification of a phone or device from which a message was first sent would be of limited value in establishing who sent the message in a criminal prosecution. Second, where an SSM Intermediary can provide the device or user account that first transmitted the content, this device or user account will only be the first *on that particular SSM Intermediary's network*. Given that a user can easily spread content between platforms by cross-posting, the identity of the first originator of content on any given network may be of limited investigative relevance.

⁴²² Gurshabad Grover, Tanaya Rajwade and Divyank Katira, 'The Ministry and the Trace: Subverting End-To-End Encryption' (2021) 14 NUJS Law Review.

Finally, there is an issue with the presumption that the first originator vis-à-vis specific content will be the first recipient in India. If this principle is applied to refer to the first time content appears on an intermediaries network in India (as opposed to being limited to a specific chain of forwards), it is possible that a malicious content creator can simply secure a foreign number and send content to a host of Indian numbers simultaneously (or a proxy Indian number), ensuring their identity is excluded from the risks of being traced by Rule 4(2). Further, messaging services will have to rely on a user's self-declared location or area-code of the phone number associated with the user's account, which may not be an accurate reflection of their true location.⁴²³ For example, a user may have a WhatsApp account affiliated to a '+91' phone number but be operating overseas, or have an account associated with a foreign phone number but be operating within India.

⁴²³ *ibid.*

Where intermediaries possess decryption key

Unlike Rule 4(4), which uses the term "*shall endeavour*", Rule 4(2) imposes a categorical obligation on SSM Intermediaries providing messaging services to identify first originators within its network. However, Rule 4(2) also notes that the SSM Intermediaries will be required to trace first originators "*as per*" the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ('IT Decryption Rules') or pursuant to a court order. Under the IT Decryption Rules, intermediaries are required to provide

decryption assistance to law enforcement agencies, but only on a best efforts' basis⁴²⁴ and crucially, 'where the intermediary controls the decryption key'.⁴²⁵

As the Intermediary Guidelines 2021 note that first originators will be traced "*as per*" the IT Decryption Rules, the extent to which intermediaries must assist law enforcement agencies remains unclear.⁴²⁶ One possible interpretation is that the IT Decryption Rules apply only to cases of 'recoverable encryption' where an encrypted message can be decrypted without the cooperation of the sender or receiver, or access to their respective devices (e.g., where the intermediary holds the decryption key).⁴²⁷ Consequently, as Rule 4(2) requires the tracing of first originators "*as per*" the IT Decryption Rules, Rule 4(2) itself only applies to cases of recoverable encryption. Under this interpretation, situations where it may not be possible for an intermediary to decrypt information, such as where it does not possess the decryption key ('unrecoverable encryption') remain outside the purview of Rule 4(2). However, the Union Government has publicly stated that Rule 4(2) will apply to unrecoverable end-to-end encrypted platforms such as WhatsApp where encryption is 'unrecoverable'.⁴²⁸

Technical feasibility vis-à-vis end-to-end encryption

At the time of this report, there also remains uncertainty over how the requirement to trace originators will be implemented. The MEITY and government sources have stated that first originators may be identified without decrypting the contents of messages by assigning every unique message on the platform an identifier, or 'hash constant'; once an unencrypted message of unlawful content is identified, the hash constant of this unlawful message will be compared against all messages sent by all users on the network to locate messages with matching hashes, uncovering all users who sent identical messages and also locating where the message first originated.⁴²⁹ The MEITY has stated that SSM Intermediaries will have to decide how the hash will be generated and where it will be stored, and that SSM Intermediaries are free to devise alternative technological solutions to enable this requirement.⁴³⁰

However, commentators have pointed out that on end-to-end encrypted platforms such as WhatsApp and Signal, the hash value generated for accounts would be tied to the identities of the sender and the receiver.⁴³¹ Thus, the hash value of identical messages between User 1 and User 2, and User 1 and User 3 will

424 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 G.S.R. 780(E) dated 27 October 2009 r. 2(g).

425 *ibid* r. 13(3).

426 Vrinda Bhandari, Rishab Bailey and Faiza Rahman, 'Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance"' [2021] SSRN Electronic Journal 12–13 <<https://www.ssrn.com/abstract=3805980>> accessed 1 May 2021.

427 *See* Bhandari, Bailey and Rahman (n 426). Explaining the distinction between recoverable and unrecoverable encryption.

428 Salman SH, 'Indian Govt Determined To Enforce WhatsApp Message Traceability' (Inc42 Media, 15 March 2021) <<https://inc42.com/buzz/indian-govt-determined-to-enforce-whatsapp-message-traceability/>> accessed 13 July 2021.

429 Ministry of Electronics and Information Technology (n 62). FAQ 24; Deeksha Bhardwaj, 'Hash Constant: Govt's Solution to Tracing Originator of Viral Messages' (Hindustan Times, 2 March 2021) <<https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-messages-101614667706841.html>> accessed 8 March 2021.

430 Ministry of Electronics and Information Technology (n 62). FAQ 24.

431 Nojeim and Maheshwari (n 420) 17–18.

be different; this would make identifying the originator of any piece of content using the hashing method virtually impossible. Another apparent issue with the hashing approach is that because hashes are assigned to every *unique* message, a small change to punctuation, spelling, or file name in the message would generate a new hash that does not match the hash of any existing unlawful content.⁴³² Experts also note that because the hashing is carried out on the user's device, the user's device could be manipulated to incorrectly hash messages; a concern aggravated by the widespread use of modified messaging clients for services such as WhatsApp.⁴³³

There are also structural concerns with the Ministry's approach. First, millions of messages are sent on messaging platforms every day and the maintaining such a hash library would be both immensely resource intensive and a violation of the data minimisation principle.⁴³⁴ Second, once the hash of a particular unencrypted unlawful message is known, identifying the first originator would require identifying *all* persons on the network who have sent identical messages, thus fundamentally undermining the confidentiality of messages of potentially thousands of other users who sent the same message.⁴³⁵ In fact, this directly contravenes the text of Rule 4(2) itself, which states that no intermediary will be required to disclose the "*contents of any electronic message*". However, searching the hash database for all messages having an identical hash to locate the first message would result in the identification of all individuals who have sent the particular message, thus disclosing both the content of the message and identity of the sender of every identical message. For example, if law enforcement receives an unencrypted version of a message: *'Hello, good morning'*, they can ascertain the hash of *'Hello, good morning'* is '4215'. They can search the network to see when the hash '4215' first appeared on the network, but this would also reveal every person who sent a message having a hash of '4215', thus revealing to law enforcement every person who ever sent the message *'Hello, good morning'* on the network. Once the hash of certain content is known, such content could be both be automatically tracked or blocked at a network wide level,⁴³⁶ raising significant speech and privacy concerns.

Industry experts in India have also argued that it may be possible to use unique identifiers to trace originators.⁴³⁷ One proposal involves attaching encrypted personally identifiable originator information to messages.⁴³⁸ Under this proposal, users would have

432 Aditi Agarwal, 'Traceability And End-to-End Encryption Cannot Co-Exist On Digital Messaging Platforms: Experts' *Forbes India* (15 March 2021) <<https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1>> accessed 21 May 2021.

433 Grover, Rajwade and Katira (n 422).

434 Nojeim and Maheshwari (n 420) 18.

435 Grover, Rajwade and Katira (n 422); Nojeim and Maheshwari (n 420) 18.

436 Grover, Rajwade and Katira (n 422).

437 Prasad Banerjee, 'Messaging Apps May Be Able to Comply with New Guidelines without Privacy Breach' (*mint*, 28 February 2021) <<https://www.livemint.com/news/india/messaging-apps-may-be-able-to-comply-with-new-guidelines-without-privacy-breach-11614521487786.html>> accessed 12 March 2021.

438 Agarwal (n 432).

the option to send ‘forwardable’ and ‘non-forwardable’ messages, and if they chose to send ‘forwardable messages’, an identifier (e.g., their phone number) would be attached to the ‘forwardable’ message in an encrypted manner, and the intermediary would hold the decryption key to the identifier in escrow.⁴³⁹ If law enforcement wished to decrypt the identifier to identify who first sent the message, they would approach the intermediary to decrypt the identifier.

439 Agarwal (n 432).

Commentators have noted that the chief problem with this proposal is that it only identifies the first sender of a *particular chain of forwards*, and not the first person to share content on the platform.⁴⁴⁰ For example, if User 1 sent a ‘non-forwardable’ message to User 2, who then sent the same message to User 3 as a ‘forwardable message’, User 2’s information would be affixed to the message as the originator, instead of User 1’s. Thus, the real originator’s details could be masked very easily. Further, even if User 1 shared the message as a ‘forwardable’ message, but User 2 used any other form of sharing, such as copy-pasting the message into a new chat window or taking a screenshot of the content and shared it with User 3, User 2 would be detected as the first originator.⁴⁴¹ Thus, there is a high chance of the wrong person being identified as the originator simply because the chain of forwarded messages was broken or interfered with at some point. Lastly, experts also note that the storing of keys by intermediaries (to decrypt the originator information affixed to messages) could be targeted by malicious actors,⁴⁴² and if disclosed, could lead to third parties identifying the originators of messages beyond the scope of Rule 4(2).

440 Nojeim and Maheshwari (n 420) 16.

441 *ibid.*

442 Grover, Rajwade and Katira (n 422).

Other experts and cryptographers have also argued that it may not be possible to trace first originators on messaging services that employ end-to-end encryption without compromising encryption and potentially, the security of all other users of the service.⁴⁴³ In particular, they have noted that as encryption systems on messaging platforms regularly change the encryption key between users, each individual instance of decryption would reveal only a fragment of the communication between users.⁴⁴⁴ In September 2020, the Telecom Regulatory Authority of India opined that imposing decryption requirements on such ‘messaging intermediaries’ would require them to change their “*entire architecture*” and may make user communication more vulnerable to unlawful actors.⁴⁴⁵

443 *See* Agarwal (n 432).

444 Bhandari, Bailey and Rahman (n 426) 16.

445 Telecom Regulatory Authority of India, ‘Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services’ (2020) <https://traai.gov.in/sites/default/files/Recommendation_14092020_0.pdf>.

A human rights impact assessment released by Meta highlighted three key issues with compromising the integrity of end-to-end encryption to detect unlawful content on messaging platforms: (i) a lack of consensus on when messaging services were purely private and outside the scope of content moderation and when services included a public facet (e.g., group messaging) that potentially warranted content moderation; (ii) the technical feasibility of such measures remained uncertain; and (iii) deployment to detect one class of unlawful content (e.g., child sex abuse material) could lead to deployment against other categories of speech, raising concerns for the freedom of expression.⁴⁴⁶ Similarly, Apple delayed the deployment of a “perceptual hashing” feature that would scan photos uploaded by users onto the cloud and compare them against known child abuse content.⁴⁴⁷ However, the company intends to deploy a feature that allows for on-device scanning for nudity in its ‘Messages’ application where the user of the iPhone is a child.⁴⁴⁸

Alternative measures

Tracing originators may also potentially be implemented purely by tracking metadata. For example, messaging services could record and track which users send messages to each other, when these messages are sent, and the size of these messages, without examining the contents of the messages. However, this approach may be hampered by the fact that different SSM Intermediaries may collect different amounts of metadata from users. Some platforms collect information such as ‘phone numbers, names, device info, app versions, start dates and times, connection status, last connection dates and times, IP addresses, e-mail addresses, and web client data’,⁴⁴⁹ potentially allowing for the identification of a user using metadata alone. For example, in 2019, senior Facebook officials proposed using the metadata collected by WhatsApp to assist Indian investigative agencies.⁴⁵⁰ Similarly, the Delhi High Court required Telegram to disclose the phone numbers and IP Addresses of users allegedly sharing copyright infringing content,⁴⁵¹ an order that Telegram eventually complied with.⁴⁵² However, other platforms do not collect this metadata. For example, when responding to a United States grand jury subpoena in 2016, the messaging service Signal stated that it only stored the timestamps of the first, and the most recent time a user connected to its service.⁴⁵³ This is likely insufficient to identify first originators.

446 BSR, ‘Human Rights Impact Assessment on Meta’s Expansion of End-to-End Encryption’ (BSR 2022) <<https://www.bsr.org/en/our-insights/report-view/metaspansion-end-to-end-encryption>> accessed 1 May 2022.

447 Alex Hern, ‘Apple Delays Plans to Scan Cloud Uploads for Child Sexual Abuse Images’ *The Guardian* (3 September 2021) <<https://www.theguardian.com/technology/2021/sep/03/apple-delays-plans-to-scan-cloud-uploads-for-child-sexual-abuse-images>> accessed 1 May 2022.

448 Alex Hern, ‘Apple to Roll out Child Safety Feature That Scans Messages for Nudity to UK iPhones’ *The Guardian* (20 April 2022) <<https://www.theguardian.com/technology/2022/apr/20/apple-says-new-child-safety-feature-to-be-rolled-out-for-uk-iphones>> accessed 1 May 2022.

449 *Antony Clement Rubin v Union of India* WP 20774 of 2018 (High Court of Madras, 25 April 2019).

450 ‘Whatsapp Monitoring: FB Moots “prospective” Solution, Fails to Appease Govt’ *Business Standard India* (15 September 2019) <https://www.business-standard.com/article/pti-stories/facebook-global-exec-moots-prospective-solution-on-whatsapp-issue-govt-stands-firm-on-traceability-119091500194_1.html> accessed 12 March 2021.

451 *Neetu Singh v Telegram FZ LLC CS* (Comm) 282 of 2020 (High Court of Delhi, 30 August 2022) [47].

452 Sofi Ahsan, ‘After Delhi High Court Ruling, Telegram Discloses Names, Phone Numbers & IP Addresses Of Users Accused Of Sharing Infringing Material’ (*Live Law*, 29 November 2022) <<https://www.livelaw.in/news-updates/after-court-order-telegram-discloses-phone-numbers-ip-addresses-of-users-accused-of-sharing-infringing-material-215311>> accessed 2 December 2022.

453 Joseph Menn, ‘Signal Messaging App Turns over Minimal Data in First Subpoena’ *Reuters* (4 October 2016) <<https://www.reuters.com/article/us-usa-cyber-signal-idUSKCN1241JM>> accessed 12 March 2021.

Several intermediaries recently argued before the High Court of Madras that they could only provide information to the extent it was collected by their platforms and was reasonably accessible.⁴⁵⁴ More recently, WhatsApp has challenged the constitutionality of Rule 4(2) of the Intermediary Guidelines 2021, arguing that the requirement to trace first originators cannot be implemented without breaking end-to-end encryption and undermining their users' right to privacy.⁴⁵⁵

In supporting documentation regarding Rule 4(2), the MEITY stated that SSM Intermediaries will not be authorised to identify first originators without an order from the government or a court.⁴⁵⁶ However, if SSM Intermediaries do possess the technical capability to identify first originators on messaging platforms, nothing in the Intermediary Guidelines 2021 prohibits them from doing so on a voluntary basis. Thus, Rule 4(2) raises the possibility of both, messaging platforms tracking messages and originators for their own benefit, and non-state entities gaining access to private communications by entering into undisclosed arrangements with messaging platforms.

Constitutionality

The Constitution of India guarantees citizens a right to privacy,⁴⁵⁷ which extends to telephonic communication.⁴⁵⁸ Therefore, any provision authorising the interception of messages or the identification of individuals based on the decryption of private communications would have to satisfy constitutional standards. The interception of communications also interferes with the freedom of speech, as private communications ensure that individuals can hold and espouse potentially unpopular opinions without the risk of unlawful suppression or retribution.⁴⁵⁹ Separately, commentators have argued that forcing *an individual* to decrypt information or provide an unencrypted device to law enforcement may violate their constitutional right against self-incrimination. This is because decryption effectively involves unscrambling the message into an intelligible form, akin to asking an individual to 'explain the message'.

A plurality of four judges in the landmark case of *KS Puttaswamy vs. Union of India* examined previous decisions of the Supreme Court and concluded that Indian courts had condoned telephonic interception or 'tapping' only where such interference was specific and targeted,⁴⁶⁰ and ruled that surveillance of

454 *Antony Clement Rubin v Union of India* WP 20774 of 2018 (High Court of Madras, 25 April 2019).

455 Sofi Ahsan, 'Tracing Messages Will Violate Privacy, Chill Free Speech: WhatsApp' *The Indian Express* (27 May 2021) <<https://indianexpress.com/article/technology/tech-news-technology/tracing-messages-will-violate-privacy-chill-free-speech-whatsapp-7331846/>> accessed 29 May 2021.

456 Ministry of Electronics and Information Technology (n 62). FAQ 6.

457 *KS Puttaswamy v Union of India* 2017 (10) SCC 1 [650].

458 See *People's Union for Civil Liberties v Union of India* 1997 (1) SCC 301.

459 David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/29/32' <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement>> accessed 17 September 2021. Para. 16.

460 *KS Puttaswamy v Union of India* 2017 (10) SCC 1 [51] citing *RM Malkani v State of Maharashtra* 1973 (1) SCC 471.

communications absent procedural safeguards would be constitutionally impermissible.⁴⁶¹ While Indian courts have not required judicial scrutiny prior to telephonic interception,⁴⁶² measures infringing the privacy of users would have to satisfy the test of proportionality.⁴⁶³

The test for proportionality under Indian law may be summarised as: (i) the measure must be sanctioned by law; (ii) the infringing measure must pursue a legitimate State aim; (iii) the infringing measure must be necessary to achieve the legitimate aim (included in this is, the infringing measure must be the least intrusive measure amongst equally effective alternatives); (iv); the infringing measure must be proportionate to the State aim sought to be achieved; and (v) there must be adequate procedural safeguards against abuse.⁴⁶⁴

(1) **Legality:** The test of legality requires both that the measure be sanctioned by law, and that the measure be formulated with sufficient precision to enable citizens to regulate their conduct to avoid conduct proscribed by the law.⁴⁶⁵ The Intermediary Guidelines 2021 have been passed under rule-making provisions that relate to Section 69A (blocking of content) and Section 79 (due diligence obligations),⁴⁶⁶ neither of which empower the Union Government to legislate for surveillance or investigatory powers. While the IT Act does empower the Union Government to make delegated legislation with respect to surveillance and encryption,⁴⁶⁷ the effect of *prima facie* referring to the incorrect rule-making provisions will have to be evaluated by courts.

It is also relevant to note that Rule 4(2) of the Intermediary Guidelines 2021 constitutes delegated legislation. The source of the State's power to direct intermediaries to intercept and decrypt information can be traced to Section 69 of the IT Act (Power to issue directions for the interception or monitoring or decryption of any information through any computer resource). Section 69 permits the government to utilise this power in the interests of the sovereignty, integrity, defence, or security of India or its relations with foreign States, public order, or preventing the incitement of an offence related to these interests.⁴⁶⁸ However, Rule 4(2) expands the applicability of this power in the context of social media messaging

461 *ibid* [58] citing *Malak Singh v State of Punjab* 1981 (1) SCC 420.

462 See *People's Union for Civil Liberties v Union of India* 1997 (1) SCC 301. Cf *KS Puttaswamy v Union of India* 2017 (10) SCC 1 [513.6] (dicta noting that it would be 'preferable' if prior judicial authorisation was required where government actions interfered with citizens' right to privacy).

463 *KS Puttaswamy v Union of India* 2017 (10) SCC 1 [310].

464 *Anuradha Bhasin v Union of India* 2020 (3) SCC 637 [60]-[80]. See also Bhandari, Bailey and Rahman (n 426); Vrinda Bhandari and Karan Lahiri, 'The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World' (2020) 3 University of Oxford Human Rights Hub Journal 15.

465 Nojeim and Maheshwari (n 420) 27.

466 Intermediary Guidelines 2021. The preamble states that the Guidelines have been issued under ss. 87(1)(z), 87(1)(zg), 87(2) of the Information Technology Act, 2000.

467 Information Technology Act, 2000 ss. 84, 87(1)(y).

468 Information Technology Act, 2000 s. 69(1).

services to include the detection or investigation of rape, sexually explicit material, or child sexual abuse material.⁴⁶⁹ The expansion of State powers that infringe on fundamental rights of citizens through delegated legislation (i.e., without Parliamentary approval) may lead to courts to rule that that Rule 4(2) is *ultra vires* the IT Act and hence legally void.⁴⁷⁰

Of additional concern is whether Rule 4(2) is sufficiently precise in its proposed operation to allow citizens to regulate their conduct. For example, it is unclear whether the first instance of content on a network or the first sender in a chain of content that goes viral will be targeted as a first originator. Thus, individuals may be wary of sharing content to trusted recipients even for the purposes of debunking or chastising it, because if it is the first time the content is shared on the messaging services network, they may be targeted by investigative agencies as the first originator. Similarly, individuals may not wish to receive messages from any foreign numbers for fear that it is unlawful content, and they are targeted as the ‘first originator in India’. Thus, the substantial uncertainty as to the operation of Rule 4(2) may render it sufficiently vague as to cause confusion amongst citizens as to when they may be identified as ‘first originators’ and embroiled in an investigation.

- (2) **Legitimate aim:** The first proviso to Rule 4(2) is instructive of the aims sought to be achieved by the measure. A ‘tracing order’ may only be passed to pursue the prevention, detection, investigation, prosecution, or punishment of an offence (or the incitement of an offence) related to: (i) public order; (ii) the sovereignty, integrity, or security of India or its friendly relations with foreign States; (iii) rape; or (iv) sexually explicit or child sexual abuse material.⁴⁷¹ Additionally, the offence in question must be punishable with a sentence of at least five years.⁴⁷² While these are admittedly expansive terms that could include both constitutional and unconstitutional actions, they do represent recognised legitimate aims on which privacy may be restricted.⁴⁷³
- (3) **Necessity:** It remains unclear whether tracing first originators is necessary to achieve the stated goal of

469 Intermediary Guidelines 2021 r. 4(2).

470 See Section 4.1(ii) of this report discussing the limits of delegated legislation.

471 Intermediary Guidelines 2021 r. 4(2) (first proviso).

472 Intermediary Guidelines 2021 r. 4(2) (first proviso).

473 *KS Puttaswamy v Union of India* 2017 (10) SCC 1 [311].

preventing, investigating, and prosecuting a broad range of offences. As the measure is significantly more intrusive of privacy, the State must justify why such an approach is more effective than any other measure presently employed by it. This is particularly problematic given that metadata collected by messaging services such as WhatsApp (which is already shared with law enforcement) could give investigative agencies comparable insight without compromising encryption and the privacy of other users,⁴⁷⁴ thus constituting a less restrictive measure and weighing against the constitutionality of Rule 4(2). As noted above, SSM Intermediaries may be able to assist law enforcement agencies with the device or account identifiers that first published unlawful content on their network, but this itself is not proof that a particular individual created or disseminated the unlawful content. The ownership and use of the device or account, the illegality of the content, and the ‘first originator’s’ role in the alleged illegality would need to be proven independently, using traditional investigative techniques. Identifying a person as a first originator is thus substantially distanced from the underlying objectives of crime prevention and prosecution.

