



# DEFEATING DISINFORMATION

Advancing Inclusive Growth and Democracy  
through Global Digital Platforms

## Safe Harbour and Content Moderation Regulation in India

Jhalak M. Kakkar, Shashank Mohan,  
and Vasudev Devadasan

WORK IN PROGRESS

## Authors

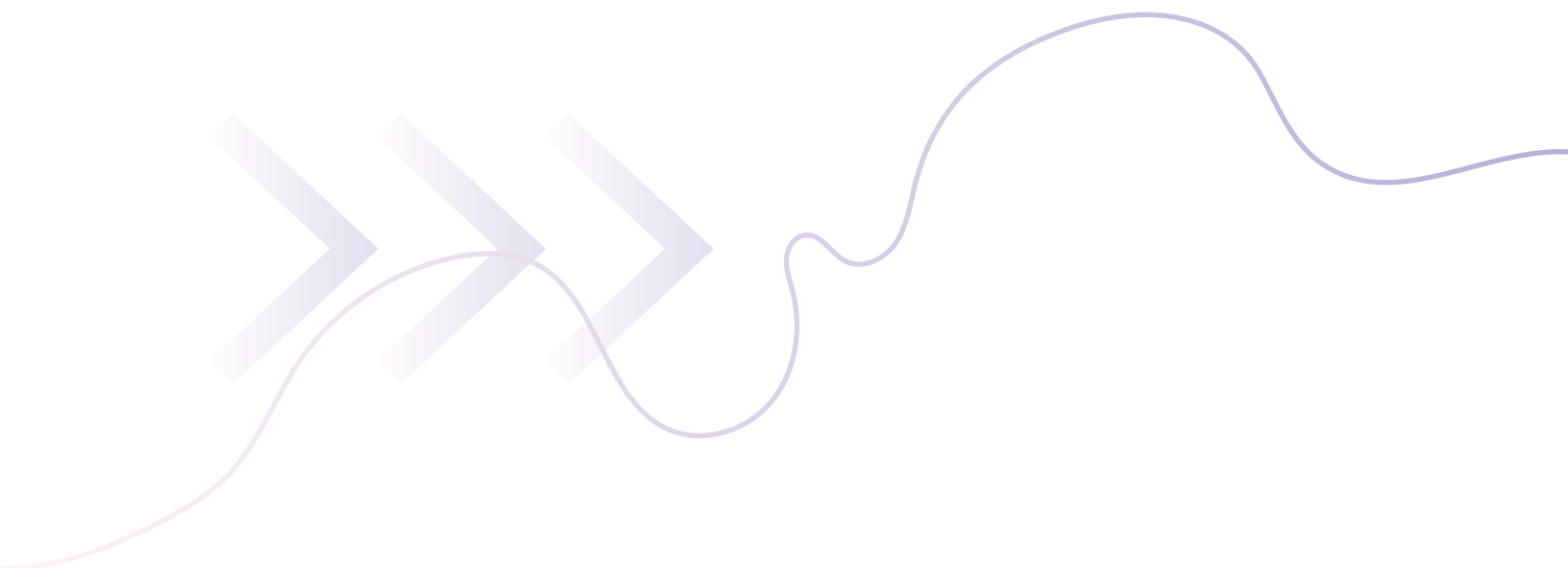
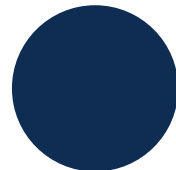
**JHALAK M. KAKKAR**  
Executive Directive, The Centre for Communication  
Governance, National Law University Delhi.



**SHASHANK MOHAN**  
Program Manager at the Centre for Communication  
Governance, National Law University Delhi.



**VASUDEV DEVADASAN**  
Project Officer at the Centre for Communication  
Governance, National Law University Delhi.



# Contents

<b>1. Introduction.....</b>	<b>4</b>
1.1 Centrality of Safe Harbour to Platform Regulation.....	5
1.2 Content Removal by Government Orders .....	6
1.3 Content Prohibited by Intermediary Guidelines and Proposed Amendments..	7
<b>2. Platform Responsibility for Various Subject Areas .....</b>	<b>9</b>
2.1 Hateful, Inciteful, and Defamatory Speech.....	9
2.2 Platform Conduct During Elections .....	10
2.3 Terrorism Related Content .....	10
2.4 Intimidation, Trafficking, Non-Consensual Intimate Content, Child Pornography, and Sexually Explicit Material.....	11
2.5 Content Removals Pursuant to Court or Government Orders.....	11
2.6 Data Protection Obligations .....	12
<b>3. Enforcement of Platform Responsibility.....</b>	<b>13</b>
3.1 Defence to Liability.....	13
3.2 Efficacy of Enforcement .....	14
3.3 Additional Enforcement Methods .....	15
<b>4. Detection and Moderation of Unlawful UGC .....</b>	<b>16</b>
4.1 Obligations to Detect Certain Content Using Automated Tools .....	16
4.2 Responsibilities when Moderating .....	16
4.3 Additional Obligations on SSMIS.....	17
4.4 Obligations on Messaging Platformsontents.....	18
<b>5. Endnotes .....</b>	<b>19</b>

## 1. Introduction

Social media platforms in India are regulated under the Information Technology Act, 2000 (“**IT Act**”). When enacted, the IT Act did not (and possibly could not) envisage the rise of social media platforms and thus, the legislation makes no specific reference to them. However, the IT Act regulates ‘intermediaries’ – defined as entities that receive, store, transmit, or provide any service with respect to third-party content, or user generated content (“**UGC**”).<sup>1</sup> As the activities conducted by social media platforms falls within this definition, platforms have been regulated as intermediaries under the IT Act for the last two decades.

In 2021, the Government issued the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (“**Intermediary Guidelines**”).<sup>2</sup> These Guidelines,<sup>3</sup> which constitute delegated legislation under the IT Act, expressly define a ‘social media intermediary’ as an intermediary which primarily enables online interaction between two or more users and allows them to upload, share, and disseminate content using its services.<sup>4</sup> The Intermediary Guidelines further differentiate between: (i) ‘intermediaries’; (ii) ‘social media intermediaries’; and (iii) ‘significant social media intermediaries’ (“**SSMIs**” i.e., social media intermediaries with more than 5 million Indian users<sup>5</sup>) – imposing additional obligations on SSMIs.<sup>6</sup> The Guidelines also impose certain distinct obligations on SSMIs that provide messaging services.<sup>7</sup> Finally, the Guidelines distinguish between foreign and domestic SSMIs by requiring foreign SSMIs to have local officers who are resident in India; officers who may be subject to personal liability.<sup>8</sup>

As social media platforms constitute intermediaries hosting and transmitting UGC under the IT Act, they are distinguishable from publishers under Indian law, which publish their own content. Platforms are also regulated distinctly from print and broadcast media, which are governed by the Press Council of India Act, 1978 and the Cable Television Networks (Regulation) Act, 1995 respectively. Recently, the Indian Government attempted to regulate online news publishers and providers of ‘online curated content’ (i.e., web-streaming providers such as Netflix and Disney) under Part III of the Intermediary Guidelines.<sup>9</sup> Part III of the Guidelines does not treat these digital media publishers as intermediaries, but rather seeks to regulate these publishers’ content by subjecting them to a broadly worded ‘Code of Ethics’.<sup>10</sup> However, the application of this Code of Ethics to online news publishers and providers of online curated content was recently stayed by the Bombay High Court.<sup>11</sup> The High Court found that drafting and operationalising the Code of Ethics was prima facie beyond the rule-making powers granted to the Government under the IT Act.<sup>12</sup>

**The legal challenges to the Intermediary Guidelines are not limited to Part III. Several individuals and organizations have filed petitions challenging the legality and constitutionality of various provisions of the Intermediary Guidelines in High Courts across the country. The Union Government has requested that all these proceedings be clubbed and heard together by the Supreme Court of India; at the time of writing the Supreme Court is yet to rule on the Union’s request.<sup>13</sup> However, the Supreme Court has directed High Courts to stop hearing the challenges to the Intermediary Guidelines.<sup>14</sup>**

## 1.1. Centrality of Safe Harbour to Platform Regulation

The Intermediary Guidelines, coupled with the rules on government blocking of content,<sup>15</sup> form the core regulatory structure which governs platform conduct in India. Section 79 of the IT Act offers intermediaries conditional legal immunity (or 'safe harbour') for unlawful UGC on their networks. One condition for safe harbour under Section 79 is compliance with the Intermediary Guidelines, which set out various additional obligations that intermediaries must comply with to avail of this safe harbour.<sup>16</sup> **As set out in Sections 3 and 4, the Government has imposed wide ranging obligations on platforms as condition precedent for safe harbour.** However, the power of the Government to prescribe pre-requisites to safe harbour is circumscribed by the Supreme Court decision in *Shreya Singhal v. Union of India*.<sup>17</sup> The Court ruled that intermediaries could not be compelled to take down content at the behest of private complainants to retain safe harbour, and that content could be removed from the internet only pursuant to a government or court order.<sup>18</sup> This has limited the Government's ability to institute a traditional notice-and-takedown regime for online platforms, where platforms risk losing safe harbour if they fail remove content pursuant to user complaints.

