



November 16, 2021

THE CENTRE'S FAQs ON THE 2021 IT RULES

AN ANALYSIS

argus
partners
SOLICITORS AND ADVOCATES

MUMBAI | DELHI | BENGALURU | KOLKATA | AHMEDABAD

Recently, in an attempt to “*explain the nuances*” of the due diligence obligations imposed upon [intermediaries](#) and the newly created class of ‘significant social media intermediaries’ (“[SSMIs](#)”) under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“[2021 IT Rules](#)”), the Ministry of Electronics and Information Technology (“[MeitY](#)”) released frequently asked questions (“[FAQs](#)”) on the 2021 IT Rules. The scope of the FAQs is limited to Part II of the 2021 IT Rules, relating to due diligence obligations by intermediaries and grievance redressal mechanism. MeitY has also clarified that the FAQs are not a legal document and do not amend/ alter the provisions of the 2021 IT Rules.

This piece provides an overview of key clarifications in the FAQs, examines certain assertions made by MeitY therein, and highlights some persisting ambiguities in the 2021 IT Rules.

Overview of Key Clarifications

1. **Definition of ‘social media intermediaries’ (“SMIs”)**: Rule 2(1)(w) of the 2021 IT Rules defines ‘SMIs’ as intermediaries “*which primarily or solely enables online interactions between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services*”. The FAQs additionally clarify that entities which only incidentally enable online interactions cannot be classified as SMIs¹. They also state that intermediaries whose primary purpose is enabling commercial or business-oriented transactions, providing access to internet or search-engine services, email services, or online storage services, etc. will not qualify as SMIs.
2. **Appointment of personnel by SSMIs**: According to the FAQs, the ‘chief compliance officer’ (“**CCO**”) and ‘nodal contact person’, who are required to be appointed by SSMIs under Rule 4(1) of the 2021 IT Rules, cannot be the same person. However, the roles of the ‘nodal contact person’ and ‘resident grievance officer’ may be discharged by the same individual².
3. **Manner of publishing periodic compliance reports**: The FAQs offer some flexibility to SSMIs, regarding publication of compliance reports under Rule 4(1)(d) of the 2021 IT Rules, by clarifying that: (a) physical copies of the reports need not be submitted to MeitY and SSMIs can simply publish these on their respective platforms; (b) no specific format needs to be adhered to for preparing the reports so long as the essential information prescribed under the rules is captured; and (c) SSMIs need not disclose granular data about each complaint received by them, as long as aggregated information about the complaints received by them -- such as nature of complaints and action taken -- is disclosed in the report³.
4. **Requirements for content removal orders**: Rule 3(1)(d), 2021 IT Rules creates a parallel mechanism for issuance of content removal directions to intermediaries, in addition to the pre-existing framework under [Section 69A](#) of the Information Technology Act, 2000 (“[IT Act](#)”) read with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (“[Blocking Rules](#)”). As per the FAQs, blocking directions under Rule 3(1)(d) should, typically: (a) specify URLs of the content at-issue; (b) the law being administered by the appropriate government/ agency issuing the direction and the specific law being violated by the content at-issue; and (c) justification and evidence⁴.
5. **Traceability and its impact on privacy**: MeitY claims that the intent behind the obligation to enable traceability of originator information, imposed under Rule 4(2), 2021 IT Rules upon SSMIs providing services primarily in the nature of messaging, is not to weaken encryption but to obtain “*registration details of the first Indian originator of the message*”. MeitY maintains

1 Response to Question 12, Pg. 9, FAQs

2 Response to Question 18, Pg. 14, FAQs

3 Response to Question 20, Pg. 15, FAQs

4 Response to Question 14, Pg. 11, FAQs

that the typical principle of detection is based on 'hash' value of unencrypted messages, wherein identical messages result in a common hash (message digest) irrespective of the encryption used by a messaging platform⁵. The FAQs allow SSMLs flexibility in coming up with alternative technological solutions to implement this principle⁶. MeitY also asserts that enabling traceability does not violate users' privacy due to the safeguards provided under Rule 4(2) for issuance of orders requiring SSMLs to enable traceability⁷.

6. **Penalties for users:** In the FAQs, MeitY has reiterated that intermediaries who are non-compliant with the provisions of the 2021 IT Rules would lose their immunity conferred under [Section 79](#), IT Act and consequently be liable for prosecution under applicable law(s). The FAQs inform that while no penalties are prescribed for individual users for non-compliance with the 2021 IT Rules, they can be prosecuted if the content circulated by them violates other laws like the Indian Penal Code, 1860, IT Act, Copyright Act, 1957, etc, in the manner prescribed under such laws.