474 Grover, Rajwade and Katira (n 422).

Further, as demonstrated in the technical feasibility section above, both proposals for implementing Rule 4(2) have a high risk of circumvention and could lead to innocent individuals being identified as the originator.⁴⁷⁵ This risk is especially high as the concept of a first originator does not account for context. If User 1 shared unlawful content with User 2, and immediately sent a follow up message debunking or chastising the content, and later User 3 widely disseminated the same content, under the hashing proposal that identified the first instance of content on the platform, User 1 would still be identified as the first originator. Lastly, Rule 4(2) itself states that the first person to receive content in India will be deemed to be the first originator in the case of content originating outside India, diluting the nexus between the role of the first originator and the illegality of the content.

475 *ibid.*

- (4) **Proportionality:** Factors that weigh in favour of proportionality include the express safeguard that a tracing order cannot be passed where less intrusive

means of identification are effective,⁴⁷⁶ and a bar on the disclosure of the contents of the electronic message itself or other information,⁴⁷⁷ suggesting that the measure is narrowly tailored.

However, there are also several factors that speak to the measure being disproportionate. Courts should consider the impact of potentially compromising the privacy rights of other users if they rule that encryption generally may be weakened through the implementation of Rule 4(2), as the Telecom Regulatory Authority of India has suggested.⁴⁷⁸ SSM Intermediaries will have to store the potential originator information or unique hash of all messages by all users to effectively be able to identify the first originator of any given message. This has led to commentators describing Rule 4(2) as a ‘mandate which infringes on the security and privacy of the many in an attempt to catch a few bad actors’.⁴⁷⁹ The risk of innocent individuals being incorrectly identified as the first originator of unlawful content and charged also weighs against the proportionality of the law. Finally, the mere possibility of enhanced surveillance and the undermining of safeguards for anonymous speech may result in a chilling effect on speech,⁴⁸⁰ restricting freedoms of speech and association – a factor that may be considered in a court’s balancing exercise. Although end-to-end encryption does impose substantial burdens on law enforcement agencies, such burdens guard against mass surveillance and also form an important check on State power, especially in a country like India where illegally collected evidence is admissible at trial.⁴⁸¹

- (5) **Procedural Safeguards:** As with Rule 4(4), the real-world safeguards and structures of accountability with respect to Rule 4(2) are limited. An order authorising tracing under Section 69 of the IT Act does not require prior judicial authorisation, and the entire process is conducted by investigative agencies and senior civil servants.⁴⁸² This lack of judicial or parliamentary oversight has been criticised by the expert committee tasked with formulating India’s upcoming data protection legislation.⁴⁸³ Thus, there exists no independent check to determine whether government agencies are utilising the power for lawful purposes, have explored less intrusive

476 Intermediary Guidelines 2021 r. 4(2) (second proviso).

477 Intermediary Guidelines 2021 r. 4(2) (third proviso).

478 Telecom Regulatory Authority of India (n 445).

479 Grover, Rajwade and Katira (n 422).

480 Nojeim and Maheshwari (n 420) 29.

481 See Bhandari, Bailey and Rahman (n 426) 25.

482 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 G.S.R. 780(E) dated 27 October 2009 r.3.

483 Bhandari, Bailey and Rahman (n 426); Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, ‘A Free and Fair Digital Economy. Protecting Privacy, Empowering Indians’ (2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>.

methods, or are adhering to the prohibition on decrypting the contents of messages. Finally, commentators have noted that at the stage of passing an order under Section 69, authorities do not possess the technical expertise to determine if the investigation can be conducted through less intrusive measures, and no structures exist for them to hear from experts or the intermediary.⁴⁸⁴

484 Nojeim and Maheshwari (n 420) 20.

As Rule 4(2) of the Intermediary Guidelines is currently subject to legal challenge, it is possible that future judicial outcomes will alter or entirely abolish the implementation of the requirement to trace first originators.

4.5. Intermediary Guidelines 2021: Subsequent developments

At the time of writing this report, there have been two key developments since the adoption of the Intermediary Guidelines 2021: several court challenges to the legality and constitutionality of the Guidelines, and key amendments to the Guidelines themselves (referred to here as the October 2022 Amendment).

(i) Legal challenges to the Intermediary Guidelines 2021

As of April 2022, there existed nine separate legal challenges to Part II of the Intermediary Guidelines 2021 that directly impact intermediary liability.⁴⁸⁵ Additional challenges have been initiated by web publishers and media organisations against Part III of the Intermediary Guidelines.⁴⁸⁶ These challenges concern the new regulations imposed on online news publications and over-the-top providers of audio-visual content. The Union Government has requested that all legal challenges pertaining to the Intermediary Guidelines be transferred to the Supreme Court and heard together.⁴⁸⁷ At the time of writing this report, the Supreme Court is yet to rule on this request but the Supreme Court has directed High Courts to stop hearing legal challenges to the Intermediary Guidelines 2021.⁴⁸⁸ This section provides a brief overview of the challenges to Part II of the Intermediary Guidelines 2021 (that regulate intermediaries). Although these challenges were initiated before High Courts, the contentions are likely to be similar even if the challenges are transferred to the Supreme Court. Notably, both Facebook and WhatsApp (owned by Facebook) have challenged Rule 4(2) requiring messaging platforms to identify the first originator of content on their platforms.⁴⁸⁹

In its petition, WhatsApp has contended *inter alia* that Rule 4(2) of the Intermediary Guidelines 2021 violated the privacy of its users and was beyond the rule-making powers relied on by the Union Government when promulgating the Guidelines.⁴⁹⁰ WhatsApp has argued that operationalising the tracing of first originators would require WhatsApp to keep records of *all* communications on its platforms (since the government could ask for the originator of any message), and this violated the requirement of proportionality laid down by the Supreme Court.⁴⁹¹ In response to WhatsApp's challenge, the Union Government released a statement saying that Rule 4(2) is a permissible and proportionate interference with the privacy of citizens which can only be invoked when less

485 *LiveLaw Media Pvt Ltd v Union of India* WP (C) 6272 of 2021 (High Court of Kerala); *Sanjay Kumar Singh v Union of India* WP (C) 3483 of 2021 (High Court of Delhi); *Uday Bedi v Union of India* WP (C) 6844 of 2021 (High Court of Delhi); *Praveen Arimbrathodiyil v Union of India* WP (C) 9647 of 2021 (High Court of Kerala); *TM Krishna v Union of India* WP (C) 12515 of 2021 (High Court of Madras); *Sayanti Sengupta v Union of India* WPA (P) 153 of 2021 (High Court of Calcutta); *Nikhil Wagle v Union of India* PIL (L) 14204 of 2021 (High Court of Bombay); *Facebook Inc v Union of India* WP (C) 7281 of 2021 (High Court of Delhi); *WhatsApp LLC v Union of India* WP (C) 7284 of 2021 (High Court of Delhi).

486 *Press Trust of India Limited v Union of India* WP (C) 6188 of 2021 (High Court of Delhi); *Foundation for Independent Journalists v Union of India* WP (C) 3125 of 2021 (High Court of Delhi); *The Leaflet (Nineteenone Media Pvt Ltd) v Union of India* WPL 14172 of 2021 (High Court of Bombay); *Quint Digital Media Ltd v Union of India* WP (C) 3659 of 2021 (High Court of Delhi); *Pravda Media Foundation v Union of India* WP (C) 5973 of 2021 (High Court of Delhi); *News Broadcasters Association v Ministry of Electronics and Information Technology* WP (C) 13675 of 2021 (High Court of Kerala); *Truth Pro Foundation of India v Union of India* WP (C) 6941 of 2021 (High Court of Karnataka); *Digital News Publishers Association v Union of India* WP (C) 13055 of 2021 (High Court of Madras); *Nikhil Wagle v Union of India* PIL (L) 14204 of 2021 (High Court of Bombay); *Indian Broadcasting & Digital Foundation v Ministry of Electronics and Information Technology* WP 25619 of 2021 (High Court of Madras).

487 Sohini Chowdhury, 'IT Rules 2021 : Supreme Court To Hear Centre's Plea To Stay Interim Orders Passed By High Courts On July 27' (Live Law, 20 July 2022) <<https://www.livelaw.in/top-stories/supreme-court-it-rules-cable-tc-amendment-rules-online-media-ott-regulation-204329>> accessed 1 August 2022.

488 *Skand Bajpai v Union of India* WP (C) 799 of 2020 (Supreme Court of India, 9 May 2022).

489 *Facebook Inc v Union of India* WP (C) 7281 of 2021 (High Court of Delhi); *WhatsApp LLC v Union of India* WP (C) 7284 of 2021 (High Court of Delhi).

490 'Copy of the Writ Petition Filed by WhatApp LLC in *WhatsApp LLC v Union of India*, WP (C) 7284 of 2021 (High Court of Delhi)' <<https://www.medianama.com/wp-content/uploads/2021/05/WhatsApp-v.-Union-of-India-Filing-Version.pdf>> accessed 17 September 2021.

491 *ibid* 39.

intrusive measures were ineffective.⁴⁹²

WhatsApp's petition also notes that the Intermediary Guidelines 2021 refer to Sections 87(2)(z) and 87(2)(zg) of the IT Act as the source of their legal power. Section 87(2)(z) grants the Union Government power to create rules for the blocking of content under Section 69A,⁴⁹³ while Section 87(2)(zg) empowers the Government to draft guidelines under Section 79(2)⁴⁹⁴ concerning an intermediary's due diligence obligations. WhatsApp has argued that requiring intermediaries to identify first originators does not concern either blocking of content or an intermediary's due diligence obligations and is thus *ultra vires* the rule-making power in the IT Act and is hence void.⁴⁹⁵

Other challenges to the Intermediary Guidelines also contend that the Guidelines infringe the privacy of citizens and exceed the Union Government's rule-making power under the IT Act.⁴⁹⁶ However, as these petitions are filed by ordinary citizens as users of online intermediaries, the standing of these petitioners differ. For example, rather than WhatsApp arguing that the privacy of those that utilise its services will be infringed, petitions by users contend that their own privacy will be impermissibly restricted. This may be relevant as natural persons typically have a more direct claim to Fundamental Rights under the Indian Constitution.⁴⁹⁷ Petitions by users additionally argue that the Intermediary Guidelines 2021 confer outsized power on private intermediaries to restrict free speech and conflict with the judgement in *Shreya Singhal*.⁴⁹⁸ The petitions contend that this shift ultimately restricts the free speech rights of ordinary internet users and undermines the rule of law.

In a preliminary hearing, the High Court of Bombay refused to stay the operation of Rule 7 of the Intermediary Guidelines 2021.⁴⁹⁹ Rule 7 of the Guidelines states that online intermediaries which do not comply with the Intermediary Guidelines will not enjoy safe harbour protections for content they host.⁵⁰⁰ However, the High Court did not arrive at this conclusion based on the content of the Guidelines, rather relying on the fact that the petitioner (a citizen) was not an intermediary under the IT Act.⁵⁰¹ This would suggest that only an intermediary would have sufficient standing to challenge the Guidelines. The case in Bombay is one amongst several challenges pending across multiple High Courts and the Supreme Court, and other courts may not come to the same conclusion on the issue of standing. For example, in a petition

492 Press Information Bureau, 'The Government Respects the Right of Privacy and Has No Intention to Violate It When WhatsApp Is Required to Disclose the Origin of a Particular Message' (26 May 2021) <<https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1721915>> accessed 17 September 2021.

493 The Information Technology Act, 2000 s. 87(2)(z).

494 *ibid* s. 87(2)(zg).

495 'Copy of the Writ Petition Filed by *WhatsApp LLC in WhatsApp LLC v Union of India*, WP (C) 7284 of 2021 (High Court of Delhi)' (n 490) 46–50.

496 'Copy of the Writ Petition Filed by Sanjay Kumar Singh in *Sanjay Kumar Singh v Union of India*' <<https://www.medianama.com/wp-content/uploads/2021/03/Social-Media-Rules-Petition-Sanjay-K-Singh.pdf>> accessed 17 September 2021; 'Copy of the Writ Petition Filed by Praveen Arimbrathodiyil in *Praveen Arimbrathodiyil v Union of India*' <https://regmedia.co.uk/2021/04/12/wpc_praveen_08042021.pdf> accessed 17 September 2021.

497 See *Tata Engineering and Locomotive Co Ltd v State of Bihar* 1965 AIR SC 40; *Cf Express Newspaper (Private) Ltd* 1958 AIR SC 578.

498 'Copy of the Writ Petition Filed by Praveen Arimbrathodiyil in *Praveen Arimbrathodiyil v Union of India*' (n 496); 'Copy of the Writ Petition Filed by Live Law Media Pvt Ltd in *Live Law Media Pvt Ltd v Union of India*' <https://drive.google.com/file/d/1JC5zUxx4jXn4OwWOpP_Zowp8YHaHCZsZ/view> accessed 17 September 2021.; 'Copy of the Writ Petition filed by Uday Bedi in *Uday Bedi v Union of India*' in WP (C) 6844 of 2021 (High Court of Delhi) (copy on record with author).

499 *Nikhil Wagle v Union of India* PIL (L) 13204 of 2021 (14 August 2021, High Court of Bombay).

500 Intermediary Guidelines 2021 r. 7.

501 *Nikhil Wagle v Union of India* PIL (L) 13204 of 2021 (14 August 2021, High Court of Bombay) [35].

initiated by an artist, the Madras High Court acknowledged that Part II of the Intermediary Guidelines 2021 may restrict free speech; it passed an order stating that any decisions taken by Indian authorities under Rules 3 and 7 of the Guidelines during the pendency of the dispute would be subject to the Court's final ruling on the issue of the constitutionality.⁵⁰² Additionally, as noted above, the Union Government has asked the Supreme Court of India to transfer all the legal challenges pending in various High Courts to the Supreme Court,⁵⁰³ and the Supreme Court has directed High Courts not to hear legal challenges pertaining to the Intermediary Guidelines 2021.⁵⁰⁴

502 *TM Krishna v Union of India* WP (C) 12515 of 2021 (High Court of Madras, 16 September 2021); Smitha Krishna Prasad and Madhavi Singh, 'IT Rules: Why Madras HC's Ruling on Digital Intermediaries Is Significant' *The Wire* (25 September 2021) <<https://thewire.in/law/it-rules-madras-high-court-ruling-digital-intermediaries-significant>> accessed 2 May 2022.

503 *Jamiat Ulama I Hind v Union of India* WP (C) 787 of 2020 (Supreme Court of India, 2 September 2021).

504 *Skand Bajpai v Union of India* WP (C) 799 of 2020 (Supreme Court of India, 9 May 2022).

(ii) October 2022 Amendment

The October 2022 Amendment made several key changes to the intermediary liability regime: imposing what appears to be a minimal obligation on *all* intermediaries to engage in content moderation; creating a 'notice and action' regime for several categories of content; and creating 'Grievance Appellate Committee(s)' to which users who wish to contest an intermediary's content moderation decision can appeal to. This section of the report discusses the October 2022 Amendment.

Amendment to Rule 3(1): Effect on knowledge and monitoring

Prior to the October 2022 Amendment, Rule 3(1)(b) of the Intermediary Guidelines 2021 required intermediaries to ensure that their terms of service prohibited their users from transmitting or storing a broad list of 'prohibited' content. A list of this 'prohibited' content is set out in the next sub-section below.

Under the October 2022 Amendment, Rule 3(1)(b) has been amended to require intermediaries to "*make reasonable efforts to cause the user*" not to transmit, store, host, or upload 'prohibited' content on the intermediaries' network.⁵⁰⁵ The content of an obligation to 'cause users' not to transmit or upload unlawful content is unclear. One possible interpretation would suggest that the regulation now requires intermediaries to mandatorily engage in a minimal level of content moderation against 'prohibited content'. As commentators have noted, requiring intermediaries to remove content without receiving 'actual knowledge' effectively imposes a disproportionate general monitoring obligation on them,⁵⁰⁶ as they must monitor all users all the time. It may be argued that such an obligation conflicts with (and is thus *ultra*

505 October 2022 Amendment, amendment to r. 3(1).

506 Arnold (n 193) 416.

vires of) the text of Section 79(3) of the IT Act by shifting from an ‘actual knowledge’ approach to a ‘constructive knowledge’ approach.⁵⁰⁷ Unlike ‘actual’ or ‘red-flag’ knowledge triggered by a private notice or court or government order, this would create an obligation on intermediaries (albeit a best-efforts one) to engage in content removal even before being notified of a specific instance of unlawful content. Thus, merely by performing the functions of an intermediary, Rule 3(1)(b) appears to posit that intermediaries *should* know of unlawful content (i.e., amount to a constructive knowledge standard, qualified by the phrase “*reasonable efforts*”). However, the October 2022 Amendment does not provide any guidance on when such an obligation may be satisfied or breached by an intermediary (i.e., how little moderation would fall below the legal threshold of “*reasonable efforts*”). But if such an interpretation is adopted, an intermediary that does not engage in any content moderation may found to be in breach of Rule 3(1)(b). It is relevant to note that this obligation applies to *all* intermediaries, not just SSM Intermediaries, although it is unclear how such an obligation may apply to network intermediaries such as ISPs or other ‘mere conduits’ who do not typically examine or interfere with the content they transmit. Thus, the obligation is best understood as applicable to websites or platforms hosting third-party content.

507 Sethia (n 186) 399. On the difference between actual and constructive knowledge.

Unlike Rule 4(4) of the Intermediary Guidelines which requires SSM Intermediaries to ‘proactively identify’ child sex abuse material or content previously restricted by court or government order, the obligation in the amended Rule 3(1)(b) applies to all ‘prohibited’ content, thus requiring intermediaries to potentially cast a much broader net. Given that Rule 3(1)(b) does not refer to the use of automated technologies or expressly use the phrase ‘proactively identify’, it may be inferred that intermediaries are not under the obligation to deploy sophisticated content classifiers and detection tools to satisfy this obligation. However, until courts clarify what the content of ‘reasonable efforts to cause users not to transmit unlawful content’ is, exactly what types of measures intermediaries may be expected to deploy or how they may be expected to act remains uncertain, especially as what constitutes ‘reasonable efforts’ may vary widely based on intermediary functionality.

The October 2022 Amendment also modifies the list of ‘prohibited’ content. Defamation and libellous content have been completely removed from the list of ‘prohibited’ content.⁵⁰⁸ Thus, intermediaries are not required to make even ‘reasonable efforts’

508 October 2022 Amendment, amendment to r. 3(1).

to cause their users not to transmit or store defamatory content. Finally, the list of ‘prohibited’ content now expressly includes both misinformation and content that promotes enmity between different groups on the grounds of religion or caste with an intent to incite violence.⁵⁰⁹

509 October 2022 Amendment, amendment to r. 3(1).

Rule 3(2): Notice and action in seventy-two hours

After *Shreya Singhal*, an intermediary only risked losing safe harbour if they failed to take down content pursuant to a court or government order against the content, except in cases of copyright content and under Rule 3(2)(b) where intermediaries were required to remove content pursuant to a private notice.⁵¹⁰ However, the October 2022 Amendment now requires intermediaries to ‘act on’ private complaints regarding the following ‘prohibited’ content within seventy-two hours:

510 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382.

- Content that is obscene, pornographic, paedophilic, invasive of another’s privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, relating to or encouraging money laundering or gambling or promoting enmity between different groups on the grounds of religion or caste with an intent to incite violence;
- Content that is harmful to a child;
- Content that deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates misinformation or information which is patently false or untrue, or misleading in nature;
- Content that impersonates another person;
- Content that threatens the unity, integrity, defence, or security or sovereignty of India or its friendly relations with foreign States, public order, or causes the incitement of a cognisable offence, prevents the investigation of any offence, or is insulting to any other nation; or
- Content that contains any software virus or computer code designed to interrupt, destroy, or limit the functionality of any computer resource.

While falling under the category of ‘prohibited’ content

that intermediaries must make reasonable efforts to cause their users not to store or transmit, the following content has been exempted from the seventy-two-hour timeline for ‘acting on’ complaints:

- Content that belongs to another person and to which the user has no right;
- Content that infringes on any patent, trademark, copyright, or other proprietary rights; and
- Content that violates any law.

By requiring intermediaries to ‘act on’ complaints (or lose safe harbour) regarding broad categories of ‘prohibited’ content within seventy-two hours, the amendment to Rule 3(2) by the October 2022 appears to modify the interpretation of ‘actual knowledge’ as a court or government order set out in *Shreya Singhal*. If the term ‘act on’ is interpreted to mean removal, this would directly contradict the interpretation in *Shreya Singhal* by now requiring intermediaries to take down content even based on a private complaint. However, unlike the Intermediary Guidelines 2011, which compulsorily required *removal* within thirty-six hours of a complaint,⁵¹¹ the October 2022 Amendments uses the phrase ‘act on’ a complaint.⁵¹² Unlike ‘actual knowledge’ which requires *removal* under Section 79(3)(b) of the IT Act (or the loss of safe harbour), the amended Rule 3(2) can be interpreted to also permit an intermediary to refuse to remove content, with the obligation under Rule 3(2) merely one of resolving the complaint *one way or another* within seventy-two hours.