To avail of safe harbour under Section 79, an intermediary must:

### 1. **Either limit its functionality to providing access to a communication system over which UGC is transmitted**

**OR**

must not: (i) initiate the transmission; (ii) select the receiver of the transmission; and (iii) select or modify the information contained in the transmission;<sup>19</sup>

### 2. **Comply with the Intermediary Guidelines;**<sup>20</sup>

### 3. **Upon receiving "Actual Knowledge" (interpreted by Shreya Singhal to mean a court order), or being notified by the appropriate government or its agency, of unlawful content on its network, remove the concerned material without vitiating any evidence;**<sup>21</sup> and

### 4. **Not aid, abet, or induce the commission of an unlawful act on its network.**<sup>22</sup>

Additional detail on each of these limbs is provided in Section 3.1 ('Defence to liability'). As noted previously, a key condition to avail of immunity under Section 79 of the IT Act is compliance with the Intermediary Guidelines (i.e., delegated legislation). The Ministry of Electronics and Information Technology ("**MEITY**") has relied on the Intermediary Guidelines to regulate platform behaviour, imposing obligations ranging from transparency reporting

and cooperation with law enforcement, to requiring users be provided with a hearing prior to their content being taken down, under the Intermediary Guidelines,<sup>23</sup> with platforms in breach of these obligations at risk of losing safe harbour. The obligations imposed on platforms under the Intermediary Guidelines are discussed in Sections 3 and 4.

The corollary of this approach is that the exclusive tool to hold social media platforms accountable is through the threat of losing safe harbour, which can only be enforced through individual actions brought before a court of law for hosting unlawful content. This approach may be contrasted with jurisdictions that employ a regulator to penalise platforms for a variety of problematic behaviour. For an intermediary to be penalised in India, an action must be brought against it for hosting unlawful content which proves: (i) the illegality of the content hosted by the intermediary; (ii) the secondary liability of the intermediary in hosting the illegal content; and (iii) the intermediary's ineligibility for safe harbour. The efficacy of this approach is analysed in Section 3.2.

The immunity provided by Section 79 may nonetheless be vital for platform operations in India because, if platforms are ineligible for such immunity, they could incur both civil and criminal liability for content they host. Without such immunity, the regulatory environment around platforms might not be suitable for the creation of a dynamic information and communication system that platforms provide today. This is because Indian law includes a wide range of content-related offences. These content areas are discussed in detail in Section 2. While no platform has definitively been held liable for hosting unlawful UGC, the wide range of criminalised content in India may incentivise platforms to comply with Section 79 and the Intermediary Guidelines to retain safe harbour.

## 1.2. Content Removal by Government Orders

The Indian Government is also empowered to directly block content on the internet under Section 69A of the IT Act in the interests of 'the defence, security, or sovereignty and integrity of India, its friendly relations with other States, public order, or to prevent the incitement of an offence related to these categories. **This provision was used between 2020 and 2022 to block over one hundred mobile applications in India, including popular platforms such as TikTok, WeChat, PUBG, and Helo.<sup>24</sup> The Indian government claimed these applications had been transmitting user data to foreign servers in a manner prejudicial to the integrity and defence of India.<sup>25</sup> Given that these applications were overwhelmingly created by Chinese developers and the restrictions were imposed contemporaneously with a border dispute between India and China, media reports suggested that the blocking of mobile applications was a strategic move by the Indian government against Chinese platforms.<sup>26</sup>**

Intermediaries who fail to comply with directions under Section 69A can be fined and imprisoned for up to seven years.<sup>27</sup> Although blocking under Section 69A ordinarily requires the user who uploaded the disputed content to be provided with a notice and hearing,<sup>28</sup> in emergencies the government may dispense with these procedural safeguards.<sup>29</sup> Further, while blocking orders are required to be reasoned and in writing,<sup>30</sup> the orders themselves are confidential.<sup>31</sup> In practice, there are no publicly reported instances of the government providing an ex-ante hearing to a user or voluntarily disclosing the blocking order.<sup>32</sup> **However, where a website owner challenged the blocking of his satirical website under Section 69A, the Delhi High Court directed the MEITY to disclose the blocking order and grant the website owner a post-decisional hearing.<sup>33</sup>**

Under Part III of the Intermediary Guidelines, the Ministry of Information and Broadcasting is also empowered to: (i) recommend Section 69A blocking of content published by online news publishers or publishers of online curated content;<sup>34</sup> and (ii) delete or modify content published by these entities.<sup>35</sup> However, **as noted above**, this latter power has been stayed by the Bombay High Court.<sup>36</sup>

### 1.3. Content Prohibited by Intermediary Guidelines and Proposed Amendments

Under Rule 3(1)(b) of the Intermediary Guidelines, platforms are required to ensure that their terms of service (“**ToS**”) prohibit users from uploading or sharing a wide range of content including content that is defamatory, harmful to children, obscene, infringes any trademark, patent or copyright, threatens public order or the security of India, or violates any Indian law.<sup>37</sup> These categories (cumulatively “**Intermediary Guidelines Prohibited UGC**”) form the broad umbrella of content that platforms are expected to restrict in their ToS.

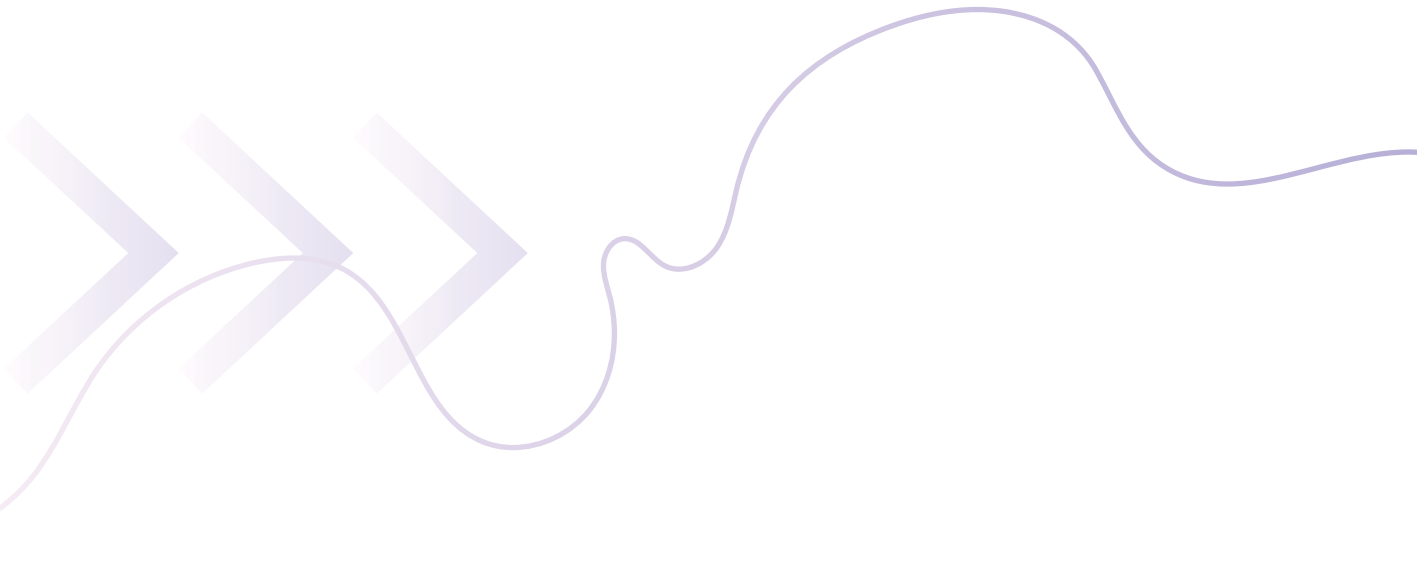
**Rule 3(1)(b) merely requires platforms to prohibit these broad categories of undesirable content through their ToS. Given that in practice, platforms are not denied safe harbour for their content moderation activities**, most large social media platforms will likely remove the above-mentioned categories of content pursuant to their voluntary content moderation activities. However, under the Intermediary Guidelines, platforms are only legally required to inform their users, at least once a year, that noncompliance with the platform’s ToS may result in the removal of non-compliant content or termination of the user’s access to the platform.<sup>38</sup> This means that platforms are merely required to ensure that their ToS’ contain prohibitions against Intermediary Guidelines Prohibited UGC. Platforms are only legally required to remove content when they receive “actual knowledge” of unlawful content on their network – interpreted in Shreya Singhal to mean a court or government order.<sup>39</sup>