MeitY's Assertions

1. **Process for promulgating the 2021 IT Rules was consultative:** The 2021 IT Rules supersede the erstwhile Information Technology (Intermediaries Guidelines) Rules, 2011 ("[2011 IT Rules](#)"). MeitY claims that the process for amending the 2011 IT Rules was consultative since public comments on new draft rules were invited on December 24, 2018. This claim is misleading since the version of the draft rules released for public comments in 2018 was entirely different from the one which MeitY ultimately promulgated in 2021. Notably, Part III of the 2021 IT Rules, regulating publishers of online curated content and news publishers, was conspicuously absent in the [2018 version](#) of the rules. Given this, the process adopted by MeitY appears to be less than transparent.
2. **The 2021 IT Rules respect the freedom of speech:** MeitY maintains that the 2021 IT Rules are consistent with the constitutional contours of the freedom of speech and expression. This bald assertion is wildly inaccurate for multiple reasons:
 - a. *Firstly*, the erstwhile content takedown regime for intermediaries elucidated by the Supreme Court in *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 ("[Shreya Singhal](#)"), required intermediaries to disable unlawful content from their platforms only on receipt of a Court order or Government notification under [Section 69A](#), IT Act. Further, any such Court order or Government notification had to strictly conform to the subject matters enumerated under [Article 19\(2\)](#) of the Constitution. Rule 3(1)(d), 2021 IT Rules, on the other hand, permits the issuance of takedown directions in respect of information/ content that is, *inter-alia*, "*prohibited under any law for the time being in force*", which far exceeds the scope of Article 19(2).
 - b. *Secondly*, in order to be able to fully exercise constitutionally guaranteed freedom of speech and expression, individuals may need to maintain their privacy, which is necessary to protect them from retaliation for expressing lawful but unpopular opinions. Rule 4(2), 2021 IT Rules disproportionately curtails the privacy of users using encrypted messaging services in India by requiring the SSMLs offering these services to enable traceability of originator information. This may cause users to self-censor their opinions, which would ultimately have a chilling effect on free speech.
3. **Enabling traceability of originator information does not undermine users' privacy:** In support of this claim, MeitY has referred to the safeguards for issuance of directions requiring

⁵ Response to Question 24, Pg. 18, FAQs

⁶ *Ibid*

⁷ Response to Question 6, Pg. 6, FAQs

certain SSMLs to enable traceability under Rule 4(2) which, *inter-alia*, require such SSMLs to trace originator information only upon receipt of authorised directions. However, to comply with these directions, such SSMLs may have to enable traceability for all messages exchanged on their platforms since it would be impossible for them to predict the scope of the Government's traceability request. This makes the traceability obligation under Rule 4(2) a disproportionate invasion into users' privacy, falling foul of the tests for legitimate curtailment of the fundamental right to privacy espoused by the Supreme Court in *K.S. Puttaswamy & Anr. v. Union of India & Ors.*, (2017) 10 SCC 1 ("[Puttaswamy I](#)").

Persisting Ambiguities under the 2021 IT Rules

1. **Procedural safeguards for content takedown requests:** The constitutionality of [Section 69A](#), IT Act was upheld in *Shreya Singhal* primarily due to the presence of procedural safeguards under the attendant Blocking Rules, which include providing a hearing to the content originator and the intermediary. By contrast, the parallel blocking mechanism created by Rule 3(1)(d) under [Section 79\(3\)\(b\)](#), IT Act, allows issuance of blocking directions for a wide array of content, without prescribing any procedural safeguards. This renders the blocking mechanism created by Rule 3(1)(d) arbitrary and unreasonable, and the FAQs fail to fill this conspicuous void in the 2021 IT Rules.
2. **Alternatives to enabling traceability:** The FAQs state that orders requiring SSMLs to enable traceability cannot be passed in case alternative measures for identifying first originator information are available. This principle is also codified in the second proviso of Rule 4(2), 2021 IT Rules and is consistent with the doctrine of proportionality adopted in *Puttaswamy I*. However, neither 2021 IT Rules nor the FAQs shed any light on what these alternative measures could be. Considering the adverse impact of traceability directions on users' privacy and free speech, it is imperative for the Government to clearly delineate what alternative measures it is willing to explore before issuance of such directions.
3. **Extent of liability of appointed personnel:** Rule 4(1)(a), 2021 IT Rules makes an SSML's CCO: (a) responsible for ensuring its compliance with the IT Act and attendant rules; and (b) liable in any proceedings arising out of its non-compliance with prescribed due diligence obligations. However, both the 2021 IT Rules and the FAQs are silent on the extent of the CCO's liability. It also remains unclear how Rule 4(1)(a) would reconcile with [Section 85](#), IT Act which already provides for attribution of liability for offences and contraventions committed by companies. Particularly, it isn't clear whether the exceptions protecting personnel of a company from liability under [Section 85](#), such as the absence of knowledge, would be available even to CCOs in any proceedings initiated against them.
4. **Preservation of user information/ records beyond prescribed periods:** Rule 3(1)(g), 2021 IT Rules requires intermediaries to preserve information and associated records for 180 days for investigation purposes, or such longer period as may be required by the court or by Government agencies who are lawfully authorised. The FAQs fail to clarify the grounds on which preservation for a period longer than 180 days may be required or the maximum (extended) period for which information/ data may have to be preserved by intermediaries.

Concluding Remarks

Although the FAQs provide some helpful clarifications, the scope of many critical obligations imposed upon intermediaries under the 2021 IT Rules remains unclear. Further, MeitY's attempt at defending the constitutionality of the 2021 IT Rules in the FAQs does not appear to be convincing. In light of their potential adverse impact on users' privacy and free speech, the constitutionality of certain provisions of the 2021 IT Rules such as Rule 3(1)(d) and Rule 4(2), remains questionable, despite MeitY's clarifications.

Even though the fate of the 2021 IT Rules is presently uncertain, given that several of its provisions have been [challenged](#) before multiple courts across India, MeitY's intention of determinedly enforcing these rules is abundantly clear from the FAQs. Intermediaries would, therefore, be well-advised to ensure compliance with the 2021 IT Rules to prevent the imposition of prescribed penalties and loss of safe-harbor.

This article has been written by Udit Mendiratta (Partner) and Dhruv Bhatnagar (Senior Associate).

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

**You can send us your comments at:
argusknowledgecentre@argus-p.com**

Mumbai | Delhi | Bengaluru | Kolkata | Ahmedabad

www.argus-p.com