511 Intermediary Guidelines 2011 r. 3(4).

512 October 2022 Amendment, amendment to r. 3(2)(i).

If this latter interpretation is adopted, an intermediary will only lose safe harbour if it fails to ‘act on’ a complaint pertaining to the above stated categories within seventy-two hours. Read in this manner, the October 2022 Amendment may be seen as not modifying the law laid down in *Shreya Singhal*, as intermediaries still only risk losing safe harbour if they fail to remove content pursuant to a court or government order. Section 79(3)(b) of the IT Act only mandates removal upon the receipt of “*actual knowledge*” and even after the October 2022 Amendment, Rule 3(1)(d) of the Intermediary Guidelines 2021 continues to use the phrase “*actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government* (emphasis supplied)”. Further, prior to the October 2022 Amendment, Rule

3(2) required intermediaries to dispose of complaints against content within fifteen days, with no suggestion that intermediaries were required to remove content within these fifteen days. This would support the understanding that Rule 3(2) merely sets up a complaint mechanism to be operated at the discretion of the intermediary, and intermediaries continue to retain safe harbour until they refuse to comply with a takedown direction in the form of a court or government order.

An intermediary may refuse (within seventy-two hours) to remove any content pursuant to a user complaint and insist on a court order without losing safe harbour. This would be within its discretion in ‘acting on’ user complaints, and it could claim it has not received ‘actual knowledge’ as understood under Rule 3(1)(d) of the Intermediary Guidelines 2021. Alternatively, intermediaries may read the October 2022 Amendment to Rule 3(2) as imposing a requirement to distinguish between legitimate and frivolous complaints and remove content within seventy-two hours (even though the legal imposition of such an obligation was disfavoured in *Shreya Singhal*). Therefore, the October 2022 Amendment introduces some ambiguity over whether Rule 3(2) now requires intermediaries to *remove* content within seventy-two hours, and the circumstances in which an intermediary may be held to have failed in its obligation to ‘act on’ complaints within this timeline. While this ambiguity may ultimately only be clarified by courts, if intermediaries consistently adopt the latter approach, it would effectively signal a return to the notice and take down regime. This risk is amplified as intermediaries, unable to distinguish between lawful and unlawful content within the short seventy-two-hour timeline may adopt a policy of systematically taking down content to avoid the risk of losing safe harbour.⁵¹³ (Although the amended Rule 3(2) would theoretically also allow them to systematically reject all complaints they are unsure of prior to the seventy-two-hour period expiring.)

513 See Kuczerawy (n 197) 527.

In this regard, the exclusion of defamation and intellectual property claims from such a potential notice and take down regime is normatively desirable, as intermediaries may be unable to determine the nature and legality of such content within seventy-two hours. A court order would balance competing rights before deciding on removal. The requirement of an *ex-ante* judicial order provides a meaningful safeguard against lawful content being taken down. This reasoning is also true for the catch-all category of ‘content that violates any Indian law’, which has also

been excluded from the seventy-two hours complaint timeline. It is notable that under the *Myspace* decision, intermediaries are required to remove allegedly copyright infringing content pursuant to a private complaint.⁵¹⁴ Thus, it remains to be seen whether future courts will read the exclusion of copyright from the seventy-two-hour complaint timeline under Rule 3(2) of the October 2022 Amendment to mean that a court order is required prior to allegedly infringing content is required to be taken down, or whether courts continue to apply the principle set out in *Myspace*.

514 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [54]. For a detailed analysis of the High Court's reasoning, refer to Section 5.2 of this report.

Assuming Rule 3(2) is interpreted to mean intermediaries themselves must remove complained against content within seventy-two hours, this would signal the return of a notice and take down regime for most forms of content and tip India's intermediary liability regime firmly in favour of a protection against online harms and undermine the free speech protections instilled by *Shreya Singhal*. Section 4.1(iv) of this report noted that the notice and take down regime that existed in India under the Intermediary Guidelines 2011 risked lawful content being taken down by failing to provide meaningful safeguards against frivolous or malicious complaints. By compelling intermediaries, at the risk of losing safe harbour, to take down content pursuant to private complaints, an opaque process was created through which content was removed pursuant to communications between complainants and intermediaries with no independent oversight to protect lawful content. Further, intermediaries that received a larger number of requests were forced to distinguish between legitimate and frivolous complaints, effectively becoming arbiters of online speech, an approach eventually rejected by the Supreme Court in *Shreya Singhal*.

The October 2022 Amendment raises these concerns again. But unlike in 2011, there are additional safeguards to prevent the removal of lawful speech. First, as discussed above, the Amendment may itself be interpreted to mean intermediaries do not lose safe harbour for failing to remove content but must merely decide complaints one way or another. Even if the Amendment is interpreted to require removal at the risk of losing safe harbour, as noted above, certain categories of speech where the illegality is hard to determine within a short timeline (defamatory and intellectual property infringing speech) have been excluded from the notice and take down regime and a court order will be required. Third, the October 2022 Amendment

allows intermediaries to ‘develop appropriate safeguards’ to weed out frivolous complaints. While well intentioned, this practice is standard amongst large intermediaries who receive numerous complaints; and the act of distinguishing between legitimate and frivolous complaints was precisely what the Supreme Court in *Shreya Singhal* sought to avoid.⁵¹⁵ The final safeguard against the take down of lawful content pursuant to a private complaint is an appeal to a Grievance Appellate Committee(s) (discussed below) that could direct reinstatement.

515 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121]-[122].

However, other valuable safeguards against lawful content being taken down have not been implemented. The list of ‘prohibited’ content continues to be expansive. For example, an *ex-ante* or even *ex-post* judicial oversight for content allegedly threatening public order or the incitement of violence would have provided stronger speech safeguards. Similarly, the *originator* whose content is complained against and potentially taken down could have been granted a notice or a hearing (i.e., a ‘notice and notice’ regime). Even Rule 4(8), which mandates that SSM Intermediaries provide users with an opportunity to dispute the removal of their content appears not to apply to situations where *another* user complains against their content. Rule 4(8) only applies to situations where SSM Intermediaries take down content on their accord (as opposed to, pursuant to a complaint by another user under the amended Rule 3(2)).⁵¹⁶ Given these factors, the impact of the amendments to Rule 3(2) on free speech will have to be closely monitored.

516 Intermediary Guidelines 2021 r. 4(8).

The Grievance Appellate Committee(s)

The October 2022 Amendment allows users who are aggrieved with any decision by the Grievance Officer of an intermediary to appeal to a ‘Grievance Appellate Committee(s)’ (‘GAC’) within thirty days.⁵¹⁷ Because a user can make a complaint to a Grievance Officer of an intermediary with respect to both their content that has been taken down and against another person’s content, the text of the amendment appears to allow users to appeal to a GAC both against a decision of an intermediary to remove their own content and also a decision by an intermediary to *not* take down another user’s content. Under the October 2022 Amendment, intermediaries have fifteen days to resolve complaints by users whose content has been blocked, but (as discussed above) only seventy-two hours to resolve content removal requests with respect to most ‘prohibited’ content.⁵¹⁸

517 October 2022 Amendment, addition of r. 3A(2).

518 October 2022 Amendment, amendment to r. 3(2)(i).

Each GAC shall consist of a chairperson and two full-time members appointed by the Union Government; of the three members, one member shall be *ex-officio* and the other two shall be independent members.⁵¹⁹ GACs shall attempt to deal with all appeals within thirty days⁵²⁰ through an online dispute resolution mechanism⁵²¹ and may take the assistance of ‘any person having expertise in the subject’.⁵²² Every order issued by a GAC shall be complied with by the intermediary, which is also required to publish a report on its website documenting compliance.⁵²³

It must be remembered that this requirement of compliance itself, as with every other obligation in the Intermediary Guidelines 2021, is itself a pre-condition for safe harbour. Thus, in principle, the consequence of non-compliance with an order of the GAC would be the loss of safe harbour. Where an intermediary has failed to remove content pursuant to a GAC order, an intermediary could be sued or criminally prosecuted for the content in question and would be ineligible for safe harbour. However, if an intermediary has failed to comply with an order of *reinstatement* by the GAC, the loss of safe harbour may be largely inconsequential, as the intermediary would not be hosting or transmitting the content and cannot be held secondarily liable for it.⁵²⁴

519 October 2022 Amendment, addition of r. 3A(2).

520 October 2022 Amendment, addition of r. 3A(4).

521 October 2022 Amendment, addition of r. 3A(6).

522 October 2022 Amendment, addition of r. 3A(5).

523 October 2022 Amendment, addition of r. 3A(7).

524 For a detailed analysis of this reasoning, refer to Section 4.4(ii) of this report.

Potential concerns with the GACs

The first legal concern with the GACs is whether such an adjudicatory body can be created within the rule-making powers under the IT Act. The Intermediary Guidelines 2021, and the October 2022 Amendment, constitute delegated legislation promulgated under Sections 87(1), 87(2)(z), and 87(2)(zg) of the IT Act.⁵²⁵ These provisions empower the MEITY to prescribe the procedure for blocking content under Section 69A of the IT Act and the guidelines to be followed for intermediaries to retain safe harbour under Section 79(2) of the IT Act respectively.⁵²⁶ The text of these rule-making provisions arguably does not envisage the creation of a new quasi-judicial body to govern online content. This interpretation is buttressed by the fact that where Parliament *has* empowered the Union Government to create or appoint adjudicatory bodies or officers to determine violations of the IT Act, it has expressly done so in the parent statute itself (see Chapter X and Section 46), including setting out the jurisdiction, powers, and procedures to be followed by such bodies and officers.⁵²⁷

525 Intermediary Guidelines 2021 Preamble; October 2022 Amendment Preamble.

526 The Information Technology Act, 2000 ss. 87(2)(z), 87(2)(zg).

527 *ibid* ch. X and s. 46.

The independence of the GACs is also uncertain. While the October 2022 Amendment does stipulate that at least two members of every GAC will be independent,⁵²⁸ no additional detail is provided as to how such independence will be secured. For example, selection by an independent body, disclosure of conflict of interests, security of tenure and salary, oath of office, or minimum judicial qualifications (e.g., a retired High Court judge) are some potential safeguards that ordinarily provide guarantees of independence.⁵²⁹ Such independence is vital as the Union Government, or its functionaries or instrumentalities may be a party before the GAC. Therefore, the members of the GACs must be independent to ensure the rule of law, and seen to be independent for users to repose trust in the institution's processes.

528 October 2022 Amendment, addition of r. 3A(2).

529 *L. Chandra Kumar v Union of India* (1997) 3 SCC 261; *Madras Bar Association v Union of India* (2015) 15 SCC 657; *Madras Bar Association v Union of India* (2020) 6 SCC 246; *Rojer Mathew v South Indian Bank Ltd* (2020) 6 SCC 1.

The regulatory efficacy of the GACs will depend on its processes, as it may be confronted with a large volume of appeals. For context, Meta's Oversight Board, which only hears appeals from content moderation decisions made by Facebook and Instagram, recorded over one million user appeals over a fifteen-month period.⁵³⁰ The October 2022 Amendment states that the GACs shall attempt to dispose of appeals within thirty days through an online dispute resolution forum.⁵³¹ However, absent a clearly established procedure for deciding the order in which appeals are heard, there is a risk that the GACs may have wide discretion

530 Oversight Board, 'Oversight Board Publishes First Annual Report' (Oversight Board 2022) 15 <<https://www.oversightboard.com/news/322324590080612-oversight-board-publishes-first-annual-report/>> accessed 3 November 2022.

531 October 2022 Amendment, addition of r. 3A(4), 3A(6).

in the order that appeals are heard, with high profile appeals being heard expeditiously while those of ordinary users (or users from marginalised communities) being heard after a delay when the value of the disputed content is significantly reduced. This concern has been highlighted in the operation of the Supreme Court of India,⁵³² and it remains a possibility in the operation of adjudicatory bodies like the GACs.

Another aspect of concern with respect to the GACs' processes is the lack of an express requirement for notice and hearing for the content originator and the absence of a requirement of a reasoned, written order. For example, if User 1 complains to the Grievance Officer of an intermediary against User 2's content, and the Grievance Officer declines to remove the content, User 1 could appeal to a GAC against this decision of the Grievance Officer. However, the October 2022 Amendment does not stipulate that User 1 must be notified or granted a hearing in such an appeal process, despite it being User 1's content that the GAC is adjudicating. This is in stark contrast to both Rule 4(8) of the Intermediary Guidelines 2021 and the procedure for blocking under Section 69A of the IT Act, which both recognise the originator as an interested party who should ideally be heard before their content is removed.⁵³³

The GACs and Fundamental Rights

Crucially, unlike a content moderation decision taken by a private intermediary, an order by a GAC would amount to a restriction by the *State* on the originator's free expression. Under India's constitutional framework, 'all authorities under the control of the Government of India' must comply with Fundamental Rights, including the right to free speech and expression.⁵³⁴ The issue of free speech is discussed below, but on the issue of process; it is incumbent on a State regulator whose orders have statutory force (such as a GAC⁵³⁵) to abide by principles of natural justice and due process, including passing an order recording reasons.⁵³⁶ Thus firstly, it flows that the originator should be granted a hearing before the relevant GAC before their content is restricted. Second, GACs should issue reasoned orders justifying their decisions. This lack of hearing and reasons may restrict individual's ability to secure their rights to free expression. For example, an order may prove vital if a user wishes to contest a restriction on their free expression imposed by a GAC before a High Court or the Supreme Court.

532 Valay Singh, 'India's Supreme Court in Spotlight over Bail for Divisive Anchor' *Al Jazeera* (13 November 2020) <<https://www.aljazeera.com/news/2020/11/13/india-top-court-under-fire-for-bailing-out-divisive-tv-presenter>> accessed 8 November 2022; Gautam Bhatia, 'Judicial Evasion, Judicial Vagueness, and Judicial Revisionism: A Study of the NCT of Delhi vs Union of India Judgment(s)' (27 June 2020) <<https://papers.ssrn.com/abstract=3637009>> accessed 3 November 2022.

533 Intermediary Guidelines 2021 r. 4(8); Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 G.S.R. 781(E) dated 27 October 2009 r. 8(1).

534 Constitution of India, 1950 arts. 12, 19(1)(a).

535 October 2022 Amendment, addition of r. 3A(7).

536 *Kranti Associates Pvt Ltd v Masood Ahmed Khan* 2010 (9) SCC 496; *Maneka Gandhi v Union of India* 1978 (1) SCC 248.

On the issue of free speech, the operation of the GACs raises important questions. Article 19(2) of the Indian Constitution sets out an exhaustive list of grounds on which the State may restrict free expression, these are: the sovereignty, integrity, or security of the India or its friendly relations with other States, public order, decency or morality, contempt of court, defamation, or the incitement to an offence.⁵³⁷ When a GAC determines that content should be removed for violating the list of ‘prohibited’ content set out in Rule 3(1)(b) of the Intermediary Guidelines, it may amount to a State restriction on the originator’s free expression rights on grounds not stipulated in Article 19(2). This is because the list of ‘prohibited content’ is broader than the terms of Article 19(2). For example, ‘misinformation’, ‘harassing’ or ‘insulting’ content may not necessarily be restricted under Article 19(2) but are regularly flagged on platforms and such subject matter may reach a GAC.

537 Constitution of India, 1950 art. 19(2).

When the Supreme Court in *Shreya Singhal* stipulated that content could only be removed by a court or government order, it noted that such orders should operate within the confines of Article 19(2) of the Constitution.⁵³⁸ Therefore, under *Shreya Singhal* and the Intermediary Guidelines 2021 (prior to the October 2022 Amendment and the GACs), court or government orders removed content that could be removed under Article 19(2) and intermediaries *privately* moderated content that was undesirable but lawful (e.g., misinformation or insulting content). Such moderation was permissible because, as private entities, intermediaries were not required to respect citizens’ Article 19 rights. However, with the establishment of the GACs, the State may be forced to determine how to regulate such ‘lawful but awful’⁵³⁹ speech without falling foul of constitutional restrictions. Lastly, it remains to be seen how intermediaries will respond if a GAC directs them to reinstate content that is lawful but violates their own terms of service.

538 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [122].

539 Keller (n 229).

Additional complications with Fundamental Rights

The October 2022 Amendment requires intermediaries to ‘respect the rights accorded to citizens under the Constitution of India’, including that of the freedom of expression.⁵⁴⁰ As noted above, ‘authorities under the control of the Government of India’ are bound by the Fundamental Rights set out in the Indian Constitution.⁵⁴¹ While social media platforms may influence public discourse, they are not authorities under the control of the government and are not directly bound by the Fundamental Rights

540 October Amendment, amendment to r. 3(1)(n).

541 Constitution of India, 1950 art 12.

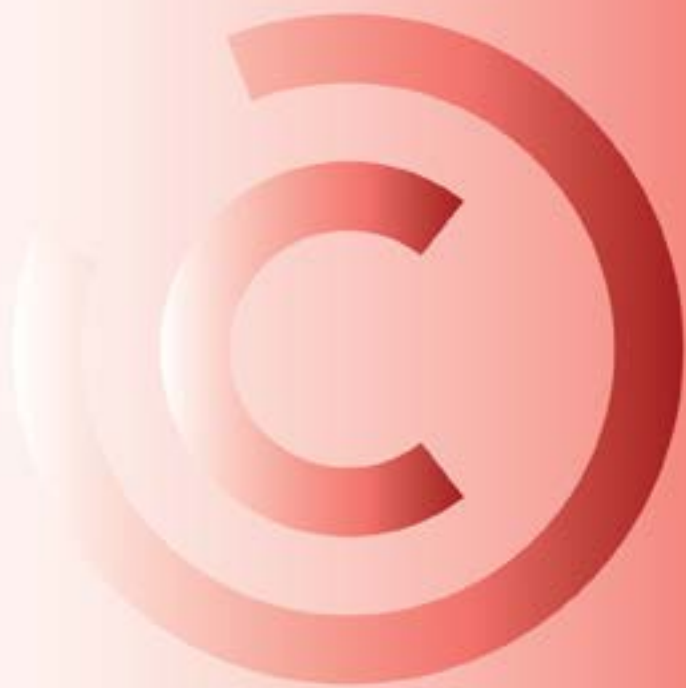
set out by the Indian Constitution. Even if the *contents* of such rights were required to be respected by intermediaries, the contours of such a legal obligation are not immediately discernible and may make compliance and enforcement haphazard and arbitrary.

The text of the Fundamental Rights articulated in the Indian Constitution are intended to operate at a high level of generality and their application to individual situations are typically carried out by State or constitutional functionaries with a high degree of specialised legal knowledge.⁵⁴² These Rights were drafted and have been applied in the context of the State's obligation to its citizens, and it is not be suitable to transpose these into the relationship between private corporations (i.e., intermediaries) and their users.⁵⁴³ The interpretation of these rights, including the freedom of expression, is constantly evolving, open to contestation, and subject to reasonable disagreement.⁵⁴⁴ Their application *vis-à-vis* intermediaries by courts and the government will have to be closely watched.

542 Vasudev Devadasan and Bilal Mohamed, 'Comments to the MEITY on the Proposed Draft for Amendment in Part-I and Part-II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccgnlud-comments-draftamendments-itrules2021-6jul22-301.pdf>>.

543 *ibid.*

544 *ibid.*



5

Safe Harbour Under
the Copyright Act,
1957

The Copyright Act imposes liability for secondary copyright infringement.⁵⁴⁵ Since 2012, the statute offers safe harbour to intermediaries accused of such infringement where storage of the infringing work is “transient or incidental”.⁵⁴⁶ The Copyright Act also provides for an independent notice and takedown regime for allegedly copyright infringing content.⁵⁴⁷ Unlike Section 79 of the IT Act, which offers intermediaries a general safe harbour against offences under any law, the safe harbour under the Copyright Act is specific to the offence of copyright infringement.⁵⁴⁸

Section 81 of the IT Act states that the provisions of the IT Act override all other laws but shall not “restrict any person from exercising any right conferred under the Copyright Act, 1957”.⁵⁴⁹ Courts initially interpreted Section 81 to mean that safe harbour under the IT Act would not apply where copyright actions were brought against intermediaries.⁵⁵⁰ Further, since the Copyright Act provides for its own notice and takedown regime, it was unclear whether the requirement for a court order prior to takedown (post the *Shreya Singhal* decision) would apply to copyright infringement disputes. In 2016, the High Court of Delhi ruled that the safe harbour protection under the IT Act and the Copyright Act operated concurrently,⁵⁵¹ but that no court order was required to take down content in copyright disputes.⁵⁵² According to the High Court of Delhi’s ruling, where an intermediary is accused of secondary copyright infringement, it may invoke both safe harbour under the Copyright Act and safe harbour under the IT Act.

545 The Copyright Act, 1957 s. 51(a)(ii).

546 *ibid* ss. 52(1)(b), 52(1)(c) as amended by The Copyright (Amendment) Act, 2012.

547 *ibid* s. 52(1)(c). Where the storage of the work is “transient or incidental” and for the purpose of providing electronic links, access or integration that has not been prohibited by the rights holder.

548 *See* The Information Technology Act, 2000 s. 79(1) (providing immunity “Notwithstanding anything contained in any law”); The Copyright Act, 1957 s. 52(1) (stating that “following acts shall not constitute an infringement of copyright”).

549 The Information Technology Act, 2000 s. 81.

550 In *Super Cassettes Industries Ltd v Myspace Inc* 2011 SCC OnLine Del 313 [64], a Single Judge of the High Court of Delhi held that where intermediaries were accused of copyright infringement, the proviso to Section 81 excluded intermediaries from availing the general safe harbour under the IT Act, and that intermediaries must rely exclusively on the safe harbour under the Copyright Act.

551 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [51]-[52].

552 *ibid* [54].

