

## Will Social Media Platforms Be Banned?

written by Sindhuja Kashyap | May 26, 2021



The internet has gone for a toss amidst the news of the failure of compliance by giant social media platforms with the new Social Media intermediary rules of India and as such, speculation of consequences ranging from banning to criminal liability has overtaken all platforms. In this article, we try to explain what the requirements under the said new law are, to whom this law applies and what the consequences of it are. We have already dealt with the new law in detail here. Therefore, this article will only focus on the specific compliances creating the uproar on the internet.

What is the “breaking news” law?

The Ministry of Electronics and Information Technology had on February 25, 2021 notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021<sup>[1]</sup> (“Rules”) with an aim to regulate the uprising unregulated social media platforms in the country.

The Rules not only increased the accountability of the social media platforms but also increased and eased the redressal mechanism for the users. While most of the compliances under the Rules were to be implemented on the date of their publication in the Official Gazette i.e. February 25, 2021, Rule 4, of the Rules which identified additional due diligence to be followed by the significant social media intermediary, was due to be effective within three months from the date of notification of the threshold i.e., three months from February 25, 2021 which ended on May 25, 2021.

What is a “Significant Social Media Intermediary”?

As per Rule 2(1)(v) read with the notification dated February 25, 2021<sup>[2]</sup>, a significant social media intermediary<sup>[3]</sup> shall mean a social media intermediary having more than fifty lakh registered users in India (“SSMI”). Therefore, any social media intermediary having more than fifty lakh registered users in India was mandated to ensure compliance with Rule 4 of the Rules by or before May 25, 2021.

What are the requirements to be complied with prior to May 25, 2021?

As per Rule 4, the SSIMs are required to observe additional due diligence while discharging their duties under the Rules:

1. Appointment of a Chief Compliance Officer<sup>[4]</sup> (“CCO”). CCO shall be responsible for ensuring compliance with the information technology law of the country. Further, they shall be responsible in any proceedings relating to any relevant third-party information, data or communication link made available

or hosted by the SSMI wherein the CCO failed to ensure that the SSMI observed adequate due diligence while discharging its duties.

2. Appointment of a nodal contact person<sup>[5]</sup>. Such a person shall be responsible for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provision of law or rules made thereunder.
3. Appointment of Resident Grievance Officer ("RGO").<sup>[6]</sup> RGO shall be required to acknowledge a complaint from a user within 24 hours and dispose of such complaint within 15 days from the date of receipt. Further, he/she shall also be responsible to receive and acknowledge any order, notice or direction.
4. Publish monthly compliance report providing details of the complaints received and action taken in addition to the details of communication/link which the SSMI has disabled or removed or any other relevant information.
5. SSMI providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as mandated by judicial order passed by the court or a competent authority under Section 69 of the IT Act.
6. Ensure the information being published/transmitted by SSMI for financial gain or to which copyright or license is owned via contract clearly showcases the requisite information as being advertised, marketed, sponsored, owned or exclusively controlled, as the case may be.
7. To deploy a technology-based measure to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which has been disabled on the computer resource of such SSMI. Further, SSMI shall ensure that appropriate human oversight is deployed for such technological measures.
8. SSMIs shall be required to have a physical contact address in India and publish it on their website, mobile application or both.
9. SSMI shall enable users, registered for their services from India or who use their services in India, to voluntarily verify their accounts by using any appropriate mechanism and upon such verification, a demonstrable and visible mark of verification shall be visible to all users of the service.
10. When the SSMI removes or disables access to information, it shall ensure the following:
11. Provide an explanation for the action being taken and the ground or reason for such action.
12. User shall have the adequate and reasonable opportunity to dispute the action and request for reinstatement of the information.
13. Ensure RGO maintains proper oversight over the mechanism of resolution of disputes.

While most of the compliances as required above are general ongoing compliances, the time bound compliances are as detailed in points a, b, c, d, g and h. Therefore, SSMIs are required to ensure that the additional due diligence has been duly observed by or before May 25, 2021.

#### Consequences of non-compliance

As per Rule 7 of the Rules, any non-compliance by the SSMI shall exempt them from safe harbour protection as provided under Section 79 of the Information Technology Act, 2000 ("Act"). However, the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and Indian Penal Code 1860. While the Rules fail to specify the exact consequences of non-compliance by the SSMIs, the consequences seem to

be wide-ranging and most likely to depend on the impact of such non-compliance by the intermediary.

#### Conclusion

SSMIs shall ensure compliance with points a, b and c at the earliest since there is no specific qualification required for such officers and the basic requirement is that they are an Indian resident and an employee of the SSMI. Also, on further analysis of the above, it is clear that the uproar related to the popular social media platforms may be rightly articulated, however, presumptions, claims of banning and criminal consequence may be slightly overreaching/exaggerated.

It shall be interesting to see how the authorities scrutinize the non-compliance and determine an adequate penalty for the same. Furthermore, WhatsApp, a messaging platform has challenged the Rules as unconstitutional on account of breach of privacy on the ground of information that this platform would be required to identify and provide under Rule 4(2).

The platform has alleged that such identification of originator would require them to break encryption for both originator and receivers, which is in contravention to their policy. It would be interesting to see if the specific clause would be modified by the central government to uphold the privacy of the individual originators of messages. In any case, the court may still uphold other provisions of the Rules and make the SSMIs liable for non-compliance irrespective of the ongoing case unless otherwise ordered.

- [1] [https://www.meity.gov.in/writereaddata/files/Intermediary\\_Guidelines\\_and\\_Digital\\_Media\\_Ethics\\_Code\\_Rules-2021.pdf](https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf)
- [2] As per Rule 2(1)(w) of the Rules, a social media intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;
- [3] Chief Compliance Officer shall mean key managerial personnel or such other senior employee of SSMI who is a resident of India.
- [4] Nodal contact person shall mean employee of SSMI other than a CCO, who is resident of India.
- [5] Resident Grievance Officer shall mean employee of SSMI, who is resident of India.

Contributed By - Sindhuja Kashyap, Senior Associate

King Stubb & Kasiva,

Advocates & Attorneys

[Click Here to Get in Touch](#)

[New Delhi](#) | [Mumbai](#) | [Bangalore](#) | [Chennai](#) | [Hyderabad](#) | [Kochi](#)

Tel: [+91 11 41032969](tel:+911141032969) | Email: [info@ksandk.com](mailto:info@ksandk.com)

**DISCLAIMER:** The article is intended for general guidance purpose only and is not intended to constitute, and should not be taken as legal advice. The readers are advised to consult competent professionals in their own judgment before acting on the basis of any information provided hereby.