### Proposed changes to obligations vis-à-vis prohibited content

In June 2022, the MEITY released draft amendments to the Intermediary Guidelines (“**Proposed Amendments**”) that amend the obligations of platforms with respect to Intermediary Guidelines Prohibited UGC. Under the Proposed Amendments, intermediaries are no longer required to merely include prohibitions against Intermediary Guidelines Prohibited UGC in their ToS, but “shall cause the user” not to upload or share such content, and “ensure compliance” with the platform’s ToS.<sup>40</sup>

A literal interpretation of this language may suggest that the Proposed Amendments change the legal obligation on platforms from – a requirement to include prohibitions against Intermediary Guidelines Prohibited UGC in their ToS’ – to an obligation to prevent users from uploading Intermediary Guidelines Prohibited UGC onto their networks. Such an interpretation would effectively create a strict liability standard for platforms because the hosting of unlawful content by a platform would be a violation of its obligation to prevent users from uploading unlawful content, leading to a breach of the Intermediary Guidelines and consequently a loss of safe harbour.

However, such an interpretation would conflict with Section 79 and other provisions of the Intermediary Guidelines. Section 79(1) of the IT Act expressly provides intermediaries immunity for hosting unlawful content. This immunity would be rendered redundant if platforms lost this immunity simply upon a user uploading unlawful content onto their network. Further, as Section 79(1) constitutes primary legislation, and the Proposed Amendments amend delegated legislation that is the Intermediary Guidelines, the Amendments cannot override the statutory scheme set out in Section 79. Similarly, Rules 3(1)(d) and 3(1)(g) of the existing Intermediary Guidelines expressly state that platforms are only required to remove unlawful content pursuant to a government or court order, or in the case of non-consensual intimate images, pursuant to a user complaint.<sup>41</sup> Thus, despite the language in the Proposed Amendments suggesting that platforms have to prevent users from uploading unlawful content, a holistic reading of Section 79 and the Intermediary Guidelines would indicate that platforms are not required to ensure an absolute prohibition against Intermediary Guidelines Prohibited UGC on their networks, but rather simply ensure such content is prohibited by their ToS'. The Proposed Amendments are currently subject to ongoing public consultation and any amendments adopted by the MEITY may need to be further analysed.





## 2. Platform Responsibility for various Subject Areas

A wide range of content is unlawful under Indian law. This includes online content (primarily regulated by offences in the IT Act), and general application statutes such as the Indian Penal Code, 1860 (“**IPC**”) which regulate content whether found on an online or offline medium. Given the wide range of unlawful content in India, social media platforms may be secondarily liable for UGC on their networks that violate Indian law unless they secure safe harbour under Section 79 of the IT Act. This is because civil or criminal proceedings may be initiated against a platform for hosting unlawful UGC unless the platform can demonstrate it qualifies for immunity under Section 79.<sup>42</sup> Section 79 immunity is applicable against both civil and criminal proceedings that may be brought against platforms.

However, platforms can avoid secondary liability for unlawful content by complying with Section 79 and taking down content upon receiving “actual knowledge” of the unlawful content in the form of a court or government order.<sup>43</sup> The obligations of platforms to take down content do not change based on the subject matter of the content hosted except in the cases of: (i) non-consensual intimate content (which must be taken down within 24 hours of receiving a complaint),<sup>44</sup> and (ii) rape and child-sex-abuse material (which SSMLs must “endeavour” to proactively identify using automated tools).<sup>45</sup> Outside of these two categories, intermediaries, including social media platforms, are only required to take down content pursuant to a court or government order. The remainder of this Section lists content that is unlawful in India and then sets out the data protection obligations imposed on intermediaries.

### 2.1. Hateful, Inciteful, and Defamatory Speech

The IPC criminalises:

Content promoting enmity between – different religious, racial, linguistic groups,<sup>46</sup> caste or communities, or any two classes of people;<sup>47</sup>

Content intended to outrage religious feelings or beliefs;<sup>48</sup>

Content prejudicial to “national integration”;<sup>49</sup> and

Content that is likely to cause “fear or alarm to the public” or incite individuals to breach the public peace.<sup>50</sup>

**Indian law recognises both civil and criminal defamation.**<sup>51</sup> Content that intentionally insults, intimidates, or humiliates a member of a Scheduled Caste or a Scheduled Tribe, including the use of abuses involving caste names is also criminalised in India.<sup>52</sup> **Section 66A of the IT Act proscribed ‘grossly offensive’ or ‘annoying’ expression online; however, this provision was struck down by the Supreme Court of India in 2015 as an unconstitutionally vague and overbroad restriction on free expression.**<sup>53</sup> The Supreme Court has also intervened in the case of Section 124A of the IPC, which criminalises seditious speech (defined as speech that causes ‘disaffection towards the government’). Section 124A is currently subject to a constitutional challenge before the Supreme Court, which in May 2022 ruled that Indian authorities should desist from instituting fresh cases during the pendency of the challenge.<sup>54</sup>

## 2.2. Platform Conduct During Elections<sup>55</sup>

Under Section 171G of the IPC, any person who publishes a statement they know or believe to be false with the intention of affecting the outcome of an election may be fined. Further, content that is “patently false or misleading in nature but may reasonably be perceived as a fact” falls within the ambit of Intermediary Guidelines Prohibited UGC and platforms must prohibit such content in their ToS.<sup>56</sup> More importantly, Indian elections have a high volume of misinformation being disseminated over private messaging platforms such as WhatsApp.<sup>57</sup> In an attempt to curb this misinformation, the Intermediary Guidelines require messaging platforms to trace the ‘originator’ of messages.<sup>58</sup> This obligation is discussed further in Section 4.4 (‘Obligations on messaging platforms’).

While the Election Commission of India’s ‘Model Code of Conduct’ does prescribe certain restrictions on election-related speech,<sup>59</sup> these restrictions are applicable against electoral candidates, and platforms are not held secondarily liable for violations by candidates. Violations of the Model Code of Conduct are typically addressed through non-monetary penalties imposed directly on the candidate (e.g., suspension of campaigning). Similarly, while the use of social media by electoral candidates and political parties is scrutinised by the Election Commission of India, platforms do not have any election-specific obligations under Indian law.

However, in 2019, major online platforms such as Facebook, Google, WhatsApp, and ShareChat (through the Internet & Mobile Association of India) adopted a voluntary ‘Code of Ethics’ that would apply during state and national elections in India.<sup>60</sup> The Code of Ethics has two key commitments. First, the platforms agreed to enforce the ‘cooling off period’ mandated by Section 126 of the Representation of the People Act, 1951;<sup>61</sup> which prohibits the display of any election related content 48 hours prior to polling.<sup>62</sup> This is operationalised by allowing the Election Commission to directly notify platforms of election related content during the ‘cooling off period’, and platforms have committed to take down the flagged content within three hours.<sup>63</sup> The Commission reported that during the 2019 national elections, 909 posts were taken down pursuant to this mechanism, suggesting that the Commission is ultimately only able to flag a small amount of unlawful content.<sup>64</sup>

The second key commitment found in the voluntary Code of Ethics is that platforms will only host political advertisements that have been pre-screened in accordance with the Election Commission’s regulations.<sup>65</sup> Such pre-screening of political advertisements was previously applicable to television, and has been extended to social media through the adoption of this voluntary Code of Ethics. Under the Code, platforms are also required to tag or label political advertisements so that viewers can distinguish between such advertisements from other content on the site.<sup>66</sup>

## 2.3. Terrorism Related Content

Section 66F of the IT Act criminalises “cyber terrorism”. This offence primarily pertains to conduct involving the unauthorised access to a computer network or the denial of access to a computer network that is likely to cause death, injury, or disrupt essential services including critical information infrastructure.<sup>67</sup> However, the provision has sporadically been used against content on social media platforms, primarily against content that allegedly incites communal violence.<sup>68</sup> Where the provision is used against content, platforms may be held secondarily liable for cyberterrorism subject to their defence of safe harbour.