5.1. Secondary infringement and safe harbour under the Copyright Act

Section 51(a)(ii) of the Copyright Act creates the offence of secondary copyright infringement while Sections 52(1)(b) and 52(1)(c) offer safe harbour from the offence of infringement. Under Section 51(a)(ii), the offence of secondary copyright infringement occurs if a person “permits for profit any place to be used” for communicating copyright-infringing material to the public unless it “was not aware” or “had no reasonable ground for believing” that such communication would be an infringement.⁵⁵³ Thus, the offence of secondary infringement consists of three elements: (i) the grant of permission; (ii) for profit; and (iii) awareness of the infringement.⁵⁵⁴

(i) Permission, place of profit, and awareness

On the question of whether a website can be a ‘place of profit’, in *Myspace vs. Super Cassettes Industries*, the High Court of Delhi refused to draw a distinction between a virtual and a physical “place”, holding that an online platform could be a place used for profit for the purposes of Section 51(a)(ii).⁵⁵⁵ The High Court consequently ruled that the automated insertion of revenue generating advertisements into copyright infringing music and video content by Myspace would amount to ‘a (virtual) place being used for profit’.⁵⁵⁶ The High Court also relied on Myspace’s insertion of advertisements into infringing material to rule that the intermediary had permitted its platform to be used for profit.⁵⁵⁷ Based on the High Court’s interpretation, the offence of secondary copyright infringement squarely applies to websites and platforms hosting infringing material,⁵⁵⁸ provided the three elements of permission, profit, and awareness are satisfied.

The High Court’s ruling has been criticised for failing to analyse the limb of permission separate from the question of profit.⁵⁵⁹ Sethia argues that a distinct analysis on the question of permission may have found that Myspace’s own user agreement clearly prohibited users from uploading and sharing infringing material, and consequently Myspace could not be construed to have ‘permitted’ the infringing activities on its site.⁵⁶⁰

Courts have ruled that intermediaries have ‘knowledge’ of infringement only where actual and specific notice has been delivered, as opposed to general and constructive knowledge

553 The Copyright Act, 1957 s. 51(a)(ii).

554 Sethia (n 186) 401.

555 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [36]. See also *UTV Software Communications Ltd v 1337x CS* (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019) [34] (relying on the statutory definition of “communication to the public” to hold that making available both online and offline, irrespective of whether the public sees it, amounted to infringement under Section 51 of the Copyright Act).

556 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [36].

557 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [36].

558 See Sethia (n 171) 401; Cf Ananth Padmanabhan, ‘Give Me My Space and Take down His’ (2013) 9 *Indian Journal of Law and Technology* 7. Padmanabhan noting that online and offline ‘places’ cannot be equated under Section 51, as the presumption that an actor can control a physical space (and consequently grant ‘permission’) does not translate to the internet.

559 Sethia (n 186) 401–402.

560 *ibid.*

of infringement on their networks.⁵⁶¹ Unlike the Supreme Court in *Shreya Singhal*, which interpreted “*actual knowledge*” to mean a court order requiring takedown, in copyright disputes, courts have interpreted knowledge to mean actual and specific notice of infringement.⁵⁶² This is sometimes referred to as ‘red-flag’ knowledge, and the standard has been described as, “*whether based on the subjective facts and circumstances, a reasonable observer would objectively discern an infringement.*”⁵⁶³

In *Myspace*, the High Court of Delhi held that there cannot exist a presumption of ‘awareness’ by the intermediary of infringement on its platform, and the mere apprehension of infringement, evidenced through the presence of filters to screen for infringing content, does not establish ‘awareness’⁵⁶⁴ (i.e., actual, and not constructive knowledge). The High Court held that the “*onus is upon the plaintiff to give detailed description of its specific works, which are infringed to enable the web host to identify them.*”⁵⁶⁵ According to the High Court, compliance with a general notice to remove infringing works risked damaging the rights of genuine license holders or other uploaders whose works only ‘superficially resemble’ the plaintiff’s works.⁵⁶⁶ Thus, notice of infringement must be specific to the individual infringed works.⁵⁶⁷ The High Court also held that Myspace’s use of automated systems to insert advertisements was *prima facie* outside its knowledge and control, and did not lead to Myspace’s actual knowledge of the infringement.⁵⁶⁸ However, because ultimately awareness or knowledge is a question of fact, evidence may be led by the plaintiff to establish whether an intermediary was “*aware*” of the infringing content or not.⁵⁶⁹

The result is the creation of two standards of actual knowledge: (i) actual knowledge meaning a court or government order under *Shreya Singhal*; and (ii) actual knowledge meaning notice or an objective determination of knowledge based on facts and circumstances in the case of copyright disputes. The reasoning of the High Court in creating this distinction is discussed below.⁵⁷⁰

(ii) Safe harbour under the Copyright Act

While Section 51(a)(ii) is a liability-imposing provision, Section 52(1) of the Copyright Act sets out two important instances when intermediaries are *not* liable. As with Section 79, the safe harbour clauses in Section 52 are exemptions and therefore only apply after a plaintiff has alleged a case of infringement.⁵⁷¹ Section 52(1)(b) provides safe harbour from copyright infringement in cases where

561 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [38]-[40]. See also; *Siddhi Vinayak Knots & Prints Pvt Ltd v Amazon India* 2017 SCC OnLine Bom 6380; *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201.

562 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [38]-[40]. See also *Tips Industries Ltd. v Glance Digital Experience Pvt Ltd* CS(Comm) 561 of 2020 (High Court of Delhi, 21 December 2020); *Triumphant Institute of Management Education Pvt Ltd v Mega Ltd* CS(Comm) 172 of 2020 (High Court of Delhi, 16 June 2020); *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201.

563 Sethia (n 186) 404.

564 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [38].

565 *ibid* [38].

566 *ibid* [40].

567 See *Tips Industries Ltd. v Glance Digital Experience Pvt Ltd* CS (Comm) 561 of 2020 (High Court of Delhi, 21 December 2020); *Triumphant Institute of Management Education Pvt Ltd v Mega Ltd* CS(Comm) 172 of 2020 (High Court of Delhi, 16 June 2020).

568 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [38] (This was a preliminary finding qualified by the High Court’s observation that “The extent of automation or for that matter the amount of manual/human control can be discerned only at trial once evidence is led to show how the automatic process works”).

569 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [38]; *Kent RO Systems Pvt Ltd v eBay India Pvt Ltd* FAO (OS) (Comm) 95 of 2017 (High Court of Delhi, 1 May 2017).

570 Section 5.2 of this report.

571 Sethia (n 186) 402.

the “*transient or incidental storage*” of a copyrighted work is “*purely in the technical process of electronic transmission or communication to the public*”.⁵⁷² Section 52(1)(c) provides a narrower safe harbour where the temporary storage of the infringing material is “*for the purpose of providing electronic links, access or integration*” that have not been expressly prohibited by the right holder, unless the alleged infringer has knowledge of the infringement.⁵⁷³

572 The Copyright Act, 1957 s. 52(1)(b).

573 The Copyright Act, 1957 s. 52(1)(c).

Interpreting the requirement that the storage be “*transient or incidental*”, the High Court of Delhi drew a distinction between (i) hosting and storing data, which may be accessible and searched for on demand; and (ii) data generated automatically to improve the performance of a core function.⁵⁷⁴ The High Court observed that storage “*which is of a temporary form aiding in the better performance of the main function*” (e.g., caching or web cookies) would be considered temporary,⁵⁷⁵ but noted that “*Problems might arise in the case of stored data, where content, for the purpose of transmission is stored on the server of the service provider.*”⁵⁷⁶ Where websites themselves uploaded and hosted infringing content, they were ineligible for safe harbour.⁵⁷⁷ Similarly, where a platform allowed users to directly download infringing material from its servers, such storage was not incidental or transient.⁵⁷⁸

574 *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [68].

575 *ibid.*

576 *ibid* [63].

577 *UTV Software Communications Ltd v 1337x* CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019) [48].

578 *Tips Industries Ltd v Wynk Music Ltd* Commercial Suit IP 113 of 2018 (High Court of Bombay, 23 April 2019) [41].

579 Sethia (n 186) 402. Referring to parliamentary debate prior to the passage of the safe harbour provisions in Section 52 of the Copyright (Amendment) Act, 2012.

580 *Tips Industries Ltd v Wynk Music Ltd* Commercial Suit (IP) 113 of 2018 (High Court of Bombay, 23 April 2019) [41]; *UTV Software Communications Ltd v 1337x* CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019) [40].

581 The Copyright Act, 1957 s. 52(1)(c).

582 The Copyright Act, 1957 s. 52(1)(c).

The primary purpose of the safe harbour provisions in the Copyright Act was to protect ISPs from liability for infringement.⁵⁷⁹ ISPs would most likely receive safe harbour under Section 52(1)(b) due to their temporary storage and transmission functionality.⁵⁸⁰ Section 52(1)(c) similarly provides a conditional safe harbour to intermediaries where they only temporarily store data “*for the purpose of providing electronic links, access or integration*” where the copyright holder has not expressly prohibited such links, access, or integration.⁵⁸¹ Section 52(1)(c) also imposes a knowledge or awareness requirement similar to Section 52(a)(ii).⁵⁸² However, this safe harbour is conditioned on compliance with a notice and takedown regime set out in the proviso to section 52(1)(c).

(iii) Notice and takedown under the Copyright Act

The proviso to Section 52(1)(c) states that safe harbour shall only be granted if, upon receipt of a written notice by the right holder alleging that the intermediary’s temporary storage of the work amounts to infringement,⁵⁸³ the intermediary takes down the allegedly infringing work for twenty one days, or for a period

583 The Copyright Act, 1957 s. 52(1)(c).

directed by a court.⁵⁸⁴ Where no court order is received within twenty one days, the intermediary “*may*” reinstate the content.⁵⁸⁵

The proviso to Section 52(1)(c) thus sets up a notice and takedown regime for allegedly infringing material, but one that also permits reinstatement unless judicially directed otherwise. The Copyright Rules, 2013 (**‘Copyright Rules’**) sets out the procedure to be followed once a copyright holder provides a written notice to the intermediary.⁵⁸⁶

There exists a discrepancy between the statutory text of Section 52(1)(c) and the Copyright Rules on whether an intermediary has any discretion in effectuating takedown after receiving a notice.⁵⁸⁷ Section 52(1)(c) states that the person storing the allegedly infringing work “*shall refrain from facilitating such access*”,⁵⁸⁸ while Rule 75(3) of the Copyright Rules states that “[the intermediary] *if satisfied from the details provided in the complaint that the copy of the work is an infringed copy*” shall disable access to the work.⁵⁸⁹ However, as the Copyright Act constitutes primary legislation, it would override contrary provisions in subordinate legislation such as Rule 75(3).⁵⁹⁰ Thus, the obligation to take down content upon receipt of a written complaint alleging infringement can be considered mandatory.

Under the Copyright Rules, a notice alleging infringement must identify and describe the work,⁵⁹¹ establish the complainant as the copyright owner or exclusive licensee of the original work,⁵⁹² establish the disputed material as infringing,⁵⁹³ provide the location of the work⁵⁹⁴ (ordinarily a URL), and where possible, the details of the person responsible for uploading the work (the originator).⁵⁹⁵ Upon receiving such a notice, the intermediary shall disable access to such content within thirty six hours.⁵⁹⁶

The Copyright Rules also provide measures that aid transparency. Intermediaries must display the reasons for disabling access to anyone trying to access the content.⁵⁹⁷ Crucially however, access to the disputed material may be restored after twenty one days unless the complainant can procure a court order directing the intermediary to take down the content permanently (or for a period greater than twenty one days).⁵⁹⁸ If the complainant fails to procure a court order directing the takedown, the intermediary is not obligated to respond to future notices by the complainant regarding the same material.⁵⁹⁹

584 The proviso to Section 52(1)(c) states “for a period of twenty-one days or till he receives an order from the competent court from facilitation access”.

585 The Copyright Act, 1957 s. 52(1)(c).

586 The Copyright Rules, 2013 G.S.R. 172(E) dated 14 March 2013 [Copyright Rules] r. 75.

587 Sethia (n 186) 405.

588 The Copyright Act, 1957 s. 52(1)(c).

589 Copyright Rules r. 75(3).

590 *Nova Ads v Metropolitan Transport Corporation* 2015 (13) SCC 257 [40]-[43]; Sethia (n 186) 405.

591 Copyright Rules r. 75(2)(a).

592 Copyright Rules r. 75(2)(b).

593 Copyright Rules r. 75(2)(c).

594 Copyright Rules r. 75(2)(d).

595 Copyright Rules r. 75(2)(e).

596 Copyright Rules r. 75(3).

597 Copyright Rules r. 75(4).

598 The Copyright Act, 1957 s. 52(1)(c).

599 Copyright Rules r. 75(6).

5.2. Safe harbour under the IT Act for copyright infringement

As noted above, the safe harbour under the Copyright Act only applies to select cases of ‘transient and incidental’ storage of copyright infringing material. Given the narrow import of this protection, there arose a question of whether intermediaries could claim safe harbour under the broader immunity provided by Section 79 of the IT Act against secondary liability for copyright infringement. The decision by a Division Bench of the High Court of Delhi in *Myspace vs. Super Cassettes Industries* analysed the interaction between the safe harbour regimes under the Copyright Act and the IT Act. Myspace operated a social media and entertainment website where users could post, share, and access music and videos without paying any fees. After becoming aware of copyright-infringing content on Myspace’s website in 2008, Super Cassettes Industries Ltd. (‘SCIL’) filed a suit alleging that Myspace was facilitating the infringement of its intellectual property under Section 52(a)(ii) and had failed to take down copyright-infringing content despite repeated notices from SCIL.⁶⁰⁰ In addition to opposing SCIL’s claims under the Copyright Act, Myspace sought immunity under Section 79 of the IT Act.

⁶⁰⁰ *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [5]-[7].

The High Court of Delhi was *inter alia* required to determine whether Myspace could avail of the general safe harbour provided by Section 79 of the IT Act in the case of copyright claims. This issue arose as the proviso to Section 81 of the IT Act expressly stated that the IT Act did not restrict “any person from exercising any right conferred under the Copyright Act, 1957”.⁶⁰¹ The High Court expressly refused to address the extent of the infringement as this was a matter for trial.⁶⁰²

⁶⁰¹ The Information Technology Act, 2000 s. 81.

⁶⁰² *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [32].

(i) The decision of the High Court in *Myspace*

The High Court of Delhi ruled that the proviso to Section 81 did not bar the intermediary from seeking immunity under the general safe harbour provided by the IT Act.⁶⁰³ According to the High Court, the saving language in the proviso to Section 81 merely preserved the right of copyright owners to bring an action against intermediaries where they may be liable for secondary infringement, as without the proviso it would be impossible to hold intermediaries liable for secondary copyright action.⁶⁰⁴ The proviso to Section 81 did not bar intermediaries from seeking safe harbour under Section 79, which neither imposes liability nor provides absolute immunity.⁶⁰⁵ Simply put, Section 79 does not

⁶⁰³ *ibid* [66].

⁶⁰⁴ *ibid* [52].

⁶⁰⁵ *ibid* [51]-[52].

“restrict any person from exercising any right conferred by the Copyright Act”; it merely provides them with a conditional immunity, in situations where third parties upload infringing content. Thus, the proviso to Section 81 does not bar intermediaries from seeking safe harbour under Section 79 in copyright actions.

This reasoning created one last issue for the High Court to resolve. If an intermediary could avail of safe harbour under Section 79 of the IT Act, the standard of ‘knowledge’ under Section 79 would also be applicable. After the *Shreya Singhal* judgement, the standard for when an intermediary had knowledge under Section 79 was “actual knowledge” in the form of a court order. However, in interpreting Section 51(a)(ii) of the Copyright Act, the High Court had ruled that actual and specific notice by a plaintiff would be the appropriate standard to determine when an intermediary was aware of infringing content on its platform. To resolve this divergence, the High Court drew a distinction between content which was sought to be restricted under Article 19(2) of the Indian Constitution⁶⁰⁶ and content which was sought to be taken down for infringing copyright. According to the High Court, in the case of the latter, it was sufficient that the copyright owner provides a specific notice of the infringing works in the prescribed format for an intermediary to effectuate removal.⁶⁰⁷

(ii) Impact and analysis of the High Court’s decision in *Myspace*

The effect of the decision in *Myspace* is to create two parallel regimes of safe harbour based on the nature of illegality alleged against the content. Where the illegality alleged against the content is not copyright infringement, Section 79 of the IT Act and the *Shreya Singhal* test for ‘knowledge’ will apply, and an intermediary will not be at risk of losing safe harbour until receiving a court or government order directing removal of content. Where the illegality alleged against the content is copyright infringement, the ‘actual and specific notice’ standard of ‘knowledge’ will apply, and an intermediary will be compelled to take down content upon receipt of a private legal notice or risk losing safe harbour.

Although the High Court opined that an intermediary may avail of safe harbour under Section 79 of the IT Act in copyright actions, by changing the threshold at which intermediaries risk

⁶⁰⁶ Under Article 19(2) of the Constitution of India, reasonable restrictions may be placed on speech in the interests of: “the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.”

⁶⁰⁷ *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 [54].

losing safe harbour from a court order to a private notice, the High Court removed a key protection for intermediaries that makes Section 79 of the IT Act a more robust safe harbour provision than Section 52 of the Copyright Act. Critics of this aspect of the High Court's approach have argued that requiring intermediaries to take down content upon receipt of a private notice (albeit a specific and verifiable one) may result in overcompliance and the chilling of legitimate speech.⁶⁰⁸

608 Sethia (n 186) 404.

One potential reconciliation of the two standards for knowledge or awareness outlined in *Myspace* and *Shreya Singhal* lies in the qualitatively different nature of the content in question, and the differential notice and takedown procedures associated with them. The Supreme Court in *Shreya Singhal* was concerned with abusive takedown notices from private parties resulting in the horizontal censorship of speech that may otherwise have been accorded a high degree of protection. The decision in *Myspace* was aimed at providing an effective remedy to copyright owners and tackling the harms of online piracy. Another consideration for the *Myspace* court may have been that the Copyright Rules expressly contemplated reinstatement of the content absent a court order within twenty-one days, negating concerns of content being indefinitely taken down absent judicial scrutiny.

Apart from the court order requirement, there are also other distinctions between the safe harbour under Sections 52(1)(b) and 52(1)(c) of the Copyright Act and Section 79 of the IT Act. For example, availing safe harbour under Section 79 does not require an intermediary to prove that its temporary storage of unlawful content was for the purpose of providing links or access. However, Section 79 has its own requirements (coupled with those set out in the Intermediary Guidelines 2021) that an intermediary must satisfy to avail of safe harbour.

Frameworks that are appropriate in commercial contexts may raise concerns of free speech being restricted in less commercially oriented products.⁶⁰⁹ The decision in *Myspace* may be viewed as an attempt to create a pragmatic and operable framework for copyright claims within a context where speech concerns were lower, and the Copyright Rules were already more protective of content than the Intermediary Guidelines 2021. However, these distinctions may collapse where substantial free speech or other constitutionally protected interests are implicated in an intellectual property context. For example, in 2020, several

609 Frederick Mostert, 'Intermediary Liability and Online Trade Mark Infringement: Emerging International Common Approaches' in Giancarlo Frosio (ed), Frederick Mostert, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 374.

publishers including Elsevier sought to obtain an injunction against the websites ‘Sci-Hub’ and ‘Library Genesis’ for hosting infringing research materials such as scientific articles and books.⁶¹⁰ Several scientists and research organisations intervened before the High Court of Delhi, arguing that that under Indian law, scientific knowledge is a public resource.⁶¹¹ On January 6, 2021, the High Court refused to grant an injunction against the sites and Sci-Hub agreed not to publish any fresh material from the plaintiff publishers’ journals.⁶¹² Similarly, research has demonstrated that newsworthy content has been removed through abusive copyright notices to intermediaries.⁶¹³ Another example of significant public interest in a copyright dispute is where a court directed the ‘temporary’ blocking of Twitter accounts associated with a political party for alleged copyright violations.⁶¹⁴

610 Divya Trivedi, ‘Cases against Sci-Hub and Libgen Imply Long-Term Consequences to Research and Education in India’ *Frontline* <<https://frontline.thehindu.com/the-nation/locking-up-research-cases-against-sci-hub-and-libgen-imply-long-term-consequences-to-research-and-education-in-india/article33641506.ece>> accessed 12 March 2021.

611 *ibid.*

612 *ibid.*

613 Shreya Tewari, ‘Over Thirty Thousand DMCA Notices Reveal an Organized Attempt to Abuse Copyright Law’ (*Lumen*, 22 April 2022) <https://lumendatabase.org/blog_entries/over-thirty-thousand-dmca-notices-reveal-an-organized-attempt-to-abuse-copyright-law> accessed 19 September 2022.

614 Aarathi Ganesan, ‘Bengaluru Court Orders Twitter to Block Congress Handles over Copyright’ (*MediaNama*, 8 November 2022) <<https://www.medianama.com/2022/11/223-bengaluru-civil-court-order-twitter-congress-copyright/>> accessed 2 December 2022.



6

Safe Harbour for E-Commerce Entities

Section 2(1)(w) of the IT Act defines an “*intermediary*” to include entities that “*provide any services with respect to an electronic record*” and explicitly includes “*online-auction sites, online-market places and cyber cafes.*”⁶¹⁵ This language demonstrates Parliament’s intent to make certain electronic commerce (e-commerce) platforms eligible for the safe harbour provided by Section 79 of the IT Act. In the past, the offering of physical services and possessing inventory in connection with online transactions gave rise to uncertainty over whether all e-commerce providers are ‘intermediaries’ eligible for safe harbour.⁶¹⁶ However, the Union Government has since enacted new consumer protection legislation and cognate rules which expressly state the types of e-commerce platforms eligible for safe harbour under Section 79 of the IT Act.⁶¹⁷

615 The Information Technology Act, 2000 s. 2(1)(w).

616 *Christian Louboutin Sas v Nakul Bajaj* 2018 SCC OnLine Del 12215.

617 Consumer Protection (E-Commerce) Rules, 2020 G.S.R. 462(E) dated 23 July 2020 [E-Commerce Rules] r. 5(1).

6.1. Consumer Protection Act 2019 and the E-Commerce Rules 2020

The Consumer Protection Act, 2019 ('Consumer Protection Act') was brought into effect on July 20, 2020. Section 2(7) of the legislation defines a "consumer" as any person buying goods or availing of services, and an explanation to the provision states that such activity "includes offline or online transactions through electronic means".⁶¹⁸ The statute further defines an "electronic service provider" as a person providing "technologies or processes" to facilitate the sale of goods and services to consumers and explicitly includes "any online market place or online auction site".⁶¹⁹ The statute thus distinguishes between a "product seller" (selling its own goods and services to consumers)⁶²⁰ and an "electronic service provider" (facilitating the sale of goods and services for product sellers).⁶²¹

618 The Consumer Protection Act, 2019 s. 2(7).

619 *ibid* s. 2(17).

