BSA SUBMISSION
ON THE
DRAFT AMENDMENTS TO THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

Shri. Dhawal Gupta,
Scientist E,
Ministry of Electronics and Information Technology,
Email: dhawal.gupta@meity.gov.in

Wednesday, July 06, 2022

Dear Sir,

Subject: BSA Submission on the draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit comments on the draft amendments (**Draft Amendments**) to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**IT Rules, 2021**) released by the Ministry of Electronics and Information Technology (**MeitY**).[2]

We acknowledge that online content platforms can play an important role in curbing the spread of unlawful content online by taking down unlawful content in a timely manner. However, we are concerned that the Draft Amendments do not account for the technical distinctions between different kinds of intermediaries, and as a result, unintentionally impose obligations that are infeasible for enterprise service providers. Several obligations in the Draft Amendments are vague and seemingly require intermediaries to act proactively to remove or filter unlawful content, contradicting the "actual knowledge" standard developed by the Supreme Court for taking down content.

We discuss our concerns and recommendations in detail below.

1. A "one-size-fits-all" approach makes compliance infeasible.

The definition of "intermediary" under the IT Act covers a wide range of service providers, including Internet service providers, cloud service providers, infrastructure-as-a-service providers, and consumer-facing social media platforms, video sharing sites, etc. Recognizing this distinction, the IT

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Proposed amendments, accessible at: https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf.

Rules, 2021 created a separate category of "social media intermediaries" that are subject to additional compliances, given the nature of services they provide. MeitY has also clarified that intermediaries whose primary purpose is enabling commercial or business-oriented transactions, and which offer online storage or other services will not be treated as a social media intermediary.[3]

However, the Draft Amendments do not account for this distinction. While the press release accompanying the Draft Amendments indicates that the requirements are aimed at social media platforms, the proposals relate to Rule 3 of the IT Rules, 2021, which applies to all intermediaries.

The Draft Amendments require intermediaries to "cause" users to not host, display, upload, modify, store or share any unlawful information.[4] This assumes that all intermediaries can identify and remove unlawful information on their own. However, enterprise service providers such as cloud service providers and others have no visibility or access to content that they host or store on behalf of enterprise customers and compliance would be practically infeasible for them. For instance, cloud Infrastructure-as-a-Service providers offer computing power and database storage upon which their enterprise customers can build and run their own public-facing online services. Software-as-a-Service (SaaS) providers similarly process data and enable capabilities such as collaboration on behalf of their customers under contractual obligations to protect the customers' data. Such enterprise cloud service providers do not have unfettered access to the data stored by their enterprise customers. Therefore, a cloud infrastructure provider would be unable to ensure that end users of the enterprise customers do not display or upload any unlawful content.

Because the Draft Amendments are intended to address risks that are unique to social media platforms, we recommend that Rule 3(1)(b) apply only to "social media intermediaries" as defined in the IT Rules, 2021. We recommend that any amendments also recognize the unique nature of enterprise service providers and refrain from imposing over-broad requirements related to content filtering or removal on all intermediaries.

2. Enhanced obligations on intermediaries are vague and contradict settled law on safe harbor.

Under India's well-settled intermediary liability regime, intermediaries are granted 'safe harbour' protection from liability for third-party content hosted on their platforms if they abide by due diligence and other requirements under the IT Rules, 2021. Intermediaries lose such protection if they do not remove unlawful content even after receiving "actual knowledge" regarding such content.[5]
In *Shreya Singhal v. Union of India*, the Supreme Court clarified that actual knowledge shall mean the receipt of a valid court order or official government order.[6]

However, the Draft Amendments require intermediaries to "ensure" users' compliance with the platform's terms of service and other guidelines and also "cause" the user to not host, display, upload, modify, publish, transmit, store, update or share any information that is determined to be unlawful content under Rule 3.[7] The scope of such an obligation is unclear, and could potentially be interpreted as an obligation for intermediaries to institute proactive filtering mechanisms. If so, this will contradict the settled position regarding content takedowns set out in the Supreme Court's decision in the Shreya Singhal case. It could lead to intermediaries being required to block even legitimate content to ensure compliance and impact free speech of users online.

[3] FAQs to the IT Rules, 2021, accessible at: https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf
[4] Rule 3(1)(b) of the Amendments.
[5] Section 79 of the Information Technology Act 2000.
[6] AIR 2015 SC 1523, accessible at: https://www.meity.gov.in/writereaddata/files/Honorable-Supreme-Court-order-dated-24th-March%202015.pdf
[7] Rule 3(1)(a) and 3(1)(b) of the Amendments.