The Indian Government remains conscious of the use of the internet to promote and facilitate terrorism; primarily responding to such situations by directly blocking content under Section 69A of the IT Act or Part III of the Intermediary Guidelines. For example, in 2015 the Government blocked 32 websites in India including vinmeo.com, dailymotion.com, and github.com until they removed content that Indian authorities alleged was ISIS propaganda.<sup>69</sup> More recently, the government has blocked YouTube channels, Facebook accounts, and Twitter accounts for allegedly engaging in coordinated disinformation campaigns that threaten national security.<sup>70</sup> These blocked accounts included accounts operated by organisations made illegal under India's primary anti-terrorism statute, The Unlawful Activities (Prevention) Act, 1967.<sup>71</sup>

## **2.4. Intimidation, Trafficking, Non-Consensual Intimate Content, Child Pornography, and Sexually Explicit Material**

The publishing of content depicting the private area of a person 'under circumstances violating their privacy' is a criminal offence under the IT Act.<sup>72</sup> Under Rule 3(2) of the Intermediary Guidelines, any user can lodge a complaint with an intermediary against content that depicts the user in a state of nudity or committing a sexual act, including content that has been digitally altered to depict the user as such. The intermediary must remove the complained-against content within twenty-four hours and implement a distinct mechanism for such complaints or risk losing safe harbour vis-à-vis this illegal content.<sup>73</sup> In the case of SSIMs, the user must be allowed to track the status of their complaint by being assigned a unique ticket number for their complaint.<sup>74</sup> It is also relevant to note that the IPC criminalises the publication of content that discloses the identity of victims of sexual violence or rape absent express authorisation.<sup>75</sup>

While India does punish extortion,<sup>76</sup> criminal intimidation,<sup>77</sup> online stalking,<sup>78</sup> trafficking,<sup>79</sup> and identity theft,<sup>80</sup> these offences primarily apply to the conduct of individuals using the internet and are thus unlikely to give rise to content-related liability for platforms. While the draft Trafficking of Persons (Prevention, Protection and Rehabilitation) Bill, 2021 punishes the publication of content that promotes trafficking,<sup>81</sup> the draft legislation has yet to be introduced into Parliament. However, India does criminalise the publication of: (i) "obscene material" (content that is lascivious, appeals to the prurient interest, or tends to deprave or corrupt persons);<sup>82</sup> and (ii) sexually explicit material.<sup>83</sup> Thus, platforms could, in principle, be prosecuted for hosting obscene or sexually explicit material; with the ultimate imposition of liability being subject to the platforms' claim to safe harbour under Section 79 of the IT Act.

Finally, the possession or storage of child pornography is criminalised in India.<sup>84</sup> Thus, platforms may be prosecuted for hosting child pornography. Further, under the Intermediary Guidelines, SSIMs have a distinct obligation to "endeavour to deploy" automated tools to proactively identify rape and child sexual abuse material.<sup>85</sup> This obligation is discussed in Section 4.1 ('Obligation to detect').

## **2.5. Content Removals Pursuant to Court or Government Orders**


One of the pre-conditions to safe harbour under Section 79 of the IT Act is that platforms remove content upon receiving court or government orders.<sup>86</sup> Court or government orders directing content removal are not limited to a specific subject area. Courts may require intermediaries to takedown specific content pursuant to injunctions in defamation,<sup>87</sup> or intellectual property suits,<sup>88</sup> the right to be forgotten,<sup>89</sup> remove non-consensual intimate images,<sup>90</sup>

or impose broader obligations to coordinate with government authorities to take down certain classes of content pursuant to public interest litigation.<sup>91</sup> Similarly, government orders have been issued against a wide range of content including (as noted above) Chinese mobile applications alleged to have national security implications,<sup>92</sup> and the Twitter accounts of media organisations.<sup>93</sup>

## 2.6. Data Protection Obligations

Although the Indian Supreme Court has ruled that the right to privacy is a fundamental right guaranteed by the Indian Constitution,<sup>94</sup> India is yet to adopt data protection legislation. The 'Personal Data Protection Bill' was introduced into India's Parliament in 2019 and scrutinised by a Joint Parliamentary Committee which released its report in December 2021.<sup>95</sup> However, the Bill was subsequently withdrawn in August 2022.<sup>96</sup> In the meantime, platforms continue to have certain data protection obligations under the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**"Personal Data Rules"**). Section 43A of the IT Act requires body corporates possessing or handling 'sensitive personal data' to implement reasonable security practices.

The Personal Data Rules define "sensitive personal data" as including passwords, financial information, sexual orientation, medical records, and biometric information. Entities that collect, store or handle sensitive personal data must: (i) collect such information for a lawful purpose; (ii) disclose to users the fact that information is collected, the purpose for which it is collected, and the intended recipients of the information; (iii) only retain sensitive personal data for the time it is necessary for the purpose collected; (iv) allow users to correct incorrect or deficient information upon request; and (v) provide a grievance redressal mechanism.<sup>97</sup> However, these obligations do not apply to entities that collect personal data "under a contractual obligation with another Indian or foreign company,"<sup>98</sup> and thus, are only applicable to entities that directly collect data from users.<sup>99</sup> If platforms fail to comply with the Personal Data Rules, they may be liable to compensate users for any losses stemming from the disclosure of sensitive personal data.<sup>100</sup>



## 3. Enforcement of Platform Responsibility

Compliance with the Intermediary Guidelines constitutes a pre-condition for safe harbour under Section 79 of the IT Act. Therefore, the threat of losing safe harbour under Section 79, which may lead to platforms being held liable for unlawful UGC on their networks, is the primary method of enforcing platform compliance with the various obligations outlined in the Intermediary Guidelines.

### 3.1. Defence to Liability

As noted in the Introduction, to avail of safe harbour, an intermediary must: (i) not initiate the transmission, select the receiver of the transmission, or modify the information contained in the transmission; (ii) comply with the Intermediary Guidelines; and (iii) remove content upon receiving “actual knowledge”.<sup>101</sup>

#### 3.1.1. Neutrality and Moderation

The requirement that platforms must not initiate the transmission, select the receiver of the transmission, or select or modify the information in the transmission is analogous to the requirements of neutrality in Article 12 of the European E-Commerce Directive (‘Mere conduit’). Section 79 does not have an equivalent to Article 14 of the Directive (‘Hosting’), wherein even platforms that are not mere conduits can avail of safe harbour provided they remove content upon receiving actual knowledge. Rather, the text of Section 79 requires intermediaries to be both mere conduits and remove content upon receiving actual knowledge. However, as noted above, no platform has been denied safe harbour due to its interference with content. Furthermore, the Intermediary Guidelines, introduced in 2021, clearly state that the removal of any Intermediary Guidelines Prohibited UGC will not amount to a breach of the neutrality required of Section 79.<sup>102</sup> The Guidelines thus recognise and promote voluntary content moderation by platforms. It remains unclear whether the use of recommender systems would violate the conditions of neutrality required by Section 79. On the one hand, recommender systems may amount to selecting the contents of a transmission. However, no court has specifically returned a finding that a platform’s recommender system violates the neutrality requirements of Section 79. Similarly, the Indian Government has neither suggested that such systems may lead to the loss of safe harbour or attempted to regulate them through the Intermediary Guidelines.

#### 3.1.2. Notice and Actual Knowledge

Neither Section 79 nor the IT Act defines the term “actual knowledge”. Under the previous iteration of the Intermediary Guidelines (adopted in 2011), “actual knowledge” was set out to mean a complaint by another internet user; effectively setting up a traditional notice and takedown regime where platforms were required to remove content pursuant to private complaints.<sup>103</sup> However, in 2015, the Supreme Court of India in *Shreya Singhal v. Union of India* interpreted “actual knowledge” to mean a court or government order.<sup>104</sup> This greatly increased the protection afforded to intermediaries as they were no longer legally required to remove content pursuant to

private complaints,<sup>105</sup> although they remained free to do so in accordance with their ToS' (i.e., voluntary content moderation). However, this interpretation increased the costs and time associated with removing content, potentially placing significant burdens on the victims of online harms.<sup>106</sup>

With the advent of the current iteration of the Intermediary Guidelines (2021), the Indian Government has codified the interpretation in *Shreya Singhal*, noting that platforms are only required to take down content pursuant to a court or government order.<sup>107</sup> While platforms are deemed to have "actual knowledge" and required to remove content pursuant to a private notice in the case of copyright infringing content,<sup>108</sup> and non-consensual intimate images,<sup>109</sup> in all other cases, a platform is not deemed to have "actual knowledge" absent a court or government order.