620 *ibid* s. 2(37).

621 *ibid* s. 2(17).

(i) Safe harbour for e-commerce entities

The Consumer Protection (E-Commerce) Rules, 2020 ('E-Commerce Rules') were notified on July 23, 2020 and define an "e-commerce entity" broadly as any person who owns, operates, or manages a "digital or electronic facility or platform for electronic commerce".⁶²² The E-Commerce Rules also define 'inventory e-commerce entities' and 'marketplace e-commerce entities' as two distinct subsets of e-commerce entities. An "inventory e-commerce entity" is an e-commerce entity which sells its own inventory of goods or services directly to consumers over an electronic platform.⁶²³ In contrast, a "marketplace e-commerce entity" is an e-commerce entity which provides an electronic platform to "facilitate transactions between buyers and sellers".⁶²⁴ A seller on a marketplace e-commerce entity is not itself an e-commerce entity.⁶²⁵

622 E-Commerce Rules r. 3(b).

623 E-Commerce Rules r. 3(f) (this includes both single brand retailers and multi-channel single brand retailers).

624 E-Commerce Rules r. 3(g).

625 E-Commerce Rules r. 3(b).

The E-Commerce Rules expressly state that a marketplace e-commerce entity may seek safe harbour under Section 79 of the IT Act in accordance with the conditions set out under the IT Act and the Intermediary Guidelines.⁶²⁶ Where an e-commerce platform is selling its own goods and services directly to the end-user (i.e., an inventory e-commerce entity), it is arguably not entitled to claim safe harbour by virtue of Section 79(2)(c) of the IT Act – as it uploads the content (the listing), thus initiating the transmission, a condition that breaches the requirements of Section 79(2) of the IT Act. It is closer to a web publisher than an intermediary.

626 E-Commerce Rules r. 5(1).

Relying on the E-Commerce Rules, the High Court of Karnataka refused to impose liability for the sale of unlicensed medicines on the e-commerce Snapdeal's online platform.⁶²⁷ Describing the platform's functionality, the High Court noted, "*When a Buyer elects to purchase a product through the website, Snapdeal shall receive the order for the product only in the capacity of an online marketplace.*"⁶²⁸ The High Court went on to rule, "*As such Snapdeal would come within the meaning of a marketplace e-commerce website, thereby affording the above exemption to Snapdeal so long as the requirements under Section 79 are followed.*"⁶²⁹ The High Court placed significant emphasis on the fact that Snapdeal's agreements with sellers expressly barred the sale of medicines.⁶³⁰

It is possible that a single entity may act as both a marketplace e-commerce entity and as an inventory e-commerce entity. The E-Commerce Rules do not indicate whether an entity's classification as a marketplace e-commerce entity (eligible for safe harbour) or an inventory e-commerce entity (ineligible for safe harbour) will be determined based on its overall functionality or its functionality in the context of a specific transaction, though as safe harbour is determined on a case-by-case basis, it should be the latter. Finally, as Section 79(1) of the IT Act states that the immunity provided overrides other laws, the provisions of the Consumer Protection Act and the E-Commerce Rules should not dilute the safe harbour e-commerce platforms are entitled to (provided they are intermediaries as defined by the IT Act) beyond the conditions set out in Sections 79(2) and 79(3) of the IT Act. In other words, if a marketplace e-commerce entity can satisfy the requirements of Sections 2(1)(w) and 79, it should be exempt from liability for hosting unlawful content under the Consumer Protection Act and the Trade Marks Act, 1999 ('**Trade Marks Act**').

Trademark litigation

Actions against e-commerce platforms often involve claims that a platform is liable for trademark infringement under the Trade Marks Act⁶³¹ for listing counterfeit products.⁶³² Unlike in the case of copyright or patents, Section 81 of the IT Act does not carve out any specific exemption for trademark disputes, removing any potential legal barriers from intermediaries availing safe harbour for trademark infringement. As Section 79(1) of the IT Act states that the immunity conferred therein overrides other laws, an intermediary is entitled to safe harbour in trademark infringement suits provided it satisfies the requirements of

627 *Kunal Bahl v State of Karnataka Cri (P)* 4676 of 2020 (High Court of Karnataka, 7 January 2021).

628 *ibid* [4.11].

629 *ibid* [12.10].

630 *ibid* [12.7]-[12.9].

631 *See* The Trade Marks Act, 1999 ss. 101, 102.

632 *See Metro Shoes Ltd v Tolexo Online Pvt Ltd* 2016 SCC OnLine Bom 9998; *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201; *Christian Louboutin Sas v Nakul Bajaj* 2018 SCC OnLine Del 12215; *L'Oreal v Brandworld* 2018 SCC OnLine Del 12309; *Luxottica Group SPA v Mify Solutions Pvt Ltd* 2018 SCC OnLine Del12307; *Skullcandy Inc v Shyam Telecom* 2018 SCC OnLine Del 12308.

Section 79 of the IT Act and the Intermediary Guidelines.⁶³³

Standard of knowledge for e-commerce platforms

In determining when an e-commerce platform had ‘knowledge’ of unlawful content on its platform, courts have not always interpreted ‘actual knowledge’ to mean a court order as set out in *Shreya Singhal*. In a trademark dispute, a Single Judge of the High Court of Delhi refused to impose a general monitoring obligation on e-commerce platforms to proactively monitor and take down counterfeit listings.⁶³⁴ On appeal, a Division Bench of the High Court upheld the reasoning of the Single Judge but also ruled that the plaintiffs may lead evidence at trial to establish that the intermediary had ‘knowledge’ of the infringement but refused to act on it.⁶³⁵ The Division Bench opined that such evidence would determine whether the intermediary satisfied the requirements of Section 79(3)(b) of the IT Act and could consequently claim safe harbour.⁶³⁶ This application of the ‘objective determination of knowledge based on facts and circumstances’ standard may suggest that courts are inclined to extend the distinction created in *Myspace*, between unlawful content that may be restricted under Article 19(2) of the Indian Constitution and copyright-infringing content, to trademark disputes concerning counterfeit products.

The High Court of Karnataka drew a distinction between “*unlawful acts*” online, where actual knowledge would mean a court order, and ‘infringements of commercial rights’ where the ‘objective determination of knowledge based on facts’ approach would apply.⁶³⁷ For example, in the above mentioned decision concerning Snapdeal, where criminal liability was sought to be imposed under the Drugs and Cosmetics Act, 1940, the High Court of Karnataka reiterated the court order requirement of *Shreya Singhal*, ruling that content could only be taken down “*upon receipt of either a court order or by notice by an appropriate government authority and not otherwise*”⁶³⁸

More recently, a Single Judge of the High Court of Delhi ruled that the standard for actual knowledge in trademark disputes should be that of a court order.⁶³⁹ The Single Judge noted that disputes over trademark are “*often a stoutly contested affair even before a civil court,*” and that “*intermediaries are certainly not situated to determine the correctness of a claim by a complainant to a trademark.*”⁶⁴⁰ This line of reasoning is consistent with the decision in *Shreya Singhal* and Rule 3(1)(d) of the Intermediary

633 See *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201; *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454.

634 *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201 [30]-[35].

635 *Kent RO Systems Pvt Ltd v eBay India Pvt Ltd* FAO (OS) (Comm) 95 of 2017 (High Court of Delhi, 1 May 2017).

636 *ibid.*

637 *Amazon Seller Services Pvt Ltd v Indusviva Health Sciences Pvt Ltd* MFA 8411 of 2018 (High Court of Karnataka, 28 August 2019).

638 *Kunal Bahl v State of Karnataka Cri (P)* 4676 of 2020 (High Court of Karnataka, 7 January 2021) [12.14].

639 *Flipkart Internet Pvt Ltd v State of NCT of Delhi Writ Petition (Cri)* 1376 of 2020 (High Court of Delhi, 17 August 2022) [27]-[28].

640 *ibid* [27]-[28].

Guidelines 2021, with even the October 2022 Amendment to the Guidelines not requiring intermediaries to ‘act on’ user complaints pertaining to intellectual property within seventy-two hours. However, given the lack of a clear line of judicial decisions on the subject, there exists some uncertainty over how courts will interpret the standard of knowledge applicable to e-commerce platforms,⁶⁴¹ and how the knowledge requirement will vary based on the illegality alleged against the content in question.

641 See Vasundhara Majithia, ‘The Changing Landscape of Intermediary Liability for E-Commerce Platforms: Emergence of a New Regime’ 15 *The Indian Journal of Law and Technology* 470.

(ii) Additional obligations on e-commerce entities

The E-Commerce Rules also impose certain substantive consumer protection obligations on online platforms engaging in electronic commerce. These obligations are not linked to hosting unlawful content, but intermediaries acting as e-commerce platforms will be required to comply with them under the Consumer Protection Act. E-commerce entities are obligated to display the address of the entity and both its geographic and web address on their platforms.⁶⁴² The E-Commerce Rules also require the appointment of a nodal point of contact who is resident in India⁶⁴³ and a customer care and grievance officer whose contact details should be clearly accessible.⁶⁴⁴ In the event of a consumer complaint, the grievance officer is obligated to acknowledge the receipt of the complaint within forty-eight hours and provide redress within one month.⁶⁴⁵

642 E-Commerce Rules r. 4(2).

643 E-Commerce Rules r. 4(1)(b).

644 E-Commerce Rules r. 4(2).

645 E-Commerce Rules r. 4(5).

In the case of marketplace e-commerce entities, entities are required to prominently display the details of the sellers including the name of the business, the geographic address, customer care number, rating or aggregated feedback, and identify whether the business is registered or not.⁶⁴⁶ After a purchase on the platform, if a consumer makes a written request for information regarding the seller, the marketplace e-commerce entity shall provide any information necessary for the buyer to communicate with the seller (for the purposes of dispute resolution).⁶⁴⁷ Finally, marketplace e-commerce entities shall make “reasonable efforts” to maintain a record of sellers who have repeatedly offered goods or services which have been previously removed (from the entity’s platform) for violating the Copyright Act, the Trade Marks Act, or the IT Act.⁶⁴⁸ The e-commerce marketplace entity is not legally obligated to terminate such a seller’s access to the platform, but may voluntarily do so.⁶⁴⁹

646 E-Commerce Rules r. 5(3)(a).

647 E-Commerce Rules r. 5(3)(a).

648 E-Commerce Rules r. 5(5).

649 E-Commerce Rules r. 5(5).

(iii) Draft amendments to the E-Commerce Rules

In June 2021, the Union Ministry of Consumer Affairs released draft amendments to the E-Commerce Rules 2020 and invited public comments on the proposed amendments.⁶⁵⁰ The draft amendments require all e-commerce entities to register themselves with the Department for Promotion of Industry and Internal Trade, which shall provide the entities with a registration number to be displayed on all invoices issued by the e-commerce entity.⁶⁵¹ Further, e-commerce entities are required to appoint a Chief Compliance Officer, a Resident Grievance Officer, and a nodal contact person.⁶⁵² As in the case with the Intermediary Guidelines 2021, the Chief Compliance Officer shall be liable for any ‘unlawful’ third-party content made available or hosted by the e-commerce entity.⁶⁵³ Finally, e-commerce entities must not allow the displaying of misleading advertisements on their platforms,⁶⁵⁴ and prominently display the name of the seller (in the same font size as the e-commerce entity) on all invoices.⁶⁵⁵

The proposed amendments to the E-Commerce Rules do not remove or restrict the ability of marketplace e-commerce entities to avail of safe harbour under Section 79 of the IT Act. However, the draft rules state that marketplace e-commerce entities will be subject to “*fall-back liability*”,⁶⁵⁶ i.e., a marketplace e-commerce entity will be liable if a consumer suffers a loss due to a registered seller on its platform failing to fulfil its obligations to consumers ‘in the manner prescribed by the marketplace e-commerce entity’.⁶⁵⁷

The Draft E-Commerce Rules extend the regulatory logic of the Intermediary Guidelines 2021 in seeking to hold online platforms more accountable for the content they host and the real-world harms they may cause. This is best exemplified by the inclusion of “*fall-back liability*” to protect consumers from fraudulent sellers on e-commerce platforms. The draft rules are also representative of the recent trend mandating local officers for intermediaries. This is intended to increase the accountability of online entities to Indian authorities. Local officers may be subject to penal sanctions if the intermediary fails to assist investigative agencies or comply with government regulations. However – in response to concerns that, if enacted, the new rules would disrupt the growth of e-commerce entities and stifle investment – the Union Government is said to be re-examining the draft rules.⁶⁵⁸

650 ‘Deadline for Suggestions on Draft E-Commerce Rules Extended till July 21’ *Hindustan Times* (5 July 2021) <<https://www.hindustantimes.com/business/deadline-for-suggestion-on-draft-e-commerce-rules-extended-till-july-21-101625497613528.html>> accessed 15 July 2021.

651 ‘Proposed amendments to Consumer Protection (E-Commerce) Rules, 2020’ <https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Comments_eCommerce_Rules2020.pdf> accessed on 15 October 2021 [Draft E-Commerce Rules 2021] r.4.

652 Draft E-Commerce Rules 2021 r. 5(5).

653 Draft E-Commerce Rules 2021 r. 5(5)(a).

654 Draft E-Commerce Rules 2021 r. 5(3).

655 Draft E-Commerce Rules 2021 r. 5(19).

656 Draft E-Commerce Rules 2021 r. 6(9).

657 Draft E-Commerce Rules 2021 r. 6(9).

658 Samyak Pandey, ‘Govt to Revisit Draft E-Commerce Rules as Liability, Grievance Redressal Norms Draw Backlash’ (*The Print*, 1 September 2021) <<https://theprint.in/india/governance/govt-to-revisit-draft-e-commerce-rules-as-liability-grievance-redressal-norms-draw-backlash/725712/>> accessed 14 September 2021.

6.2. Contested functionality of e-commerce platforms

There has existed uncertainty over whether e-commerce platforms were ‘intermediaries’ under the IT Act, and when exactly they were entitled to safe harbour. For example, the High Court of Patna refused to stop criminal proceedings against the e-commerce platform India Mart, when a seller on the platform had taken payment but refused to provide the goods in question.⁶⁵⁹ The High Court went on to state, “Section 79 no where talks of granting any exemption from prosecution for an act of fraud committed by a supplier using the Website of the intermediary”.⁶⁶⁰ However, this decision was later reversed by the Supreme Court which ruled that India Mart merely provided a platform for the fraudulent transaction and was thus entitled to safe harbour under Section 79 of the IT Act.⁶⁶¹

In 2018, the case of *Christian Louboutin vs. Nakul Bajaj* held that if an e-commerce entity offered certain physical services (such as transporting products and providing quality assurances), it could no longer be termed an “intermediary”.⁶⁶² According to the High Court of Delhi, offering such services would render the entity an ‘active participant’, consequently disentitling the platform from safe harbour.⁶⁶³ These observations were questioned by a subsequent decision in *Amazon Seller Services vs. Amway India Enterprises*,⁶⁶⁴ which held that physical services were not fundamentally incompatible with an e-commerce platform’s status as an “intermediary” under the IT Act. It is thus worth closely examining the High Courts’ observations in the above-mentioned cases.

(i) *Christian Louboutin vs. Nakul Bajaj*

‘Christian Louboutin’ was a registered trademark in India and Christian Louboutin Sas sold its luxury products through an authorised network of exclusive distributors in India. Christian Louboutin Sas brought an action for trademark infringement against Darveys.com (an online shopping platform) for selling luxury products with the Christian Louboutin brand name and logo. In response, the defendants contended that they were not selling the products but merely facilitating customer orders for various sellers across the world. A Single Judge of the High Court of Delhi opined that the defendant’s case rested entirely on its claim to safe harbour as an intermediary under Section 79 of the IT Act, and decided the case based on the written submissions of the parties without calling for evidence on the website’s operations.⁶⁶⁵

659 *Dinesh Agrawal v State of Bihar* WP (Cri) 347 of 2018 (High Court of Patna, 2 May 2018).

660 *ibid.*

661 *Dinesh Agrawal v State of Bihar* Criminal Appeal 1356 of 2019 (Supreme Court of India, 7 November 2019).

662 *Christian Louboutin Sas v Nakul Bajaj* 2018 SCC OnLine Del 12215. *See also Amazon Seller Services Pvt Ltd v Indusviva Health Sciences Pvt Ltd* MFA 8411 of 2018 (High Court of Karnataka, 28 August 2019) (noting that the issuance of bills in the name of the e-commerce platform and providing logistical support may disentitle an e-commerce platform from availing of safe harbour under Section 79 of the IT Act).

663 *Christian Louboutin Sas v Nakul Bajaj* 2018 SCC OnLine Del 12215 [66].

664 2020 SCC OnLine Del 454.

665 *Christian Louboutin Sas v Nakul Bajaj* 2018 SCC OnLine Del 12215 [7].

The High Court began by acknowledging that Section 2(1)(w) of the IT Act contemplated an entity that “*receives, stores or transmits a particular electronic record or provides a service with respect to the record*”.⁶⁶⁶ However, the High Court then proceeded to list a series of activities that it opined would extend beyond what was permissible under the phrase ‘a service with respect to a record’. In other words, ‘a service with respect to a record’ did not mean ‘*any* service with respect to a record’.⁶⁶⁷ This is a notable inquiry in and of itself, as previous courts had not examined ancillary services provided by platforms.

666 *ibid* [59].

667 *ibid* [60].

According to the High Court in *Christian Louboutin*, the list of activities that were outside the scope of permissible services *inter alia* included: (i) transporting products from the seller to the platform’s warehouse; (ii) uploading the entry of the product on the website; (iii) providing quality assurances and authenticity guarantees; (iv) enrolling members upon payment of a membership fees; (v) promoting or advertising the products on its platform; (vi) packaging products and transporting them to the purchaser; (vii) employing delivery personnel; (viii) accepting cash or payments through promoted payment gateways; and (ix) booking ad-space on search engines and using trademarks through meta-tags to attract web-traffic.⁶⁶⁸

668 *ibid* [59].

In the High Court’s view, where e-commerce platforms or online marketplaces undertook these activities, they transcended the ‘inactive’ role as “*mere conduits or passive transmitters*” envisaged for intermediaries under the IT Act.⁶⁶⁹ Further, the High Court observed that undertaking this ‘active’ role by e-commerce platforms may rise to ‘aiding, conspiring, inducing, abetting or aiding’ trademark infringement, and such platforms would be disentitled from safe harbour as they violated the requirement set out in Section 79(3)(a) of the IT Act.⁶⁷⁰ The High Court opined that the storage of counterfeit goods, use of trademarks on invoices, advertising products using a registered trademark to promote the sale of counterfeit products, enclosing counterfeit products in its own packaging would “*aid the infringement or falsification*” and thus disentitle an e-commerce platform from safe harbour.⁶⁷¹ In these circumstances, the High Court found Darveys.com to be promoting the sale of counterfeit products and ineligible for immunity under Section 79 of the IT Act.⁶⁷² However, as Darveys.com contended that it had not actually sold any Louboutin goods (despite they being advertised on the platform), the High Court did not impose monetary damages on the intermediary.⁶⁷³ The

669 *ibid* [67].

670 *ibid* [66]. Under Section 79(3)(a) of the IT Act, an intermediary is not entitled to immunity under Section 79(1) if “the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of an unlawful act”.

671 *ibid* [80].

672 *ibid* [82].

673 *ibid* [85].

High Court also ordered Darveys.com to seek Louboutin Sas's consent prior to offering products bearing Louboutin's mark on its platform.⁶⁷⁴

674 *ibid.*

Analysis

The decision in *Christian Louboutin* created a distinction between 'active' and 'passive' e-commerce platforms. Following the decision, the High Court of Karnataka also noted that certain additional facilities may disentitle intermediaries from safe harbour.⁶⁷⁵ However, this analysis overlooks the fact that an entity's 'status' as an 'intermediary' does not apply across all its operations, but is better evaluated in relation to the conduct for which secondarily liability is sought to be imposed.⁶⁷⁶ In this view, it would be mistaken to examine an entity's *overall* operations and decide whether it was an intermediary or not; it would be more appropriate to examine the functionality it provided *with respect* to the alleged trademark infringement. The judgement in *Christian Louboutin* has also been criticised for failing to provide a rationale for the activities that differentiate between active and passive e-commerce platforms and the implication that 'any service' in Section 2(1)(w) of the IT Act excludes physical services such as transport and delivery.⁶⁷⁷ Crucially, in *Christian Louboutin* no evidence was led on who the product sellers were, and whether the products themselves were genuine. Thus, it was unclear whether Darveys.com was an 'inventory e-commerce entity' selling its own counterfeit goods or a 'marketplace e-commerce entity' facilitating transactions between buyers and third-party sellers.

675 *Amazon Seller Services Pvt Ltd v Indusviva Health Sciences Pvt Ltd* MFA 8411 of 2018 (High Court of Karnataka, 28 August 2019).

676 For a detailed discussion on this reasoning, refer Section 3.1 of this report.

677 *Majithia* (n 641) 479–480.

A year after *Christian Louboutin*, a Division Bench of the High Court of Delhi in *Clues Network Pvt. Ltd. vs. L'Oreal* held that a definitive determination of whether an e-commerce platform is an "intermediary" and consequently entitled to seek safe harbour under Section 79 of the IT Act cannot be made without evidence being led on the intermediary's functionality.⁶⁷⁸ The Division Bench was hearing appeals against decisions that relied on the rationale laid down in *Christian Louboutin*, casting doubt on the correctness of the rationale applied.

678 *Clues Network Pvt Ltd v L'Oreal* 2019 SCC OnLine Del 7984 [33].