If applied to enterprise service providers, a proactive monitoring requirement could also implicate significant privacy and cybersecurity concerns. While some social media platforms voluntarily implement filtering technologies, imposing a blanket requirement on enterprise service providers would result in numerous unintended – and potentially catastrophic – impacts. BSA members provide cloud-based tools and services to enterprise customers, including organizations in the healthcare, banking, energy, and defense industries. Given the sensitivity of their customers' data, enterprise cloud service providers design their systems so that they have limited – if any – visibility into the data they are hosting and/or processing on behalf of their clients. Imposing a filtering requirement on enterprise cloud service providers – e.g., infrastructure-as a-service providers and platform-as-a-service providers -- would thus, require them to reengineer their networks in ways that would create significant privacy and security concerns. It could, for instance, prevent enterprise service providers from offering user-controlled encryption protections that are critical to the security of sensitive data. Such an outcome could place service providers out of compliance with legal and contractual obligations, thus exposing them to potential liability.

The MeitY, however, has clarified that the additional compliances prescribed under proposed Rule 3(1)(a) and 3(1)(b) are to be read with the existing obligations under Rules 3(1)(d) and 3(1)(g),[8] which provide for action to be taken by intermediaries on the basis of actual knowledge of any violation (and not proactive monitoring for compliance) and storage of related records for 180 days. This implies that intermediaries must build mechanisms to act quickly whenever informed of any violation by the government or a user – which is aligned with Section 79 of the IT Act and the Supreme Court's *Shreya Singhal v. Union of India* judgement. While the clarification is appreciated, it is not legally binding. This means that companies cannot effectively rely upon it while planning their compliance and commercial operations.

In this regard, we recommend that the MeitY incorporate this clarification into the text of the Draft Amendments, by making specific changes to the language of proposed Rules 3(1)(a) and 3(1)(b).

The Draft Amendments also require intermediaries to respect users' constitutional rights and to take reasonable measures to ensure "accessibility of its services to users along with reasonable expectation of due diligence, privacy and transparency".[9] The meaning of the term "accessibility" is unclear, while there is an equal amount of confusion on how intermediaries are meant to implement the requirement to respect users' constitutional rights. The broad and ambiguous nature of these obligations can create an environment of regulatory uncertainty, which will make it harder for companies to plan and implement their compliance programs. Further, the IT Rules, 2021 already set out a host of due diligence requirements for intermediaries, such as displaying their terms and conditions and privacy policy prominently on their website, informing users about unlawful or prohibited content, removing unlawful content on receiving actual knowledge, among others. It is unclear if these obligations require intermediaries to go beyond these due diligence requirements.

We recommend that the MeitY reconsider the addition of Rules 3(1)(m) and 3(1)(n) in the Draft Amendments due to the lack of clarity on the objectives for introducing these provisions, along with concerns around their implementation.

3. Sharp timelines for content takedown are impractical.

We acknowledge the government's concerns over the spread of fake news and harmful content online. However, the Draft Amendments set a 72-hour timeline for removal of unlawful content which

[8] Statement made by Hon'ble Minister of State for Electronics and Information and Technology on 23 June 2022, at the stakeholder consultation on the Draft Amendments.
[9] Rule 3(1)(m) of the Amendments.

will be difficult to implement in practice.[10] In particular, enterprise software service providers such as hosting and cloud service providers lack the visibility and control over content to action such requests in a timely manner. First and foremost, any such requests should be directed at the customer responsible for the content rather than the enterprise software service provider supporting that content. Otherwise, once a request is received by the enterprise software service providers, the providers must reach out to their customers to identify and then remove content. If a hosting service provider receives a request for removing unlawful content, it will not be able to selectively identify the offending content and will have to simply shut down the enterprise customer's entire service. Further, compliance with these sharp timelines for content removal may drive intermediaries to remove all allegedly unlawful content in the interest of time. This could have a chilling effect on users' free speech and in fact, runs counter to Rule 3(n) of the Draft Amendments which requires intermediaries to respect users' constitutional rights.

Given that different types of service providers have different levels of access to content hosted or shared on their platforms, we recommend that the MeitY remove the requirement under Rule 3(2)(i) for intermediaries to redress user requests for removing unlawful content within a 72-hour timeline.

4. The powers and role of the proposed grievance appellate committee are not well-defined.

The "Grievance Appellate Committee" (**GAC**) under the Draft Amendments is envisaged as an alternative redressal mechanism for individuals. While we acknowledge the government's intent in providing a remedy to users, in its current form, the GAC is not subject to any checks and balances. Since the GAC will hear appeals from users about removal of unlawful content, it will sit as a quasi-judicial body, assessing whether the offending content in question falls within the list of unlawful content and weighing a user's fundamental right to free speech against the infringing content's alleged illegality. However, the Draft Amendments do not specify any details around appointment of the chairperson and members of the GAC, their qualifications and eligibility, whether they are required to be technical experts, the terms of their service, or powers of the GAC. It is also unclear how an intermediary (or a user) can appeal against an order of the GAC. Typically, such quasi-judicial bodies are established through legislation, which circumscribes their powers and functions.

We recommend a wider public consultation on the need for alternative mechanisms for grievance redressal and possible modes before setting up a new administrative machinery.

Thank you again for the opportunity. If you require further information in respect of this submission, please contact Mr. Venkatesh Krishnamoorthy at venkateshk@bsa.org.

Sincerely,

BSA | The Software Alliance

[10] Proviso to Rule 3(2)(a)(i) of the Amendments.