### 3.1.3. Additional Conditions for Safe Harbour in Intermediary Guidelines

The Intermediary Guidelines also stipulate other conditions platforms must comply with to secure safe harbour, including: (i) data retention obligations;<sup>110</sup> (ii) cooperation with law enforcement;<sup>111</sup> reporting of cyber security incidents;<sup>112</sup> and in the case of SSMLs: (iii) appointing local compliance and grievance officers;<sup>113</sup> (iv) providing users with a notice prior to taking down their content pursuant to ToS violations;<sup>114</sup> (v) publishing transparency reports;<sup>115</sup> (vi) endeavouring to proactively detect rape and child-sex abuse material;<sup>116</sup> and for SSMLs providing messaging services, (vii) identification of the first originator of messages.<sup>117</sup>

### 3.1.4. Proposed Amendments

The Proposed Amendments to the Intermediary Guidelines stipulate that, where a complaint pertains to a request to remove Intermediary Guidelines Prohibited UGC, the complaint shall be "acted on" and "redressed" within 72 hours.<sup>118</sup> The Supreme Court in *Shreya Singhal* expressly disapproved of this approach, noting that platforms receive a high volume of user complaints, and this would effectively lead to platforms deciding which complaints were legitimate and which were not, effectively determining what speech was legal and what speech is not.<sup>119</sup> The Proposed Amendments state that platforms may institute "appropriate safeguards" to avoid abusive complaints by users.<sup>120</sup> However, short time-frames to decide complaints against content has been proven to result in platform overcompliance with removal requests.<sup>121</sup>

## 3.2. Efficacy of Enforcement

The IT Act and the Intermediary Guidelines rely on the risk of losing safe harbour as the primary regulatory tool to govern platform behaviour, imposing varied obligations (see Sections 3.1.3 and 4) on platforms as pre-requisites to safe harbour. However, given that the loss of safe harbour is determined on a case-by-case basis, and the lengthy nature of litigation in India, no platform has definitively been held liable for hosting unlawful content. For example, in 2008 criminal defamation proceedings were instituted against Google for content on its Google Groups platform. Google sought to have the criminal complaint summarily quashed. The issue of whether the charges against Google should be summarily quashed or decided by trial took over a decade to decide, with the Supreme Court ultimately ruling that a trial should be conducted.<sup>122</sup>

This litigation highlights how the nature of litigation in India coupled with the legal resources of platforms may render intermediary liability (i.e., the risk of liability enforced through private lawsuits) a weak regulatory tool to regulate platform behaviour. However, there is some evidence to suggest that the government may believe a loss of safe harbour itself is a penal consequence, with the MEITY having issued Twitter multiple warnings to 'comply with the Intermediary Guidelines or be liable to punishment under the IT Act'.<sup>123</sup>

Finally, it is also relevant to note that the IT Act applies to 'any offence committed outside India'.<sup>124</sup> Additionally, the IPC also applies to any offences that 'target computer resources located in India'.<sup>125</sup> Thus, both statutes envisage extra-territorial application in certain situations. As the primary mechanism to regulate platform conduct is currently Section 79 and the Intermediary Guidelines, which are in the form of pre-requisites to safe harbour against lawsuits initiated against platforms in India, India's regime of platform regulation relies on platforms being subject to the jurisdiction of Indian courts.

### 3.3. Additional Enforcement Methods

In addition to the loss of safe harbour, there exist three methods through which Indian authorities ensure that platforms comply with specific obligations. First, non-compliance with a government direction for content removal under Section 69A of the IT Act is punishable with a prison term of up to seven years and a fine.<sup>126</sup> Similarly, if a platform does not comply with an order of a court, contempt proceedings may be initiated against it.<sup>127</sup> Finally, under the Intermediary Guidelines, SSMLs are required to appoint a Chief Compliance Officer who is a resident in India.<sup>128</sup> This Officer may be held personally liable in any proceedings relating to unlawful UGC on the platform's network if the Officer fails to ensure the platform acts with "due diligence" in complying with the IT Act and the Intermediary Guidelines.<sup>129</sup> However, no liability will be imposed on the Compliance Officer without the Compliance Officer being granted a hearing.<sup>130</sup>



## 4. Detection and Moderation of Unlawful UGC

The Intermediary Guidelines, compliance with which is necessary for platforms to avail of safe harbour under Section 79, impose certain obligations on SSMLs with respect to content moderation. These obligations are not imposed on ordinary intermediaries (that do not perform social media functions or have less than 5 million Indian users).

### 4.1. Obligations to Detect Certain Content Using Automated Tools

SSMLs are required to “endeavour to deploy technology-based measures” to “proactively identify” content that: (i) depicts rape or child sexual abuse material; or (ii) is identical to content that either a court or government order directed be removed.<sup>131</sup> SSMLs are required to disable access to these two categories of content and inform users trying to access this content why the content has been blocked.<sup>132</sup> This best-efforts mandate to use automated tools to detect and remove content is subject to certain safeguards: (a) The action taken by the SSML must be proportionate to the free speech and privacy interests of internet users;<sup>133</sup> (b) the automated tools used by the SSML must be subject to “appropriate human oversight” and periodic review of these automated tools;<sup>134</sup> and finally, (c) the automated tools used by the SSMLs are to be evaluated to ensure “accuracy and fairness”, guard against “the propensity of bias and discrimination”, and determine their impact on privacy and security.<sup>135</sup> While the inclusion of these safeguards is commendable, in the absence of a designated regulator with meaningful oversight and enforcement powers, it is hard to determine whether these safeguards are complied with in practice.

### 4.2. Responsibilities when Moderating

Where an SSML seeks to remove any Intermediary Guidelines Prohibited UGC voluntarily from its platform, Rule 4(8) of the Intermediary Guidelines requires the SSML to provide the user who uploaded the relevant content a notice explaining the grounds for removal before the SSML removes the content.<sup>136</sup> The user must also be provided with an “adequate and reasonable opportunity to dispute” the removal of their content, and seek reinstatement if the content has already been removed.<sup>137</sup> Such disputes must be decided within fifteen days.<sup>138</sup> The Resident Grievance Officer of the SSML is expected to oversee the dispute settlement mechanism under Rule 4(8).<sup>139</sup>

Despite the Intermediary Guidelines being in operation for more than a year, there is no evidence that SSMLs are complying with this notice and hearing requirement. One potential reason for this could be that the consequence of non-compliance with Rule 4(8), as with any provision of the Intermediary Guidelines, is a loss of safe harbour. In another words, failure to provide notice and hearing under Rule 4(8) could lead to a platform losing its immunity for hosting unlawful content. However, when a platform voluntarily removes content, it is not hosting this content and has removed unlawful content prior to when it is legally required to do so (i.e., prior to a court or government order). Therefore, it cannot be held secondarily liable for unlawful content and has few incentives to comply with the conditions necessary to avail of safe harbour. Thus, the loss of safe harbour flowing from a breach of Rule 4(8) may be inconsequential to an SSML where it has already voluntarily decided to not host content.