(ii) *Amazon Seller Services vs. Amway India Enterprises*

Amway Enterprises and other 'direct sellers' of healthcare products filed a suit for tortious interference against various e-commerce platforms including Amazon. Amway claimed that

that the Union Government’s Direct Selling Guidelines prevented direct sellers from selling their products on e-commerce platforms. Amway stated that it had not ‘authorised’ any of its distributors (the individuals Amway sold their products to) to sell Amway’s products online. It therefore claimed that Amazon was acquiring Amway’s products from ‘unauthorized’ re-sellers and illegally selling the products on its online platform, violating the Direct Selling Guidelines and causing Amway financial and reputational loss. Amazon responded by arguing that it provided an online platform facilitating transactions between customers and sellers, and Amway was free to pursue an action against the sellers selling Amway’s products on Amazon’s platform.

A Single Judge of the High Court of Delhi ruled that; (i) the Union Government’s Direct Selling Guidelines were legally binding; and (ii) to sell on Amazon’s platform, the seller had to be an ‘authorised seller’ and have the consent of the trademark owner (Amway). Following *Christian Louboutin Sas*, the Single Judge drew a distinction between ‘active’ and ‘passive’ e-commerce platforms and ordered Amazon and other e-commerce platforms to obtain Amway’s consent prior to listing Amway’s products on their platforms. On appeal, the decision was set aside by a Division Bench of the High Court of Delhi. The Division Bench held that the Direct Selling Guidelines were not legally binding,⁶⁷⁹ and nothing prevented the individuals whom Amway sold their products to from further selling the products online, including on Amazon’s platform.⁶⁸⁰ The principle of ‘exhaustion’ negated any rights Amway had to control the further sale of its products.⁶⁸¹

679 *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454 [101].

680 *ibid* [107].

681 *ibid* [20]-[21].

The Division Bench in *Amazon Seller Service* cast doubt on the correctness of the approach in *Christian Louboutin*.⁶⁸² The Division Bench noted that that the *raison d’etre* of Section 79 was “to ensure that the liability for non-compliance and/or violation of law by a third party, i.e. the seller, is not fastened on the online market place.”⁶⁸³ The Division Bench further noted that there was *prima facie* merit in Amazon’s contention that providing value-added service such as logistical support, packaging and delivery services would not automatically disqualify Amazon from safe harbour under Section 79 of the IT Act, especially as Section 2(1)(w) of the IT Act envisaged that “such intermediaries could provide value-added services to third party sellers”.⁶⁸⁴ However, it is important to note that it is the requirements of Section 79, and not Section 2(1)(w) alone that intermediaries must satisfy when seeking safe harbour.

682 *ibid* [141].

683 *ibid* [142].

684 *ibid* [144]-[145].

Finally, the Division Bench noted that Amway had failed to definitively establish any interference with its rights by Amazon for the ‘affirmative defence’ of safe harbour to be contemplated.⁶⁸⁵ Following the principle laid down in *Clues Network*, the Division bench ruled that a final determination of whether Amazon was an “intermediary” under Section 2(1)(w) of the IT Act entitled to safe harbour under Section 79 could only be done after evidence had been led on Amazon’s exact functionality.⁶⁸⁶

685 *ibid* [143].

686 *ibid* [145].

Analysis

The decision in *Amazon Seller Service* discarded the distinction between ‘active’ and ‘passive’ intermediaries based on factors external to the text of Section 2(1)(w) and held that providing value-added services does not dilute an intermediary’s claim to safe harbour. The E-Commerce Rules clearly state that marketplace e-commerce entities are eligible for safe harbour if they satisfy the conditions of Sections 79(2) and 79(3).⁶⁸⁷ However, the answer as to when marketplace e-commerce entities do satisfy these conditions continue to evolve with judicial decisions. Additionally, there remains some uncertainty over whether the standard of knowledge to be applied vis-à-vis e-commerce platforms is that of ‘an objective determination of knowledge’ or ‘court order’. Finally, the tests applied by courts to distinguish between marketplace and inventory e-commerce platforms will also impact which entities are eligible for safe harbour.

687 E-Commerce Rules r. 5(1).



7

Courts, Non-Monetary Liability, and Website Blocking

Obligations may be imposed on both ISPs and online intermediaries purely to ensure ‘efficiency or fairness’⁶⁸⁸ while courts determine the ultimate question of liability. Safe harbour does not prevent injunctions from being ordered against intermediaries;⁶⁸⁹ in fact, the decision in *Shreya Singhal* expressly contemplates such injunctions by stating that intermediaries will remove content pursuant to a court order. In India, intermediaries are regularly impleaded as defendants not only where they are allegedly secondarily liable, but also merely because they are well-situated to operationalise the cessation of unlawful content online.⁶⁹⁰ This may be for a variety of reasons, including the content originator being unknown.⁶⁹¹ Commentators have noted that the colloquial understanding of intermediaries ‘not being liable’ is thus best understood as not being *monetarily* liable.⁶⁹² In this regard, it is useful to differentiate between monetary and non-monetary liability,⁶⁹³ the latter constituting obligations that must be fulfilled even absent a finding of wrongdoing and the imposition of monetary liability. Non-monetary liability may be further sub-divided into prohibitory (or preventive) and mandatory obligations.⁶⁹⁴ Under Indian law, a preventive injunction restrains a party from carrying out an act while a mandatory injunction compels a party to do a specific thing.⁶⁹⁵ Further, injunctions may be temporary (until a court finally decides the dispute) or permanent.⁶⁹⁶

Previous sections of this report have examined the regulatory frameworks of the IT Act, Copyright Act, and Consumer Protection Act that govern intermediary liability. This section of the report focusses on how the enforcement objectives of courts have impacted the obligations of intermediaries in India. Specifically, it examines the standards applied by courts when granting injunctions against online content, additional enforcement obligations imposed on intermediaries, and finally, web-site blocking that takes place outside the regulatory framework of the IT Act, at the sole behest of India’s higher judiciary.

688 See Martin Husovec, ‘Remedies First, Liability Second: Or Why We Fail to Agree on Optimal Design of Intermediary Liability’ in Giancarlo Frosio (ed), Martin Husovec, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 93.

689 Riordan, ‘Safe Harbours’ (n 112) 386.

690 See *UTV Software Communications Ltd v 1337x CS* (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019) [5].

691 *Jagran Prakashan Limited v Telegram FZ LLC CS* (Comm) 146 of 2020 (High Court of Delhi); *Subodh Gupta v Herdsceneand CS* (OS) 483 of 2019 (High Court of Delhi); *Sunil Sachdeva v www.cjr7.com CS* (OS) 385 of 2019 (High Court of Delhi).

692 Riordan, ‘Safe Harbours’ (n 112) 398.

693 Giancarlo Frosio, ‘Mapping Online Intermediary Liability’ in Giancarlo Frosio (ed), Giancarlo Frosio, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 6–7.

694 Frosio (n 693).

695 *State of Haryana v State of Punjab 2004* (12) SCC 673 [37].

696 *ibid.*

7.1. Injunctions and non-monetary liability

The decision in *Shreya Singhal* stipulated that parties must acquire a court order directing takedown prior to an intermediary removing content from its platform. Private parties⁶⁹⁷ often approach courts seeking the takedown of content as part of civil actions such as defamation⁶⁹⁸ or intellectual property infringement.⁶⁹⁹ Where parties approach courts, judges must decide whether the online content should be taken down for the duration of the legal dispute, and potentially permanently. If courts grant injunctions, they may impose both preventive and mandatory obligations on ISPs and online intermediaries.

(i) Standards for granting injunctions

Indian courts grant injunctions based on three factors: (i) whether the plaintiff has established a *prima facie* case; (ii) whether the balance of convenience lies in favour of an injunction; and (iii) whether refusal to grant an injunction will cause the plaintiff irreparable harm.⁷⁰⁰ While the High Court of Delhi has rejected a distinct (and lower) threshold for injunctions against online content,⁷⁰¹ in practice there is little uniformity amongst courts as to whether the three factors set out above, or alternate/additional factors, should be considered when granting injunctions against online content. For example, in *Luv Ranjan vs. Midday Infomedia*, the High Court of Delhi referred to the traditional aforementioned three-part injunctive standard when injuncting online content during the pendency of a defamation suit.⁷⁰² However, in its ultimate analysis, the sole reason cited for granting the injunction is the “*potential damage to the plaintiff’s reputation*”.⁷⁰³

Similarly, where a plaintiff sought the removal of content on the Instagram page ‘*Herdsceneand*’ as part of a defamation suit, in an *ex-parte* proceeding the High Court of Delhi merely noted that the allegations of sexual harassment against the plaintiff on the page were *prima facie* defamatory, and directed the Instagram page, Instagram, Facebook, and Google to take down all content pertaining to the plaintiff and block a list of eighteen URLs.⁷⁰⁴ Critics of the High Court’s approach have pointed out that courts should refrain from asking intermediaries such as Google to take down articles without hearing the specific websites and originators concerned.⁷⁰⁵

697 The government does not approach courts seeking injunction against potentially unlawful content online, although the Government may decide to block such content under Sections 69A or 79(3)(b) of the IT Act. *See*, Sections 8 and 4.3(iii) of this report respectively for discussions on the procedures employed under those provisions.

698 *Subodh Gupta v Herdsceneand* CS (OS) 483 of 2019 (High Court of Delhi); *Sunil Sachdeva v www.cjr7.com* CS (OS) 385 of 2019 (High Court of Delhi); *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi); *Swami Ramdev v Facebook Inc* 2019 SCC OnLine Del 10701; *Zulfiqar Ahmad Khan v Quintillion Business Media* CS (OS) 642 of 2018 (High Court of Delhi).

699 *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* 2020 SCC OnLine Del 454; *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382.

700 *Maria Margarida Sequeira Fernandes v Erasmo Jack De Sequeira* 2012 (5) SCC 370 [86].

701 *Tata Sons Ltd v Greenpeace International* 2011 SCC OnLine Del 466.

702 *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi, 21 October 2019). *See also Jagran Prakashan Limited v Telegram FZ LLC* CS (Comm) 146 of 2020 (High Court of Delhi, 29 May 2020) (granting an injunction against alleged copyright and trademark infringement).

703 *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi, 21 October 2019).

704 *Subodh Gupta v Herdsceneand* CS (OS) 483 of 2019 (High Court of Delhi, 18 September 2019).

705 Vrinda Bhandari and Anja Kovacs, ‘What’s Sex Got to Do with It? Mapping the Impact of Questions of Gender and Sexuality on the Evolution of the Digital Rights Landscape in India’ [2021] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3769942>> accessed 1 May 2021; Ganesan, ‘Bengaluru Court Orders Twitter to Block Congress Handles over Copyright’ (n 614).

Courts also have other reasons to be cautious when issuing injunctions against online content. Experts note that it is hard to predict the impact of an injunction given that: (i) evidence is typically sparse at preliminary hearings; (ii) respondents may fail to appear or be unrepresented during such hearings; (iii) the actual effect of an injunction order may not be known until it is implemented; and (iv) the actions taken by website operators and ISPs may restrict lawful material.⁷⁰⁶ The removal of content from the internet also impacts the rights of all internet users to receive information. Therefore, it is incumbent on courts to lay down clear judicial standards for injunctions against online content that encapsulate all these considerations.

Standard for blocking a website

Where the plaintiff seeks an order blocking an entire website, courts have considered a broader range of factors. Where a copyright holder initially secured an injunction blocking specific URLs and then later sought to obtain an injunction against the entire website, the High Court of Delhi in *Dept. of Electronics & IT vs. Star India* noted that such a sweeping order may be disproportionate as it would restrict other legitimate business being conducted by the website.⁷⁰⁷ The High Court noted that a judicial order blocking infringing content on the internet, must consider: (i) the comparative importance of the rights at issue; (ii) the availability of less restrictive or ‘onerous’ measures; (iii) the costs associated with implementing the measures; and (iv) the efficacy of the measures as implemented by the ISPs.⁷⁰⁸ Ultimately, the High Court directed the blocking of the websites, as the copyright holder was able to demonstrate that the website was used exclusively to host infringing material and facilitate further infringement.⁷⁰⁹ Even though the online intermediary (website) chose not to participate in the proceedings, the High Court held that it could at a future point challenge the order by demonstrating that its “*dominant activity is lawful*”.⁷¹⁰

In a similar case dealing with ‘rogue websites’, where the websites were hosting copyright infringing material and did not appear before the High Court of Delhi, the Court held that the test for whether to block an infringing website was qualitative and not quantitative,⁷¹¹ and outlined several factors that may inform a judge’s decision including: (i) whether the primary function of the website is to commit or facilitate infringement; (ii) whether the registration details of the website may be traced; (iii) whether

706 Jaani Riordan, ‘Blocking Injunctions’ in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 492.

707 *Department of Electronics and Information Technology v Star India Pvt Ltd* FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016). See also *Balaji Motion Picture Ltd v Bharat Sanchar Nigam Ltd* 2016 SCC OnLine Bom 6607.

708 *Department of Electronics and Information Technology v Star India Pvt Ltd* FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016) [7], [12].

709 *ibid* [12].

710 *ibid* [18].

711 *UTV Software Communications Ltd v 1337x* CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019) [69].

there has been inaction on behalf of the website; (iv) whether the owner or operator of the website displays a general disregard for copyright; (v) whether the websites have been blocked by courts in other jurisdictions; (vi) whether the website contains instructions on how to circumvent blocking measures; and (vii) the volume of traffic on the website.⁷¹² Although the High Court held that website blocking may be a proportionate response to copyright infringement,⁷¹³ the Court also held that ISPs could not be required to determine whether the list of URLs provided by the plaintiffs contained infringing material.⁷¹⁴ The High Court eventually delegated this task to the Registrar of the Court.⁷¹⁵

712 *ibid* [59].

713 *ibid* [86].

714 *ibid* [100].

715 *ibid* [101].

(ii) Content of injunction orders with respect to intermediaries

As with the standard for injunctions, there is little uniformity in the obligations imposed on intermediaries through injunction orders. Injunction orders may initially be granted ‘until the next court hearing’, but often persist during the duration of the legal dispute, which can last considerably longer.⁷¹⁶ Like all forms of content takedown, injunction orders restrict the free speech rights of content originators and information access rights of internet users, and their duration should be limited to the time necessary to determine any potential harms stemming from the content. However, given the lengthy nature of legal disputes in India,⁷¹⁷ content that is preliminarily enjoined by courts may stay down for extended periods of time.

716 *See Subodh Gupta v Herdsceneand CS* (OS) 483 of 2019 (High Court of Delhi); *Sunil Sachdeva v www.cjr7.com* CS (OS) 385 of 2019 (High Court of Delhi); *Luv Ranjan v Middy Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi); *Swami Ramdev v Facebook Inc* 2019 SCC OnLine Del 10701; *Zulfiqar Ahmad Khan v Quintillion Business Media* CS (OS) 642 of 2018 (High Court of Delhi).

717 *See* ‘India Justice Report’ (2019) <<https://www.tatatrusts.org/upload/pdf/overall-report-single.pdf>> accessed 13 May 2021.

Injunction orders should also be limited to the specific URLs or content that are determined to be *prima facie* unlawful. An example of this principle *not* being followed is where three tweets from two accounts associated with the Congress party were accused of using copyright infringing material. Rather than direct the removal of the tweets, a Bangalore civil court directed the ‘temporary blocking’ of both accounts in their entirety.⁷¹⁸ The content of the injunction may also impose broad obligations on intermediaries. For example, when a plaintiff alleged that YouTube was hosting videos that instructed users how to gain unauthorised access to the plaintiff’s (television broadcasting) services, YouTube was directed to remove all content which ‘sought to demonstrate any trick or hack to access the plaintiff’s devices or services’.⁷¹⁹ Similarly, in passing an injunction against an allegedly defamatory online article, the High Court of Delhi restrained the defendant intermediaries from

718 Ganesan, ‘Bengaluru Court Orders Twitter to Block Congress Handles over Copyright’ (n 614). This order was eventually set aside by the High Court of Karnataka.

719 *Tata Sky Ltd v YouTube LLC* 2016 OnLine Del 4476 [5].

republishing the complaints alleged in the article or any articles ‘based on’ the original allegedly defamatory article.⁷²⁰ Twitter (one of the defendants) challenged this injunction, arguing that such a broad and general obligation to prevent unlawful content was incompatible with an intermediary’s functionality under the IT Act.⁷²¹ Accepting Twitter’s argument, the High Court modified its earlier injunction order, directing Twitter to only take down specific URLs provided by the plaintiff.⁷²²

However, allowing plaintiffs to provide URLs effectively sets up court-sanctioned notice and takedown regime between the plaintiff and intermediaries. There is no independent verification of the URLs provided by the plaintiff, undermining the key principle of judicial oversight of takedowns set out in *Shreya Singhal*. For example, Bhandari and Kovacs note that in *Subodh Gupta vs. Herdsceneand*, several of the URLs provided by the plaintiff included ‘unrelated or fairly reported’ articles, leading to overbroad censorship at the behest of the plaintiff.⁷²³ Similarly, in a public interest litigation on whether pornographic content online should be restricted, the petitioner provided the Union Government with a list of 857 websites allegedly hosting pornographic content.⁷²⁴ The Union Government subsequently directed ISPs to block these websites.⁷²⁵

The High Court of Delhi expressly highlighted this issue, stating that injunctions could only be issued with respect to “*content which has been considered or found to be unlawful and there is no question of any prior restraint or blanket ban orders being issued*” which may suppress free expression.⁷²⁶ However, the standard for determining when content is *prima facie* unlawful confers significant discretion on judges, and no regulatory mechanism has yet been evolved to govern future uploads at different locations online after the injunction order has been passed.

Efficacy of takedown required of intermediaries

There also remains uncertainty over the efficacy that intermediaries must achieve to satisfactorily comply with court orders directing the takedown of content. In a 2019 defamation suit against Facebook, Google, YouTube, Google Plus, and Twitter, a Single Judge of the High Court of Delhi held that ‘disabling access’ under Section 79(3)(b) of the IT Act would necessitate a *global* blocking order, as opposed to a geographically limited order, where the content was originally uploaded from India.⁷²⁷

720 *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi, 21 October 2019).

721 *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi, 21 January 2020).

722 *ibid.*

723 Bhandari and Kovacs (n 705). See also *Subodh Gupta v Herdsceneand* CS (OS) 483 of 2019 (High Court of Delhi, 30 September 2019)

724 *ibid.*

725 Department of Telecommunications, No. 813-7/25/2011-DS (Vol.V), Communication dated 31 July 2015 <https://cis-india.org/internet-governance/resources/dot-morality-block-order-2015-07-31/at_download/file> accessed on 15 October 2021.

726 *X v Union of India* WP (Cri) 1082 of 2020 (High Court of Delhi, 20 April 2021) [63].

727 *Swami Ramdev v Facebook Inc* 2019 SCC OnLine Del 10701 [91]-[95].

Observing that “*any order passed by the Court has to be effective*”,⁷²⁸ the High Court ruled that if the content remained on global platforms that Indian internet users could access, then access had not been ‘disabled’ *vis-à-vis* Indian users. This approach is contradictory to the ‘Country-Withheld-Content’ strategy adopted by several platforms, under which authorities can notify and demand that intermediaries take down content within a specific jurisdiction.⁷²⁹ The High Court decision has been appealed by the defendant intermediaries.⁷³⁰ Although the broader issue remains unresolved, in this case the plaintiffs have stated that no contempt proceedings will be initiated during the pendency of the appeal.⁷³¹

It is important to distinguish between ‘blocking’ (as carried out by ISPs) and ‘content removal’ (affected by the intermediary hosting the content). Blocking merely causes the ISP to deny their subscribers access to a particular location (URL) on the internet, while content removal ensures the content is taken down at its source. Thus, blocking can be circumvented by using a different ISP or a virtual network provider with servers located in a jurisdiction where the content is not blocked, while content removal is a universal remedy that destroys the original unlawful content.⁷³² Blocking avoids the extra-territorial impact of an overbroad injunction, as its impact is limited to the ISPs under the court’s jurisdiction.⁷³³ ISP blocking may also be a particularly useful remedy where the host of the content is unresponsive to removal requests.⁷³⁴

The desired effect of blocking is better viewed as making it substantially more onerous on ordinary users to access the *prima facie* unlawful material, thus dissuading ordinary users from seeking access to the disputed content.⁷³⁵ Blocking measures increase the cost of accessing the potentially unlawful material by adding to ‘search costs’ (having to find an alternative webpage), ‘configuration costs’ (having to download or configure specific software such as proxies), and ‘service costs’ (potentially having to pay a virtual network provider).⁷³⁶ The effectiveness of a blocking order will ultimately depend on the extent to which individuals are sensitive to these various costs, though traffic to blocked URLs can be expected to decline. However, unlike content removal, website operators themselves may circumvent ISP blocking by: (i) altering the URL where unlawful content is hosted; (ii) providing users with circumvention tools and techniques; and (iii) changing to new protocols or adopting new technology that may nullify the effect of blocking.⁷³⁷

728 *ibid* [106].

729 MacKenzie Common and Rasmus Kleis Nielsen, ‘How to Respond to Disinformation While Protecting Free Speech’ (*Reuters Institute for the Study of Journalism*) <<https://reutersinstitute.politics.ox.ac.uk/risj-review/how-respond-disinformation-while-protecting-free-speech>> accessed 14 July 2021.

730 *Facebook Inc v Swami Ramdev* FAO (OS) 212 of 2019 (High Court of Delhi).

731 *ibid* (31 October 2019).

732 Riordan, ‘Blocking Injunctions’ (n 706) 462.

733 *ibid* 462–463.

734 *ibid* 491.

735 *ibid* 462.

736 *ibid* 495.

737 *ibid*.

While courts typically require that parties implement their directions in both letter and spirit, it may be impossible for intermediaries to totally restrict access to content as nearly all restrictions ‘can be circumvented with some specialist knowledge’.⁷³⁸ Injunction orders should ideally not impose a requirement on intermediaries to achieve a total cessation of unlawful content on their platforms, but rather limit themselves to the extent to which intermediaries can reasonably assist in enforcement objectives.⁷³⁹ Further, an overreliance on intermediaries for enforcement dissuades plaintiffs from pursuing remedies against content originators where they may be identifiable. This is also in line with the requirement that the interference with the intermediaries’ own rights be the least restrictive measure that would continue to meaningfully protect the injured plaintiff’s rights.⁷⁴⁰ Thus, ‘disabling access’ under the IT Act should be understood as a measure that reasonably dissuades users from accessing the content without imposing disproportionate burdens on intermediaries or other internet users.

A new ‘template’

To harmonise injunctions against online content, a Single Judge of the High Court of Delhi recently set out a series of directions that may be used as a “*template*” to ensure that the takedown of content is ‘effective’ while balancing the rights of the plaintiff/complainant, intermediaries, and internet users.⁷⁴¹ The directions set out by the High Court include:

- Once a court is satisfied that the content should be taken down, it can issue an order to the online intermediary, which must take down the content within twenty-four hours;
- The online intermediary must also take down ‘similar kinds of content’;
- The court may mandate that the concerned intermediaries and search engines “*endeavour to employ proactive monitoring by using automated tools, to identify and remove or disable access to any content which is ‘exactly identical’ to the offending content*”;
- The court may issue a direction to commonly used search engines such as Google, Yahoo, Bing, and DuckDuckGo to de-index and de-reference all concerned webpages and

738 Christophe Geiger and Elena Izyumenko, ‘Blocking Orders: Assessing Tensions with Human Rights’ in Giancarlo Frosio (ed), Christophe Geiger and Elena Izyumenko, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 582.

739 See Husovec (n 688); Geiger and Izyumenko (n 738).

740 Geiger, Frosio and Izyumenko (n 199) 148–49; Geiger and Izyumenko (n 738) 581.

741 *X v Union of India* WP (Cri) 1082 of 2020 (High Court of Delhi, 20 April 2021) [90]

subpages where the offensive content is found within twenty-four hours;

- The injured party can use the injunction order to approach law enforcement agencies to remove offending content from other websites on which “*same or similar offending content is found*”, and law enforcement agencies must issue appropriate orders to block the content; and
- If an online intermediary objects to such an order by a law enforcement agency, it may approach the court that passed the injunction order, but only after first taking down the content.⁷⁴²

742 *ibid.*

The High Court also noted that the intermediary, when taking down content, must also follow the procedure set out in Rule 4(8) of the Intermediary Guidelines 2021 (give the uploader a chance to contest the takedown and seek re-instatement).⁷⁴³ At the time of this report, an appeal has been filed against the decision.⁷⁴⁴

743 *ibid.*

744 *Google LLC v X LPA 174 of 2021* (High Court of Delhi).

The High Court’s approach fails to consider several facets of the Intermediary Guidelines 2021. For example, the twenty-four hour timeline adopted by the Judge is found in Rule 3(2)(b) of the Intermediary Guidelines 2021, which applies to complaints by users directly to the Grievance Officer of an intermediary. In contrast, Rule 3(1)(d) of the Intermediary Guidelines expressly grants intermediaries thirty-six hours to take down content pursuant to a court order.⁷⁴⁵ Further, the obligation for intermediaries to employ automated tools to proactively monitor content is only applicable to SSM Intermediaries under Rule 4 of the Intermediary Guidelines,⁷⁴⁶ and not all intermediaries as the High Court’s template suggests. Lastly, the obligation to notify users under Rule 4(8) only applies to cases of voluntary moderation and not takedowns pursuant to court orders,⁷⁴⁷ where it is presumed that all relevant parties will be heard by the court prior to any decision on removing content.

745 Intermediary Guidelines 2021 r. 3(1)(d) (second proviso).

746 Intermediary Guidelines 2021 r. 4(4).

747 Intermediary Guidelines 2021 r. 4(8) (where an SSM Intermediary removes content “on its own accord”).

Importance of speech safeguards when issuing injunctions

The High Court of Delhi itself in *Myspace* has cautioned against overbroad injunction orders, noting that “*a vague order of injunction against works which are yet to exist is not only contrary to law but also impossible to monitor.*”⁷⁴⁸ The High Court noted that in

748 *Myspace Inc v Super Cassettes Industries Ltd 2016 SCC OnLine Del 6382* [75].

order to avoid contempt of court, the intermediary was likely to remove all content that might remotely be covered by a broadly-worded injunction order, which would result in “*unwarranted private censorship*” which “*would go beyond the ethos of established free speech regimes.*”⁷⁴⁹ In another case, the High Court also cited the requirement of proportionality as negating the use of orders that would require intermediaries to pre-filter or proactively monitor content.⁷⁵⁰

Other valuable safeguards that can be adopted by courts when issuing injunctions are: (i) requiring ISPs to notify their subscribers the reason a particular URL has been blocked, ideally providing their subscribers with the relevant case details to allow third parties to challenge a blocking injunction; (ii) permitting third parties whose right to receive information is restricted by the removal or blocking of online content to appear before the court challenge the injunction;⁷⁵¹ and (iii) in the case of preliminary injunctions, continually review the injunction given the lengthy nature of Indian litigation. The proportionality of an injunction should also be judged by its effectiveness in remedying the underlying harm caused by the content.⁷⁵² Thus, steps could be taken to explain to URL visitors why the content was blocked and the harm caused by the underlying illegality. In cases of copyright infringing content, users may be redirected to non-infringing sources for the same content.⁷⁵³

(iii) ‘John Doe’ and *quia timet* orders

Courts in India have issued *quia timet* injunctions coupled with ‘John Doe’ or ‘Ashok Kumar’ orders. A *quia timet* injunction is a prospective remedy sought by a plaintiff to restrain a defendant from committing a wrongful act. *Quia timet* injunctions are sought *prior* to the wrongful act when the act is imminent but has not yet occurred.⁷⁵⁴ John Doe orders are directions granted in *ex-parte* proceedings where there is a substantial risk that the imminent actions of an *unknown* (John Doe) defendant will cause significant harm to the plaintiff.⁷⁵⁵ Ordinarily, once defendants are identified, they are impleaded and have an opportunity to challenge the order.

In India, *quia timet* and John Doe injunctions have been used by copyright owners to direct ISPs to block websites pre-emptively to prevent the dissemination of infringing material.⁷⁵⁶ In 2011, when the producers of the movie ‘*Singham*’ approached the High Court of Delhi on the apprehension that certain unnamed

749 *ibid* [71].

750 *UTV Software Communications Ltd v 1337x* CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019) [79].

751 Riordan, ‘Blocking Injunctions’ (n 706) 493.

752 *ibid* 495.

753 *ibid*.

754 *Snapdeal Pvt Ltd v GoDaddy LLC* CS (Comm) 176 of 2021 (High Court of Delhi, 18 April 2022) [93].

755 *See Vodafone India Ltd v RK Productions Pvt Ltd* 2012 SCC OnLine Mad 4164 [33].

756 *See Star India Pvt Ltd v 7Movierulz*. *tc* CS (Comm) 604 of 2022 (High Court of Delhi, 2 September 2022); *RK Productions Pvt Ltd v Bharat Sanchar Nigam Limited* 2012 SCC OnLine Mad 4184; *Reliance Big Entertainment Pvt Ltd v Jyoti Cable Network* CS (OS) 1724 of 2011 (High Court of Delhi 20 July 2011).

defendants would engage in the infringement (piracy) of their movie; the High Court passed an order against the unnamed defendants, restraining them from making available, distributing, or displaying the movie through all mediums including the internet.⁷⁵⁷ The same practice has been adopted more recently, with the High Court of Delhi granting injunctive relief to movie producers prior to a theatrical release and directing ISPs to blocking eighteen websites, even directing the concerned domain name registrants to disclose the names, email addresses, and IP addresses associated with the websites.⁷⁵⁸ Such orders have been criticised as being open-ended, not prescribing a time limit for their application, and failing to distinguish between websites solely designed to facilitate infringement and websites incidentally hosting the infringing content without being aware of it.⁷⁵⁹ When the open-ended nature of such an injunction was challenged by ISPs as technically difficult to implement and imposing a general monitoring obligation, the High Court of Madras directed the plaintiffs to provide ISPs with specific URLs to block.⁷⁶⁰

In *Snapdeal Pvt Ltd vs. GoDaddy LLC*, the High Court of Delhi refused to grant a *quia timet* action which sought to injunct the future registration of all domain names containing the plaintiff's trademark (Snapdeal).⁷⁶¹ The High Court ruled that an injunction could not be granted against “*hypothetical or imaginary infringements*” of a trademark, ruling that the plaintiff must draw the court's attention to the specific and identifiable mark that was allegedly infringing when seeking an injunction.⁷⁶² Despite this decision and the instructive rulings in *Dept. of Electronics & IT vs. Star India* and *Myspace*, Indian courts regularly grant content-restricting injunctions based solely on plaintiffs proving that the content is *prima facie* unlawful.⁷⁶³ Given the low evidentiary threshold to be met, such injunctions, when extended to the internet,⁷⁶⁴ can impose substantial obligations on intermediaries and internet users unless a detailed proportionality analysis is carried out.

Further, key issues remain unresolved, including: (i) the exact level of efficacy the intermediary should achieve in implementing broadly-worded orders; (ii) whether intermediaries are always obligated to internalise the costs of implementation; (iii) the extent to which plaintiffs must attempt to pursue remedies against originators; and (iv) what measures should be taken to allow internet users to exercise their right to access information *vis-à-vis* blocked content. Imposing a clear time limit on the

757 *Reliance Big Entertainment Pvt Ltd v Jyoti Cable Network* CS (OS) 1724 of 2011 (High Court of Delhi 20 July 2011).

758 *Star India Pvt Ltd v 7Moverulz.tc* CS (Comm) 604 of 2022 (High Court of Delhi, 2 September 2022)

759 Juhi Gupta, 'John Doe Copyright Injunctions in India' (2013) 18 *Journal of Intellectual Property Rights* 351, 353–54.

760 *RK Productions Pvt Ltd v Bharat Sanchar Nigam Limited* 2012 SCC OnLine Mad 4184 [36].

761 *Snapdeal Pvt Ltd v GoDaddy LLC* CS (Comm) 176 of 2021 (High Court of Delhi, 18 April 2022) [95].

762 *ibid.*

763 *Luv Ranjan v Midday Infomedia Ltd* CS (OS) 535 of 2019 (High Court of Delhi, 21 October 2019); *Subodh Gupta v Herdsceneand* CS (OS) 483 of 2019 (High Court of Delhi, 18 September 2019); *Sunil Sachdeva v www.cjr7.com* CS (OS) 385 of 2019 (High Court of Delhi, 2 August 2019); *Zulfiqar Ahmad Khan v Quintillion Business Media* CS (OS) 642 of 2018 (High Court of Delhi, 13 December 2018). *See also Selvi Jayalalitha v Penguin Books India* OA 417 of 2011 (High Court of Madras, 27 August 2012); *Shilpa Shetty v Magma Publications* AIR 2001 Bom 176.

764 *Swami Ramdev v Facebook Inc* 2019 SCC OnLine Del 10701 [91]-[95].

prohibition, communicating to internet users why the content has been taken down, and allowing affected third parties to intervene and challenge the injunctive order all safeguard against the abuse of injunctions.⁷⁶⁵

765 Arnold (n 193) 417–18.

7.2. Blocking at the behest of courts

In addition to litigation initiated by private parties, courts have repeatedly entertained public interest litigation seeking to curb allegedly harmful content online.⁷⁶⁶ These cases are different from traditional claims for injunctive relief as the plaintiffs in public interest litigation are not parties directly injured by the content, but rather ‘public-spirited citizens’ who both seek and propose general reliefs from courts. For example, in a public interest litigation filed to curb the online advertisement of pre-natal sex determination procedures (which are illegal in India), the Supreme Court directed Google, Microsoft, and Yahoo to “*auto-block*” a list of trigger words that would likely reveal the unlawful advertisements.⁷⁶⁷ In response to Google’s contentions that the restrictions must be limited to ‘advertisements’ for the procedures and should not limit user’s access to information, the Supreme Court directed the Union Government to set up a ‘Nodal Agency’ that would allow users to report advertisements for the prohibited procedures and directed the three online search engines to de-list the reported pages within thirty six hours.⁷⁶⁸

The High Court of Jammu and Kashmir also passed a broad order in proceedings initiated at the Court’s behest. The High Court directed intermediaries such as YouTube, Facebook, and Twitter to “*removal all the materials / posts / publications which tend to disclose the identity*” of an infant victim of sexual violence.⁷⁶⁹ The High Court went on to impose an ongoing removal obligation on these platforms.⁷⁷⁰ This order was challenged by Facebook, which argued that it was impossible to monitor all material which is posted on its platform, and requested the Court to narrow the scope of the order.⁷⁷¹ The High Court declined to modify the temporal scope of its order, but removed the words “*tend to disclose*”, limiting the obligation to posts that do disclose the identity of the victim.⁷⁷²

Courts have also entertained public interest litigation asking ISPs and online intermediaries to block pornography,⁷⁷³ child sex abuse material,⁷⁷⁴ the sharing of videos depicting rape,⁷⁷⁵ and a mobile game allegedly promoting suicide.⁷⁷⁶ In some of these cases, the Supreme Court of India has asked intermediaries to engage in consultations with the Union Government to suggest measures that could restrict the specific class of content on the internet.⁷⁷⁷ Courts have also passed broad orders directing large amounts of content to be restricted on the internet.⁷⁷⁸ For

766 *In Re “In the matter of, Incidence of Gang Rape in a Boarding School situated in Bhauwala” v State of Uttarakhand* (2018) SCC OnLine Utt 871; *Sabu Mathew George v Union of India* 2017 (2) SCC 514; *Registrar (Judicial) v Union Ministry of Communications* 2017 SCC OnLine 25298 Mad; *In re: Prajwala Letter dated 18.2.2015* SMW (Cri) 3 of 2015 (Supreme Court of India).

767 *Sabu Mathew George v Union of India* 2017 (2) SCC 514.

768 *ibid* [21]. In an order passed on 13 December, 2017 the Supreme Court noted that the advertisements were not being taken down despite the existence of the Nodal Agency and directed the Central Government, the Nodal Agency, Google, and Microsoft to consult with each other and provide suggestions on how to curb the illegal advertisements.

769 *Court on its own motion* PIL 12 of 2019 (High Court of Jammu and Kashmir, 28 October 2020).

770 *Court on its own motion* PIL 12 of 2019 (High Court of Jammu and Kashmir, 28 October 2020) [7].

771 *Court on its own motion* PIL 12 of 2019 (High Court of Jammu and Kashmir, 1 December 2020) [2]-[3].

772 *Court on its own motion* PIL 12 of 2019 (High Court of Jammu and Kashmir, 1 December 2020) [9].

773 *In Re “In the matter of, Incidence of Gang Rape in a Boarding School situated in Bhauwala” v State of Uttarakhand* (2018) SCC OnLine Utt 871.

774 *See Kamlesh Vaswani v Union of India* WP (C) 177 of 2013 (Supreme Court of India).

775 *In re: Prajwala Letter dated 18.2.2015* SMW (Cri) 3 of 2015 (Supreme Court of India).

776 *Registrar (Judicial) v Union Ministry of Communications* 2017 SCC OnLine 25298 Mad.

777 *Sabu Mathew George v Union of India* 2017 (2) SCC 514; *In re: Prajwala Letter dated 18.2.2015* SMW (Cri) 3 of 2015 (Supreme Court of India, 22 March 2017).

778 *Registrar (Judicial) v Union Ministry of Communications* 2017 SCC OnLine 25298 Mad.

example, when passing directions to restrict the mobile game “Blue Whale”, which the High Court of Madras believed was linked to a suicide, the High Court directed ISPs to “*take due diligence to remove all the links and hash-tags presently being circulated in the social media platforms such as Facebook, Twitter etc. and also in dark net with URLs/links related to Blue Whale Game.*”⁷⁷⁹ This broad language effectively imposes a general monitoring obligation on ISPs which is incompatible with their function under the IT Act.

⁷⁷⁹ *ibid* [31].



8

Blocking Content Under IT Act

While Section 79(3)(b) of the IT Act leaves open the possibility of the government sending intermediaries takedown notices,⁷⁸⁰ Section 69A specifically empowers the Union Government to block public access to content on the internet. The procedure for blocking content is set out in the Information Technology (Procedure and Safeguards for Blocking of Information by Public) Rules, 2009⁷⁸¹ ('IT Blocking Rules') and aims to offer a measure of due process to content originators and intermediaries. However, neither judicial authorisation nor independent oversight is provided for, and the process allows the executive to bypass key due process requirements in the case of emergencies.

780 See Section 4.3(iii) of this report.

781 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 G.S.R. 781(E) dated 27 October 2009 [IT Blocking Rules].

8.1. Procedure for blocking content

Under Section 69A, the Union Government may direct an intermediary to block public access to content if the Government is satisfied that it is necessary to do so in the interests of public order, the sovereignty, integrity, or defence of India or its friendly relations with other States, or the prevention of an offence under these categories.⁷⁸² The reasons for blocking content must be recorded in writing⁷⁸³ and an intermediary that fails to comply with a direction for blocking may be fined and imprisoned for up to seven years.⁷⁸⁴ Blocking directions have been issued by the Union Government to both ISPs⁷⁸⁵ and online intermediaries.⁷⁸⁶

(i) The IT Blocking Rules

Under the IT Blocking Rules, the ‘Nodal Officer’ of any ministry or department of the Union Government may submit a request for blocking content to the ‘Designated Officer’ in charge of processing blocking requests.⁷⁸⁷ The requests of the Nodal Officer may stem from their respective department or ministry, or from a complaint by a member of the public.⁷⁸⁸ In the latter case, the Nodal Officer shall first seek the approval of the Chief Secretary of the concerned State or Union Territory,⁷⁸⁹ and the relevant ministry and department shall satisfy itself that the complaint is related to content that should be acted upon under Section 69A.⁷⁹⁰ Blocking requests may also be sent to the Designated Officer by a competent court.⁷⁹¹

Once the Designated Officer receives a request for blocking and a sample of the offending content, a committee chaired by the Designated Officer and consisting of senior civil servants from the Ministries of Law and Justice, Home Affairs, MIB, and the Indian Computer Emergency Response Team shall examine the request⁷⁹² within seven days.⁷⁹³ The Designated Officer shall “*make all reasonable efforts*” to identify the intermediary hosting the offending content or the content originator, and issue a notice to them asking them to indicate why the disputed content should not be taken down.⁷⁹⁴

The IT Blocking Rules state that the “*person or intermediary who has hosted the information*” will be notified,⁷⁹⁵ but the Supreme Court in *Shreya Singhal* noted that “*it is not merely the intermediary who may be heard. If the “person” i.e. the originator is identified he is also to be heard before a blocking order is passed.*”⁷⁹⁶ The Supreme Court has therefore

782 The Information Technology Act, 2000 s. 69A(1).

783 *ibid* s. 69A(1).

784 *ibid* s. 69A(3).

785 Jay Mazoomdar and Ritu Sarin, ‘India Tops List of Websites Blocked, Its Telcos Filter the Most’ *The Indian Express* (25 April 2018) <<https://indianexpress.com/article/india/india-tops-list-of-websites-blocked-its-telcos-filter-the-most-netsweeper-5150620/>> accessed 2 March 2021.

786 Tushar Dhara, ‘Facebook Blocks Atheist Republic Page on Government Directive, Twitter Suspends Founder’ *The Caravan* (8 February 2021) <<https://caravanmagazine.in/media/facebook-blocks-atheist-republic-page-twitter-suspends-founder-on-government-directive>> accessed 2 March 2021.

787 IT Blocking Rules r. 5.

788 IT Blocking Rules r. 6(1).

789 IT Blocking Rules r. 6(1).

790 IT Blocking Rules r. 6(2).

791 IT Blocking Rules r. 5.

792 IT Blocking Rules r. 7.

793 IT Blocking Rules r. 11.

794 IT Blocking Rules r. 8(1).

795 IT Blocking Rules r. 8(1).

796 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [115].

clearly recognised the need to notify and hear the originator but has also acknowledges that there may be situations where the originator may not be identifiable despite ‘reasonable efforts’ being made by the Union Government. This issue is discussed in detail in the section below on the legal and practical challenges to blocking.

The intermediary or the content originator must appear or reply within forty-eight hours of receiving the notice,⁷⁹⁷ and if they fail to do so, the Committee shall make a recommendation based on the information it possess at the end of the forty-eight hour period.⁷⁹⁸ The period of forty-eight hours may be extended in cases where the intermediary or content originator is a foreign entity.⁷⁹⁹ The Committee shall submit its recommendation to the Secretary, Department of Information Technology,⁸⁰⁰ and upon the Secretary’s approval, the Designated Officer shall direct the intermediary to block the content.⁸⁰¹

In the case of an emergency, where the Designated Officer believes “no delay is acceptable” and it is “necessary or expedient or justifiable to block such information”, the Designated Officer may directly make a recommendation to the Secretary of Department of Information Technology⁸⁰² who may issue directions to an intermediary to block content without hearing the originator or the intermediary.⁸⁰³ In such cases, the Designated Officer shall place the offending content before the Committee within forty-eight hours of the emergency blocking direction being passed,⁸⁰⁴ and a final order shall be issued.⁸⁰⁵ The IT Blocking Rules do not provide for an *ex-post* hearing for the intermediary or originator where the emergency procedure is utilised by the Designated Officer.

Intermediaries are obligated to designate at least one person to receive and handle blocking directions issued under the IT Blocking Rules.⁸⁰⁶ The person designated by the intermediary shall acknowledge the receipt of the blocking directions within two hours.⁸⁰⁷ A ‘Review Committee’ shall meet at least once in two months and examine whether the directions issued under the IT Blocking Rules comply with the requirements for blocking content under Section 69A.⁸⁰⁸ The Review Committee may set aside blocking directions;⁸⁰⁹ however, the Rules do not allow content originators or intermediaries to appear before or challenge the findings of the Review Committee. A right to information request revealed that the Review Committee has never revoked a blocking order when scrutinising actions taken under Section 69A.⁸¹⁰ The

797 IT Blocking Rules r. 8(1).

798 IT Blocking Rules r. 8(2).

799 IT Blocking Rules r. 8(3).

800 IT Blocking Rules r. 8(5).

801 IT Blocking Rules r. 8(6).

802 IT Blocking Rules r. 9(1).

803 IT Blocking Rules r. 9(2).

804 IT Blocking Rules r. 9(3).

805 IT Blocking Rules r. 9(4).

806 IT Blocking Rules r. 13(1).

807 IT Blocking Rules r. 13(2).

808 IT Blocking Rules r. 14.

809 IT Blocking Rules r. 14.

810 Aarathi Ganesan, ‘Does This RTI Point to MeitY’s “rubber Stamp” Review Committee?’ (*MediaNama*, 11 August 2022) <<https://www.medianama.com/2022/08/223-meity-review-committee-not-one-69a-blocking-order-revoked/>> accessed 4 November 2022.

complaints and requests for blocking are ‘confidential’ under the IT Blocking Rules.⁸¹¹ However, as discussed below, when the non-disclosure of blocking orders was challenged as violating constitutional guarantees to free speech and information, the High Court of Delhi directed that the blocking order be provided to the originator.⁸¹²

811 IT Blocking Rules r. 16.

812 *Tanul Thakur v Union of India* WP (C) 13037 of 2019 (High Court of Delhi, 11 May 2022). See Section 8.3 of this Report.