The Proposed Amendments also contemplate the creation of Grievance Appellate Committee(s), with members appointed by the Indian Government.<sup>140</sup> Any user who is aggrieved with a platform's decision with respect to: (i) the removal/non-removal of non-consensual intimate content; (ii) the removal/non-removal of Intermediary Guidelines Prohibited UGC; or (iii) the suspension or removal of the user's account, may initiate an appeal to the Grievance Appellate Committee.<sup>141</sup> Appeals must be initiated within 30 days of being notified of the platform's decision, and the Committee shall "endeavour" to decide the appeal within 30 days.<sup>142</sup> The Proposed Amendments also clarify that appeals to the Appellate Committee are without prejudice to the user's ability to approach a court of law to seek redress,<sup>143</sup> and that platforms shall respect the constitutional rights of Indian citizens.<sup>144</sup> However, while an individual has sued to enforce his constitutional free speech rights against a platform's moderation decision (citing the platform's power over public speech), this case is still pending before the Delhi High Court.<sup>145</sup> Under current constitutional doctrine, Indian citizens may not enforce their constitutional free speech rights against private social media platforms.<sup>146</sup>

### 4.3. Additional Obligations on SSMLs

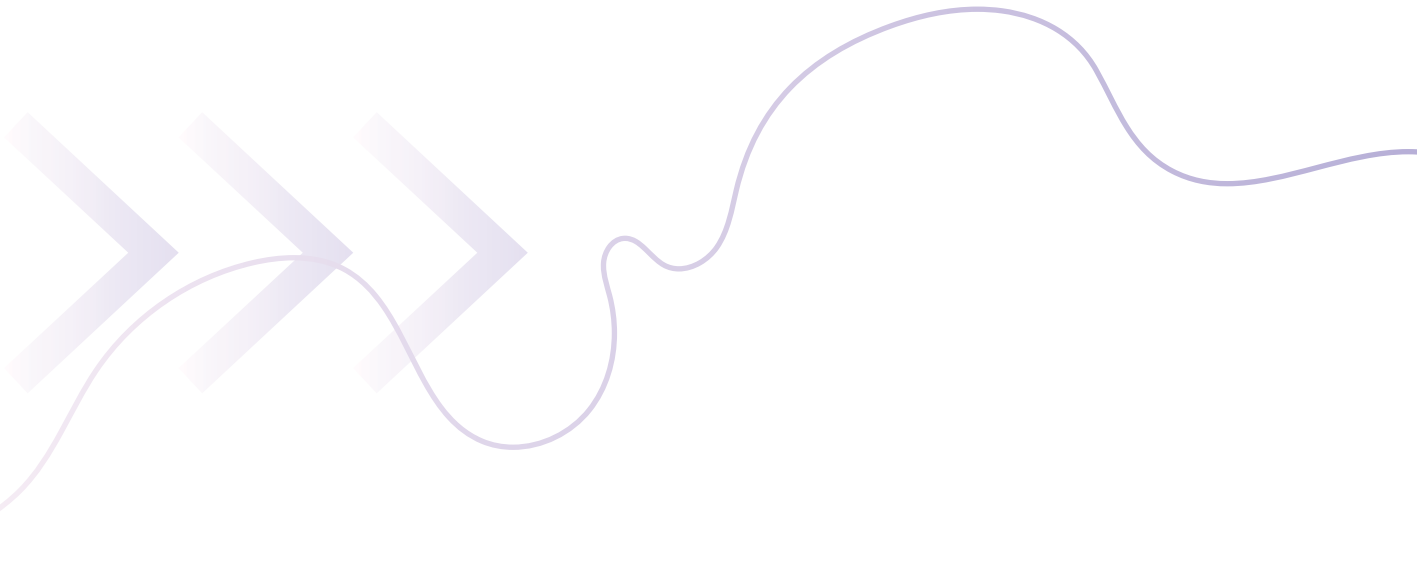
SSMLs are required to publish reports documenting their voluntary content moderation activities and responses to user complaints.<sup>147</sup> However, an analysis of these reports suggests they reveal more about the scale of platform moderation in India than they do about the quality of moderation.<sup>148</sup> SSMLs are also required to provide a user with a "demonstrable and visible mark of verification" (akin to Twitter's 'blue-tick') if the user voluntarily verifies their account using "any appropriate mechanism" including an Indian mobile number.<sup>149</sup> Finally, as noted above, SSMLs are also required to appoint a Resident Grievance Officer, a Chief Compliance Officer who are residents in India,<sup>150</sup> and a nodal contact person to facilitate coordination with law enforcement.<sup>151</sup> However, only the Chief Compliance Officer may be held personally liable.<sup>152</sup>

### 4.4. Obligations on Messaging Platforms

Rule 4(2) of the Intermediary Guidelines requires SSMLs that provide services "primarily in the nature of messaging" to "enable the identification of the first originator" of content on their platforms when directed by a court or an order passed under Section 69 of the IT Act ('power to issue directions for interception, monitoring, or decryption').<sup>153</sup> 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.<sup>154</sup>

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; 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.<sup>155</sup> 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,<sup>156</sup> and that the SSML shall not be required to disclose the contents of any message or any other information regarding the content originator or any information related to its other users.<sup>157</sup>

Critics of the Rule have argued that messaging platforms providing end-to-end-encrypted services cannot trace originators on their platform,<sup>158</sup> and that this is beyond the scope of technical assistance platforms are required to provide law enforcement under Indian law.<sup>159</sup> Facebook and WhatsApp have challenged the legality and constitutionality of Rule 4(2) in the Delhi High Court.<sup>160</sup> As discussed in Section 1, the Union Government has requested these challenges be transferred to the Supreme Court and heard alongside other challenges to the Intermediary Guidelines.



## Endnotes

- 1 The Information Technology Act, 2000, § 2(1)(w).
- 2 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Part III [hereinafter Intermediary Guidelines].
- 3 The Intermediary Guidelines (2021) replaced earlier guidelines which had been in effect since 2011. The 2011 guidelines did not specifically define social media intermediaries. The Intermediary Guidelines 2021 introduce numerous conditions in addition to their predecessor, which have been explained in detail in this paper. See discussion *infra* Sections 3.1.3, 4.
- 4 Intermediary Guidelines, Rule 2(w).
- 5 Ministry of Electronics and Information Technology, S.O. 942(E) (Notified on February 25, 2021).
- 6 Intermediary Guidelines, Rules 2(1)(v), 2(1)(w), 4. See discussion *infra* Sections 3.1.3, 4.
- 7 Intermediary Guidelines, Rule 4(2). See discussion *infra* Section 4.4.
- 8 Intermediary Guidelines, Rule 4(1)(a). See discussion *infra* Section 3.3.
- 9 Intermediary Guidelines, Part III.
- 10 Intermediary Guidelines, Appendix.
- 11 *Nikhil Mangesh Wagle v. Union of India* 2021 SCC Online Bom. 2938.
- 12 *Id.* ¶¶ 24-29.
- 13 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 (2022), <https://www.livelaw.in/top-stories/supreme-court-it-rules-cable-tc-amendment-rules-online-media-ott-regulation-204329> (last visited Aug 1, 2022).
- 14 *Skand Bajpai v. Union of India* WP (Civil) 799 of 2020, decided on 9 May 2022 (Supreme Court of India).
- 15 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 [hereinafter Blocking Rules].
- 16 See discussion *infra* Sections 3.1.3, 4.
- 17 (2015) 5 SCC 1.
- 18 *Id.* ¶ 122. See discussion *infra* Section 3.1.2.
- 19 The Information Technology Act, 2000, § 79(2)(a)-79(2)(b).
- 20 The Information Technology Act, 2000, § 79(2)(c).
- 21 The Information Technology Act, 2000, § 79(3)(b).
- 22 The Information Technology Act, 2000, § 79(3)(a).

## Endnotes

- 23 See discussion *infra* Sections 3.1.3, 4.
- 24 Chinese apps banned in India: India bans 59 Chinese apps including TikTok, WeChat, Helo, THE ECONOMIC TIMES, July 29, 2020, <https://economictimes.indiatimes.com/tech/software/india-bans-59-chinese-apps-including-tiktok-helo-wechat/articleshow/76694814.cms> (last visited Sep 26, 2020); PUBG Mobile, 117 Chinese apps banned in India: Check the full list, THE INDIAN EXPRESS, September 5, 2020, <https://indianexpress.com/article/technology/tech-news-technology/india-bans-pubg-mobile-116-chinese-apps-full-list-6580365/> (last visited Sep 22, 2020); Govt bans 54 Chinese apps over security threat concerns, HINDUSTAN TIMES, February 14, 2022, <https://www.hindustantimes.com/india-news/govt-to-ban-54-chinese-apps-that-pose-threat-to-india-report-101644814634095.html> (last visited Apr 26, 2022).
- 25 Press Information Bureau, Government Blocks 118 Mobile Apps Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order, PRESS INFORMATION BUREAU (2020), <https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1650669> (last visited Aug 30, 2022).
- 26 Sameer Yasir & Hari Kumar, India Bans 118 Chinese Apps as Indian Soldier Is Killed on Disputed Border, THE NEW YORK TIMES, September 2, 2020, <https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html> (last visited Mar 14, 2021).
- 27 The Information Technology Act, 2000, § 69A(3).
- 28 Blocking Rules, rule 8.
- 29 Blocking Rules, rule 9.
- 30 The Information Technology Act, 2000, § 69A(1).
- 31 Blocking Rules, rule 16.
- 32 Apar Gupta, But what about Section 69A?, THE INDIAN EXPRESS, March 27, 2015, <https://indianexpress.com/article/opinion/columns/but-what-about-section-69a/> (last visited Mar 3, 2021).
- 33 Tanul Thakur v. Union of India WP (Civil) 13037 of 2019, decided on 11 May 2022 (High Court of Delhi).
- 34 Intermediary Guidelines, Rule 16.
- 35 Intermediary Guidelines, Rule 14(5)(e).
- 36 Nikhil Mangesh Wagle v. Union of India 2021 SCC Online Bom. 2938.
- 37 Under Rule 3(1)(b) platforms are expected to prohibit the following categories in their ToS:
  - Content that contains a software virus or code that is designed to interrupt, destroy, or limit the functionality of a computer resource;

## Endnotes

- belongs to another person and to which the user does not have any right;
  - 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;
  - 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 relates to or encourages money laundering or gambling;
  - Content that infringes on any trademark, patent, copyright or other proprietary rights;
  - Content that is defamatory, obscene, pornographic, paedophilic, invasive of another user's privacy (including bodily privacy), libellous, insulting of other users on the basis of gender, racially or ethnically objectionable;
  - 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.
- 38 Intermediary Guidelines, Rule 3(1)(c).
- 39 The Information Technology Act, 2000, § 79(3); Intermediary Guidelines, Rule 3(1)(d); *Shreya Singhal v. Union of India* (2015) 5 SCC 1, ¶ 122. See discussion *infra* Section 3.1.2.
- 40 Ministry of Electronics and Information Technology, Proposed draft amendments to the IT Rules, 2021 (Jun. 6, 2022), <https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf> [hereinafter Proposed Amendments] Rules 3(1)(a)-3(1)(b).
- 41 Intermediary Guidelines, Rule 3(2).
- 42 The Information Technology Act, 2000, § 81. There are certain minor carve outs with respect to copyright and patent actions that are not relevant to the present paper.
- 43 See discussion *infra* Section 3.1.2.
- 44 Intermediary Guidelines, Rule 3(2). See discussion *infra* Section 2.4.
- 45 Intermediary Guidelines, Rule 4(4). See discussion *infra* Section 4.1.
- 46 The Indian Penal Code, 1860, § 153A.
- 47 The Indian Penal Code, 1860, § 505(2).
- 48 The Indian Penal Code, 1860, §§ 298, 295A.

## Endnotes

- 49 The Indian Penal Code, 1860, § 153B.
- 50 The Indian Penal Code, 1860, § 505(1).
- 51 The Indian Penal Code, 1860, § 499; Subramaniam Swamy v. Union of India (2016) 7 SCC 221, ¶¶66-68.
- 52 The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989, §§ 3(1)(r)-3(1)(s).
- 53 Shreya Singhal v. Union of India (2015) 5 SCC 1.
- 54 S G Vombatkere v. Union of India WP (Civil) 682 of 2021, decided on May 11, 2022 (Supreme Court of India).
- 55 Intermediary Guidelines, Rule 3(1)(b).
- 56 VIDYA NARAYANAN ET AL., News and Information over Facebook and WhatsApp during the Indian Election Campaign, (2019), <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-memo.pdf>.
- 57 Intermediary Guidelines, Rule 4(2). See discussion infra Section 4.4.
- 58 Model Code of Conduct, ELECTION COMMISSION OF INDIA, <https://eci.gov.in/mcc/> (last visited Apr 20, 2022).
- 59 Press Information Bureau, “Voluntary Code of Ethics” by Social Media Platforms to be observed in the General Election to the Haryana & Maharashtra Legislative Assemblies and all future elections, (2019), <https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1586297> (last visited Apr 20, 2022).
- 60 Internet and Mobile Association of India, Voluntary Code of Ethics - reg. (Sep. 23, 2019), <https://static.pib.gov.in/WriteReadData/userfiles/IAMAI-ECI%20VCE.pdf> [hereinafter IAMAI Code of Ethics].
- 61 The Representation of the People Act, 1951, § 126(1)(b).
- 62 IAMAI Code of Ethics.
- 63 Nalin Mehta, Digital Politics in India’s 2019 General Elections, 54 ECONOMIC AND POLITICAL WEEKLY (2019), <https://www.epw.in/engage/article/digital-politics-indias-2019-general-elections> (last visited Sep 25, 2020).
- 64 IAMAI Code of Ethics.
- 65 IAMAI Code of Ethics.
- 66 The Information Technology Act, 2000, § 66F.
- 67 Three Kashmiri students arrested in Agra for celebrating Pakistan’s cricket win against India, <https://scroll.in/>, October 28, 2021, <https://scroll.in/latest/1009069/three-kashmiri-students-arrested-in-agra-for-celebrating-pakistans-cricket-win-against-india> (last visited Jun 29, 2022); Mukesh Kumar, Hisar journalists say junk FIR as cops look for colleague, THE TIMES OF INDIA, April 12, 2021, [https://timesofindia.indiatimes.com/city/chandigarh/journalists-say-junk-fir-as-cops-look-for-colleague/articleshow/82021430.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cppst](https://timesofindia.indiatimes.com/city/chandigarh/journalists-say-junk-fir-as-cops-look-for-colleague/articleshow/82021430.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst) (last visited Jun 29, 2022).

## Endnotes

- 68 Kim Arora, Government blocks 32 websites to check ISIS propaganda, THE TIMES OF INDIA, January 1, 2015, <https://timesofindia.indiatimes.com/tech-news/government-blocks-32-websites-to-check-isis-propaganda/articleshow/45712815.cms> (last visited Jun 12, 2022).
- 69 Sarvesh Mathi, MIB blocks twenty-two YouTube channels for spreading fake news, MEDIANAMA (2022), <https://www.medianama.com/2022/04/223-mib-blocks-youtube-channels/> (last visited Jun 12, 2022).
- 70 Id.
- 71 The Information Technology Act, 2000, § 66E.
- 72 Intermediary Guidelines, Rule 3(2)(b).
- 73 Intermediary Guidelines, Rule 4(6).
- 74 The Indian Penal Code, 1860, § 228A.
- 75 The Indian Penal Code, 1860, § 383
- 76 The Indian Penal Code, 1860, § 505
- 77 The Indian Penal Code, 1860, § 354D
- 78 The Indian Penal Code, 1860, § 370.
- 79 The Information Technology Act, 2000, § 66C
- 80 Ministry of Women and Child Development, Draft Trafficking in Persons (Prevention, Care and Rehabilitation) Bill, 2021 (Jun. 2021), <https://wcd.nic.in/sites/default/files/DRAFT%20TRAFFICKING%20IN%20PERSONS%20%28PREVENTION%2C%20CARE%20AND%20REHABILITATION%29%20BILL%202021%20%281%29.pdf>, Section 29.
- 81 The Information Technology Act, 2000, § 67.
- 82 The Information Technology Act, 2000, § 67A.
- 83 The Protection of Children from Sexual Offences Act, 2012, § 15; the Information Technology Act, 2000, § 67B.
- 84 Intermediary Guidelines, Rule 4(4). See discussion *infra* Section 4.1.
- 85 The Information Technology Act, 2000, § 79(3); Intermediary Guidelines, Rule 3(1)(d).
- 86 Subodh Gupta v. Herdsceneand CS (OS) 483 of 2019 decided on Sep. 18, 2019 (High Court of Delhi); Zulfiqar Ahmad Khan v. Quintillion Business Media CS (OS) 642 of 2018, decided on Dec. 14, 2018 (High Court of Delhi).
- 87 Jagran Prakashan Ltd. v. Telegram FZ LLC CS (Comm) 146 of 2020, decided on May 29, 2020 (High Court of Delhi); Dept. of Electronics and Information Technology v. Star India Pvt. Ltd. FAO (OS) 57 of 2015, decided on Jul. 29, 2016 (High Court of Delhi); Snapdeal Pvt. Ltd. v. GoDaddy LLC CS (Comm) 176 of 2021, decided on Apr.