(ii) Blocking of news and curated content under the Intermediary Guidelines 2021

A similar but parallel⁸¹³ procedure also exists under the Intermediary Guidelines 2021 for blocking the content of publishers of “*news and current affairs content*” and “*online curated content*”⁸¹⁴ under the control of MIB.⁸¹⁵ However, as noted at the end of this section, this power been partially stayed by High Courts in Bombay and Madras and is currently subject to consideration by the Supreme Court.

813 Intermediary Guidelines 2021 r. 8(3).

814 Intermediary Guidelines 2021 r.8(1), r.15.

815 Intermediary Guidelines 2021 r. 8(1).

The Intermediary Guidelines 2021 set up a three-tier regulatory system for such publishers, allowing grievances with content to be escalated from a self-regulatory mechanism by publishers themselves, to professional regulatory bodies, to an inter-departmental committee led by MIB.⁸¹⁶ Grievances may be brought against publishers for violating a broadly worded ‘Code of Ethics’, which requires publishers to consider factors such as “*India’s multi-racial and multi-religious context*” prior to publication.⁸¹⁷ The inter-departmental committee may hear disputes arising from the self-regulatory mechanism or the professional regulatory body, or any other cases expressly referred to it by MIB.⁸¹⁸ Publishers are granted a hearing before the committee,⁸¹⁹ which may subsequently issue a direction to “*delete or modify content for preventing incitement*” of a public order offence,⁸²⁰ or pass a direction under Section 69A of the IT Act read with the IT Blocking Rules.⁸²¹ The ‘Authorised Officer’ (similar to the ‘Designated Officer’ under the IT Blocking Rules) shall place the committee’s recommendation before the Secretary, MIB, who shall make the final decision.⁸²² Just as with the IT Blocking Rules, there exists provisions for an emergency order which bypasses the requirement that the publisher is heard⁸²³ and a review committee to scrutinise decisions *ex-post*.⁸²⁴

816 Intermediary Guidelines 2021 r. 9(3).

817 Intermediary Guidelines 2021 Appendix.

818 Intermediary Guidelines 2021 r. 14(2).

819 Intermediary Guidelines 2021 r. 14(4).

820 Intermediary Guidelines 2021 r.14(5)(e).

821 Intermediary Guidelines 2021 r.14(5)(f).

822 Intermediary Guidelines 2021 r. 15(5).

823 Intermediary Guidelines 2021 r. 16.

824 Intermediary Guidelines 2021 r. 17.

Although it is publishers who are represented in hearings, the directions for blocking are specifically made applicable to *intermediaries* (not just the publishers themselves).⁸²⁵ This may be

825 Intermediary Guidelines 2021 r. 8(1) (proviso), 14, 15, 16.

of relevance where the emergency procedure that dispenses with hearings is resorted to, as making the directions applicable to intermediaries would allow the blocking of content without having to engage with the publishers of online news and curated content.

Legal challenges by web-publishers and court stays

Several web publishers challenged the regulatory framework Part III of the Intermediary Guidelines 2021, noting that the ‘Code of Ethics’ was broadly worded and senior civil servants could exercise blocking powers over content.⁸²⁶ The Bombay High Court stayed the operation of the three-tiered mechanism for seeking compliance with the ‘Code of Ethics’, but did not injunct the MIB’s emergency power to block content under Part III of the Intermediary Guidelines 2021.⁸²⁷ The High Court noted that the ‘Code of Ethics’ found in the Intermediary Guidelines sought to enforce *legally* norms that even legislation that specifically regulated publishers (such as the Press Council Act, 1965) only enforced by moral reprimand.⁸²⁸ The High Court also ruled that Part III of the Intermediary Guidelines exceeded the rule-making power of the Union Government under the IT Act and may have a chilling effect on free speech.⁸²⁹ The High Court of Madras also stayed the operation of the three-tier mechanism, and clarified that the decision of the High Court of Bombay has pan-India effect.⁸³⁰

However, as discussed in section 4.5(i) of this report, the Union Government has requested that all legal challenges pertaining to the Intermediary Guidelines be transferred to the Supreme Court and heard together.⁸³¹ At the time of writing this report, the Supreme Court is yet to rule on this request. However, the Supreme Court has directed that the High Courts stop hearing legal challenges to the Intermediary Guidelines 2021,⁸³² but stated orally that the interim (stay) orders passed by the High Court would continue to have effect.⁸³³

826 *Press Trust of India Limited v Union of India* WP (C) 6188 of 2021 (High Court of Delhi); *Foundation for Independent Journalists v Union of India* WP (C) 3125 of 2021 (High Court of Delhi); *The Leaflet (Nineteenone Media Pvt Ltd) v Union of India* WPL 14172 of 2021 (High Court of Bombay); *Quint Digital Media Ltd v Union of India* WP (C) 3659 of 2021 (High Court of Delhi); *Pravda Media Foundation v Union of India* WP (C) 5973 of 2021 (High Court of Delhi); *News Broadcasters Association v Ministry of Electronics and Information Technology* WP (C) 13675 of 2021 (High Court of Kerala); *Truth Pro Foundation of India v Union of India* WP (C) 6941 of 2021 (High Court of Karnataka); *Digital News Publishers Association v Union of India* WP (C) 13055 of 2021 (High Court of Madras); *Nikhil Wagle v Union of India* PIL (L) 14204 of 2021 (High Court of Bombay); *Indian Broadcasting & Digital Foundation v Ministry of Electronics and Information Technology* WP 25619 of 2021 (High Court of Madras).

827 *Agij Promotion of Nineteenone Media Pvt Ltd v Union of India* WP (L) 14172 of 2021 (High Court of Bombay, 14 August 2021).

828 *ibid* [27].

829 *ibid* [28].

830 *TM Krishna v Union of India* WP (C) 12515 of 2021 (High Court of Madras, 16 September 2021); Prasad and Singh (n 502).

831 Chowdhury (n 487).

832 *Skand Bajpai v Union of India* WP (C) 799 of 2020 (Supreme Court of India, 9 May 2022).

833 Mehal Jain, ‘Supreme Court Restrains High Courts From Proceeding In Pleas Challenging IT Rules 2021 & Cable TV Amendment Rules; Interim Orders To Continue’ (*Live Law*, 9 May 2022) <<https://www.livelaw.in/top-stories/breaking-supreme-court-restrains-high-courts-from-proceeding-in-pleas-challenging-it-rules-2021-cable-tv-amendment-rules-interim-orders-to-continue-198614>> accessed 1 August 2022.

8.2. Legal and practical challenges to blocking

Section 69A of the IT Act and the IT Blocking Rules were challenged before the Supreme Court of India in the *Shreya Singhal* proceedings. The petitioners argued that the Rules did not afford content originators a pre-decisional hearing before blocking their content, and the requirement of confidentiality was violative of the Fundamental Rights under the Indian Constitution.⁸³⁴ The Supreme Court disagreed, noting that Section 69A of the IT Act itself created a high threshold for restricting content, and this threshold was in line with constitutionally permissible restrictions free speech.⁸³⁵ As discussed above, the Court observed that the IT Blocking Rules did allow the content originator to be heard before the content was blocked if they were identified.⁸³⁶ Finally, the Supreme Court emphasised that the reasons for blocking were recorded in writing, and thus could be subjected to judicial review.⁸³⁷

Despite this analysis by the Supreme Court, there exists limited evidence of the Union Government in fact issuing pre-decisional notices or conducting hearings prior to blocking content. In response to a request under India's Right to Information Act, 2005 ('RTI Act'), the MEITY stated that it does not keep records of the number of individuals (i.e., originators) that attended hearings under the IT Blocking Rules, although it noted that intermediaries are typically present.⁸³⁸ Reporting on individualised accounts of blocking also supports the conclusion that that originators are not granted hearings. For example, in 2019, a satirical website known as 'Dowry Calculator' was blocked by the Union Government under Section 69A of the IT Act without any pre-decisional notice.⁸³⁹ Despite the owner of the website publicly taking ownership and filing a Right to Information request for disclosure of the blocking direction, the Union Government failed to provide the blocking direction.⁸⁴⁰ This lack of disclosure and pre-decisional hearing was challenged before the High Court of Delhi. The High Court directed the MEITY to disclose the blocking direction under Section 69A and grant the website owner a post-decisional hearing.⁸⁴¹ This is one of the few recorded instances of the MEITY either disclosing the direction under Section 69A or granting an originator a hearing.⁸⁴²

In January 2021, following violence at a public protest in New Delhi, the Union Government directed Twitter to block around 250 user accounts belonging *inter alia* to media organisations,

834 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [113].

835 *ibid* [114].

836 *ibid* [115].

837 *ibid* [114].

838 Internet Freedom Foundation, 'Revealed: MeitY Blocked 6096 URLs and 347 Applications' (*Internet Freedom Foundation*, 23 April 2022) <<https://internetfreedom.in/revealed-meity-blocked-6096-urls-and-347-applications-in-2021-but-held-less-than-40-hearings/>> accessed 1 May 2022.

839 Zaheer Merchant, 'Internet Freedom Foundation Files RTI, Approaches MEITY after Website Satirising Dowry Is Blocked' (*MediaNama*, 15 May 2019) <<https://www.medianama.com/2019/05/223-internet-freedom-foundation-files-rti-approaches-meity-after-website-satirising-dowry-is-blocked/>> accessed 3 March 2021.

840 *ibid*.

841 *Tanul Thakur v Union of India* WP (C) 13037 of 2019 (High Court of Delhi, 11 May 2022).

842 Anushka Jain, 'Show Order for Blocking Website: Delhi High Court to IT Ministry' (*MediaNama*, 19 May 2022) <<https://www.medianama.com/2022/05/223-order-delhi-high-court-meity-section-69a-petition/>> accessed 1 August 2022.

actors, and leaders of the protest, under Section 69A of the IT Act.⁸⁴³ Twitter initially complied with the request but later unblocked several accounts, stating that it had ‘restored access to content in a manner it believed was consistent with Indian law’.⁸⁴⁴ However, following a meeting between Twitter officials and Union Government officials, Twitter substantially complied with the Government’s request.⁸⁴⁵ The Union Government did not disclose the blocking orders, nor was there any record of the originators having been issued a notice or being heard.

In 2022, Twitter instituted a writ petition in the High Court of Karnataka challenging several blocking orders issued under Section 69A of the IT Act.⁸⁴⁶ Twitter has contended that the orders are both procedurally and substantively deficient because they fail to provide a notice to the originator and the content being blocked does not have a nexus with the grounds set out in Section 69A.⁸⁴⁷ Twitter has also claimed that the orders are disproportionate, because at least some orders direct the blocking of entire accounts, and not specific tweets.⁸⁴⁸ In its written response, the Union Government has contended that Twitter’s writ petition seeks to enforce free speech rights, which, as a foreign corporation, it is not entitled to under India’s constitutional framework.⁸⁴⁹ At the time of writing this report, the Karnataka High Court is yet to deliver a verdict.

One possibility is that the Union Government regularly, if not exclusively, adopts the emergency procedure under the IT Blocking Rules, which dispenses with the requirements for the content originator and intermediary to be heard. However, in both the Twitter and Dowry Calculator cases, the Union Government did not contend that the emergency procedure was relied on, indicating that the Union Government’s position is that the originator does not need to be notified under Rule 8 of the Blocking Rules. This understanding is also supported by the fact that the Union Government has blocked content tweeted by Members of Parliament and Members of State Legislative Assemblies without granting them a hearing.⁸⁵⁰ In such situations, identifying the originators and providing them with a notice would clearly be possible within the ‘reasonable efforts’ language set out in Rule 8 of the Blocking Rules.

This interpretation would appear to conflict with the approach set out in *Shreya Singhal*, where the Supreme Court indicated that

843 Revathi Krishnan, ‘Accounts of Prasar Bharati CEO, Caravan, Actor Sushant Singh among Those “withheld” by Twitter’ (*ThePrint*, 1 February 2021) <<https://theprint.in/india/accounts-of-prasar-bharati-ceo-caravan-actor-sushant-singh-among-those-withheld-by-twitter/596638/>> accessed 3 March 2021.

844 Twitter Inc., ‘Updates on Our Response to Blocking Orders from the Indian Government’ (*Twitter Safety Blog*) <https://blog.twitter.com/en_in/topics/company/2020/twitters-response-indian-government.html> accessed 3 March 2021.

845 Saurabh Singh, ‘Twitter Falls in Line, Removes 97% Accounts Flagged by Government of India’ *Financial Express* (12 February 2021) <<https://www.financialexpress.com/industry/technology/twitter-falls-in-line-removes-97-accounts-flagged-by-government-of-india/2193334/>> accessed 3 March 2021.

846 Soumyarendra Barik, ‘Explained: Why Twitter Has Moved Court against Govt’s Content-Blocking Orders’ *The Indian Express* (6 July 2022) <<https://indianexpress.com/article/explained/explained-twitter-lawsuit-government-content-blocking-8012322/>> accessed 4 November 2022.

847 *ibid.*

848 *ibid.*

849 Aarathi Ganesan, ‘Union Pushes to Dismiss Twitter Writ on Section 69A Blocking Orders’ (*MediaNama*, 2 September 2022) <<https://www.medianama.com/2022/09/223-indian-govt-dismiss-twitter-petition-blocking-orders-69a/>> accessed 4 November 2022.

850 Aroon Deep, ‘Twitter Censors Tweets from MP, MLA, Editor Criticising Pandemic Handling’ (*MediaNama*, 24 April 2021) <<https://www.medianama.com/2021/04/223-twitter-mp-minister-censor/>> accessed 4 November 2022.

if the originator was identifiable, they would be heard.⁸⁵¹ The Supreme Court's reasoning also flows from broader constitutional doctrine on State action, that where the State seeks to restrict an individual's fundamental rights, they must do so in a manner that complies with due process and the principles of natural justice.⁸⁵² Finally, it is also worth noting that in addition to the originator, where the Government restricts content under Section 69A, the rights of *all* citizens to *receive* this information is restricted. Thus, any citizen should potentially be able to challenge a blocking order as restricting their right to receive information.

Absent a systematic study of the blocking orders and their supporting documentation, the legal procedures followed by the Union Government are difficult to ascertain. The decision by the High Court of Delhi in the Dowry Calculator case directing the disclosure of the blocking order is a promising judicial intervention, and the case involving Twitter in the Karnataka High Court may provide additional guidance on how Section 69A and the Blocking Rules are to be applied.

Non-disclosure of blocking orders

Despite the Supreme Court's observation that a blocking direction made in writing may be challenged in a court *ex post*, the Union Government has refused to disclose blocking directions under the RTI Act by citing the 'confidentiality' requirement in the IT Blocking Rules.⁸⁵³ This position by the Union Government remains open to debate as the provisions of the RTI Act override other laws,⁸⁵⁴ and themselves contain grounds on which information can be withheld, grounds which do not include 'confidentiality'.⁸⁵⁵ Thus, disclosure of information should only be refused by the government by citing exemptions under the RTI Act itself.⁸⁵⁶ In the Dowry Calculator case, the 'confidentiality' requirement in the Rules was challenged in court as violating the right to information and freedom of speech guaranteed by the Indian Constitution, as it prevents content originators (whose free speech rights are abridged by the orders) and third parties (who may have a right to receive information) from challenging the blocking directions. While High Court of Delhi did not provide any specific reasoning on this issue, it did direct the MEITY to provide the website owner with a redacted copy of the blocking order.⁸⁵⁷

More generally, the Supreme Court of India recently ruled that the Union Government must disclose government orders restricting

851 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [115].

852 *Kranti Associates Pvt Ltd v Masood Ahmed Khan* 2010 (9) SCC 496; *Maneka Gandhi v Union of India* 1978 (1) SCC 248.

853 Software Freedom Law Centre, 'RTI: MeitY Provides Details of Blocked Websites/URLs' (SFLC.in, 2 December 2018) <<https://sflc.in/rTI-meity-provides-details-blocked-websitesurls>> accessed 15 July 2021; Srishti Jaswal, 'Centre Rejects RTI about Blocking Caravan's Twitter Account Citing National Security' (*The Caravan*) <<https://caravanmagazine.in/media/centre-rejects-rTI-about-blocking-caravan-twitter-account-citing-national-security>> accessed 15 July 2021.

854 Right to Information Act, 2005 s. 22.

855 Right to Information Act, 2005 s. 8.

856 Software Freedom Law Centre, 'RTI' (n 853); Jaswal (n 853).

857 *Tanul Thakur v Union of India* WP (C) 13037 of 2019 (High Court of Delhi, 11 May 2022).

internet services in Jammu and Kashmir.⁸⁵⁸ Dealing with government orders suspending the internet under the Telegraph Act, the Supreme Court expressly noted that where State action was challenged as restricting fundamental rights under the Indian Constitution, the State must either disclose the basis of its decision or claim a specific privilege with respect to confidential documents, and the validity of the government's privilege claim would be subject to judicial determination.⁸⁵⁹ This reasoning, coupled with the order in the Dowry Calculator case may guide future courts when faced with confidential blocking orders.

858 *Anuradha Bhasin v Union of India* 2020 (3) SCC 637.

859 *ibid* [24].

8.3. Disclosures of blocking by the Union Government

The limited disclosures that *have* been made by the government point to the frequent use of Section 69A to block content on the internet. The Union Government informed the Indian Parliament, that in 2017, 1,385 webpages, websites, or user accounts had been blocked, while in 2018 and 2019 this number was 2,799 and 3,635 respectively.⁸⁶⁰ The Government also informed the Rajya Sabha (Upper House of Parliament) that 296 mobile applications had been restricted under Section 69A of the IT Act between 2014 and 2020.⁸⁶¹ In response to a right to information request, the Union Government disclosed that it had blocked 6,096 URLs and 347 mobile applications in 2021.⁸⁶²

However, because there exists little clarity on the methodologies and metrics used to arrive at these figures, either by platforms or the government, it is hard to arrive at an accurate representation of the total volume of content restricted under the IT Act. For example, Google's transparency report distinguishes between the number of government requests and the number of "items" sought to be removed; with the company noting that in 2017 it received 1,540 requests to remove 4,696 items from the Indian government, while in 2018 it received 2,474 requests to remove 12,124 items.⁸⁶³ Further, Google's transparency reporting distinguishes between government requests for 'content removal' and 'government-mandated service blockages'.⁸⁶⁴ Given the limited disclosures by the government, disagreements over the informational basis and methodology of calculating the volume of content, and a lack of an independent and systematic study documenting blocked content, the true volume of content blocked under Section 69A remains unclear.

860 Krishnan (n 39).

861 'Government Blocked 296 Mobile Apps since 2014, Says Union Minister Sanjay Dhotre' (n 39).

862 Internet Freedom Foundation (n 838).

863 Google, 'Government Requests to Remove Content' (*Google Transparency Report*) <https://transparencyreport.google.com/government-removals/by-country/IN?country_request_amount=group_by:requestors;period;;authority:IN&lu=country_request_amount> accessed 15 March 2021.

864 Google, 'Government Requests to Remove Content FAQs - Transparency Report Help Center' <<https://support.google.com/transparencyreport/answer/7347744#zippy=%2Chow-is-removal-different-from-blocking-services>> accessed 1 May 2022.

About the National Law University Delhi (NLUD)

The National Law University Delhi is one of the leading law universities in the capital city of India. Established in 2008 (by Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold the constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law.

The University offers a five year integrated B.A., LL.B (Hons.) and one-year postgraduate masters in law (LL.M), along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research. Over the last decade, the University has established many specialised research centres and this includes the Centre for Communication Governance (CCG), Centre for Innovation, Intellectual Property and Competition, Centre for Corporate Law and Governance, Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

About CCG

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research in India on information technology law and policy in India and in a short span of time has become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain.

CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, Law Commission of India, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, and the Tech Policy Design Centre at the Australian National University.

The Centre has had multiple publications over the years including the Hate Speech Report, a book on Privacy and the Indian Supreme Court, and most recently an essay series on Democracy in the Shadow of Big and Emerging Tech. The Centre has launched freely accessible online databases - Privacy Law Library (PLL) and High Court Tracker (HCT) to track privacy jurisprudence across the country and the globe in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. CCG also has an online 'Teaching and Learning Resource' database for sharing research-oriented reading references on infor-

mation technology law and policy. In recent times, the Centre has also offered Certificate and Diploma Courses on AI Law and Policy, Technology Law and Policy, and first principles of cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and ensure their nuanced engagement with the dynamic space of existing and emerging technology and cyberspace, their implications for the society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy.

About the Author

Vasudev Devadasan is a Project Officer at the Centre for Communication Governance, National Law University Delhi (CCG) working on issues of intermediary liability, platform governance, and online speech. Prior to working at CCG, he was a Corporate, Financing, and Restructuring Associate at Trilegal, Mumbai and a Law Clerk to Dr. Justice Dhananjaya Y. Chandrachud (Supreme Court of India).



CENTRE FOR
COMMUNICATION
GOVERNANCE

The Centre for Communication Governance
of The National Law University Delhi (NLU-CCG)
Sector-17, Dwarka, New Delhi-110075, India

www.ccgindia.org

Email: ccg@nludelhi.ac.in

Twitter: [@CCGNLUD](https://twitter.com/CCGNLUD)