## Endnotes

- 18, 2022 (High Court of Delhi).
- 88 *Jorawer Singh Mundy v. Union of India* WP (Civil) 3918 of 2021, decided on Apr. 17, 2021 (High Court of Delhi).
- 89 *X V. Union of India* WP (Cri) 1082 of 2020, decided on Apr. 20, 2021 (High Court of Delhi).
- 90 *Sabu Mathew George v. Union of India* (2017) 2 SCC 514 (advertising for pre-natal sex determination procedures); *Registrar (Judicial) v. Union Ministry of Communications* 2017 SCC Online 25298 Mad. (content related to video games alleged to promote suicide); *In re: Prajwala* Letter dated 18.2.2015 SMW (Cri) 3 of 2015 (rape videos).
- 91 Chinese apps banned in India: India bans 59 Chinese apps including TikTok, WeChat, Helo, *supra* note 27; Yasir and Kumar, *supra* note 29.
- 92 Revathi Krishnan, Accounts of Prasar Bharati CEO, Caravan, actor Sushant Singh among those “withheld” by Twitter, THEPRINT (2021), <https://theprint.in/india/accounts-of-prasar-bharati-ceo-caravan-actor-sushant-singh-among-those-withheld-by-twitter/596638/> (last visited Mar 3, 2021). *K S Puttaswamy v. Union of India* (2017) 10 SCC 1.
- 93 *K S Puttaswamy v. Union of India* (2017) 10 SCC 1.
- 94 The Personal Data Protection Bill, 2019, PRS LEGISLATIVE RESEARCH, <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019> (last visited Jun 13, 2022).
- 95 Govt withdraws data protection bill, 2021, THE ECONOMIC TIMES, August 4, 2022, <https://economictimes.indiatimes.com/tech/technology/govt-withdraws-data-protection-bill-2021/articleshow/93334281.cms> (last visited Aug 8, 2022).
- 96 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011; Collection & Processing in India - DLA Piper Global Data Protection Laws of the World, <https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=IN> (last visited Jun 13, 2022).
- 97 Ministry of Communications & Information Technology, Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under section 43A of the Information Technology Act, 2000 (Aug. 24, 2011), [https://www.meity.gov.in/writereaddata/files/PressNote\\_25811.pdf](https://www.meity.gov.in/writereaddata/files/PressNote_25811.pdf).
- 98 ADITI CHATURVEDI, GDPR and India, (2017), <https://cis-india.org/internet-governance/files/gdpr-and-india> (last visited Jun 16, 2022).
- 99 The Information Technology Act, 2000, § 43A.
- 100 See discussion *supra* Section 1.1.
- 101 Intermediary Guidelines, Rule 3(1)(d)(third proviso).



## Endnotes

- 102 CHINMAYI ARUN & SARVJEET SINGH, NoC Online Intermediaries Case Studies Series: Online Intermediaries in India, (2015), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2566952](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566952).
- 103 Shreya Singhal v. Union of India (2015) 5 SCC 1.
- 104 Kyung-Sin Park, From Liability Trap to the World's Safest Harbour: Lessons from China, India, Japan, South Korea, Indonesia, and Malaysia, in OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 250 (Giancarlo Frosio ed., 2020).
- 105 T Prashant Reddy, Back to the drawing board: What should be the new direction of intermediary liability law?, 1 NLUJ. OF LEGAL STUDIES 38 (2019).
- 106 Intermediary Guidelines, Rule 3(1)(d).
- 107 The Copyright Act, 1957 § 52(1)(c); The Copyright Rules, 2013, Rule 75; Myspace Inc. v. Super Cassettes Industries Ltd. 2016 SCC Online Del. 6382; Aradhya Sethia, The troubled waters of copyright safe harbours in India, 12 JOURNAL OF INTELLECTUAL PROPERTY LAW & PRACTICE 398-407 (2017).
- 108 Intermediary Guidelines, Rule 3(2).
- 109 Intermediary Guidelines, Rules 3(1)(g)-3(1)(h).
- 110 Intermediary Guidelines, Rule 3(1)(j).
- 111 Intermediary Guidelines, Rule 3(1)(l).
- 112 Intermediary Guidelines, Rule 4(1)(a)-(c).
- 113 Intermediary Guidelines, Rule 4(8). See discussion *infra* Section 4.2.
- 114 Intermediary Guidelines, Rule 4(1)(d). See discussion *infra* Section 4.3.
- 115 Intermediary Guidelines, Rule 4(4). See discussion *infra* Section 4.1.
- 116 Intermediary Guidelines, Rule 4(2). See discussion *infra* Section 4.4.
- 117 Proposed Amendments, Rule 3(2)(i).
- 118 Shreya Singhal v. Union of India (2015) 5 SCC 1.
- 119 Proposed Amendments, Rule 3(2)(i).
- 120 ARUN AND SINGH, *supra* note 106; Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, SSRN JOURNAL (2011), <http://www.ssrn.com/abstract=2038214> (last visited Feb 18, 2021).
- 121 Google India Pvt. Ltd. v. Visaka Industries (2020) 4 SCC 162.
- 122 Aashish Aryan & Surabhi Agarwal, Twitter India given 'last chance' to follow IT rules, ETTELECOM.COM, <https://telecom.economictimes.indiatimes.com/news/twitter-india-given-last-chance-to-follow-it->

## Endnotes

- rules/92532133 (last visited Jun 30, 2022).
- 123 The Information Technology Act, 2000, § 1(2).
- 124 The Indian Penal Code, 1860, § 4(3).
- 125 The Information Technology Act, 2000, § 69(3).
- 126 Facebook Inc v. Swami Ramdev FAO (OS) 212 of 2019, decided on Jan. 28, 2020 (High Court of Delhi).
- 127 Intermediary Guidelines, Rule 4(1)(a).
- 128 Intermediary Guidelines, Rule 4(1)(a).
- 129 Intermediary Guidelines, Rule 4(1)(a).
- 130 Intermediary Guidelines, Rule 4(4).
- 131 Intermediary Guidelines, Rule 4(4).
- 132 Intermediary Guidelines, Rule 4(4) (first proviso).
- 133 Intermediary Guidelines, Rule 4(4) (second proviso).
- 134 Intermediary Guidelines, Rule 4(4) (third proviso).
- 135 Intermediary Guidelines, Rule 4(8)(a).
- 136 Intermediary Guidelines, Rule 4(8)(b).
- 137 Intermediary Guidelines, Rule 4(8)(b).
- 138 Intermediary Guidelines, Rule 4(8)(c).
- 139 Proposed Amendments, Rule 3(3)(a).
- 140 Proposed Amendments, Rule 3(3)(b).
- 141 Proposed Amendments, Rule 3(3)(c).
- 142 Proposed Amendments, Rule 3(3)(a).
- 143 Proposed Amendments, Rule 3(1)(n).
- 144 Shrayya Reddy, Does Twitter perform public functions? The Sanjay Hegde case, BAR AND BENCH, November 13, 2020, <https://www.barandbench.com/columns/does-twitter-perform-public-functions-the-sanjay-hegde-case> (last visited May 16, 2021).
- 145 See Ananth Padmanabhan, Rights: breadth, scope, and applicability, in OXFORD HANDBOOK ON THE INDIAN CONSTITUTION (Sujit Choudhry, Madhav Khosla, & Pratap Bhanu Mehta eds., 2016).
- 146 Intermediary Guidelines, Rule 4(1)(d).

## Endnotes

- 147 Vasudev Devadasan, Compliance reports by social media platforms are unhelpful, MEDIANAMA, April 18, 2022, <https://www.medianama.com/2022/04/223-transparency-reports-social-media-platforms-unhelpful/> (last visited Apr 27, 2022).
- 148 Intermediary Guidelines, Rule 4(7).
- 149 Intermediary Guidelines, Rules 4(1)(a), 4(1)(c).
- 150 Intermediary Guidelines, Rule 4(1)(b).
- 151 Intermediary Guidelines, Rule 4(1)(a).
- 152 Intermediary Guidelines, Rule 4(2).
- 153 Intermediary Guidelines, Rule 4(2) (fourth proviso).
- 154 Intermediary Guidelines, Rule 4(2) (first proviso).
- 155 Intermediary Guidelines, Rule 4(2) (second proviso).
- 156 Intermediary Guidelines, Rule 4(2) (third proviso).
- 157 Aditi Agarwal, Traceability And End-to-end Encryption Cannot Co-exist On Digital Messaging Platforms: Experts, FORBES INDIA, March 15, 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> (last visited May 21, 2021).
- 158 Vrinda Bhandari, Rishab Bailey & Faiza Rahman, Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance," SSRN JOURNAL (2021), <https://www.ssrn.com/abstract=3805980> (last visited May 1, 2021).
- 159 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).
- 160



RESEARCH PARTNER

