Draft Intermediary Liability Rules, 2018: Docking at Unsafe Harbours?

1. Introduction

The Information Technology Act, 2000 ("**IT Act**") defines an "intermediary" to be a person[1] who receives, stores, transmits or provides any service with respect to an electronic record[2] on behalf of another. It is common knowledge that majority of general public internet is under control of behemoth intermediaries such as Google, Facebook, Twitter, WhatsApp, etc. In keeping with international best practices, section 79(1) of IT Act grants intermediaries immunity from any illegality perpetuated by virtue of third party information hosted by them. However, one of the pre-conditions for availing this immunity is the intermediaries ensuring requisite due-diligence in accordance with the Information Technology (Intermediaries Guidelines) Rules, 2011 ("**2011 Rules**"). On December 24, 2018, the Ministry of Electronics & IT ("**Meity**") released the Draft Intermediary Liability Rules, 2018 ("**Draft Rules**") with the intent of substituting the 2011 Rules. The purpose of these Draft Rules is to curb misuse of social media by anti-social elements that spread fake news, recruit terrorists, spread disharmony and incite violence.[3]

This newsletter seeks to critically examine key rules of the Draft Rules, comprehend implications for intermediaries and evaluate effectiveness qua stated objectives.

2. Interception, Monitoring and Decryption of Information

Rule 3(5) of the Draft Rules prescribes that within 72 hours of receiving a *lawful order*, an intermediary shall provide information or assistance as requested by a government agency in matters concerning: (i) security of the state, (ii) cyber-security, (iii) investigation, detection, prosecution or prevention of offence(s), (iv) tracing out of originator of information required by legally authorized government agencies, and (v) those connected with or incidental to (i) to (iii). In our view, rule 3(5) presents the legal and practical issues below.

2.1 What Constitutes a "Lawful Order"?

Rule 3(5) states that intermediaries' obligation to provide requested information or assistance triggers on receipt of a lawful order. The Draft Rules do not indicate whether such lawful order is a judicial or administrative order. We can presume that it shall include an administrative order on the basis of the:

- IT (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("**Cyber-Security Monitoring Rules**") wherein only Deputy Secretaries of government agencies who have been authorized by Secretary, Government of India ("**GoI**"), Department of Information Technology, can send requisition to intermediaries for disclosure of information. This requisition must relate to cyber-security purposes as enumerated under rule 3(2) of Cyber-Security Monitoring Rules.

[1] Person includes individuals and body corporates such as companies, limited liability partnerships, etc
[2] Electronic record means data, image, or sound, stored, received or sent in an electronic form
[3] Draft IT Rules issued for public consultation, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770 (Last accessed on February 13, 2019)

- IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**Interception Rules**"), wherein interception, monitoring, or decryption of information stored in a computer resource is permitted only pursuant to an order of a (i) Secretary, Ministry of Home Affairs ("**MHA**"), in case of Central Government; or (ii) Secretary in charge of the Home Department, in case of State Government or Union Territory. Under Interception Rules, interception, monitoring or decryption of information can occur only if it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states, public order or for preventing incitement to the commission of any cognizable offence or investigation of an offence ("**Lawful Grounds**").

- The MHA has through section 69(1) of IT Act read with rule 4 of Interception Rules authorized 10 government agencies to conduct such interception, monitoring or decryption of any information stored or transmitted in a computer resource if the request is basis any of the foregoing Lawful Grounds.[4] Therefore, it seems that a requisition from such government agencies shall constitute a lawful order.

2.2 Vagaries of Draft Rule 3(5)

Rule 3(5) does not make reference to Cyber-Security Monitoring Rules, or Interception Rules as forming basis of a lawful order. Consequently, there may be a situation where government agencies submit requests to intermediaries for procuring information or assistance without proper authorization. If the intermediaries in turn comply with such requests in a bid to retain their immunity under section 79(1) of IT Act, they would violate Cyber-Security Monitoring Rules and Interception Rules, thereby exposing them to liability for allowing unauthorized incursions.[5] Further, some government agencies may seek to evade safeguards built in the Interception Rules and Cyber-Security Monitoring Rules by making use of this ambiguity in rule 3(5). Such unauthorized and illegal interception, monitoring or decryption would be an incursion against the right to privacy of originators of information, which would fail the three-fold test of legality, necessity, and proportionality laid down by the Supreme Court of India in *Puttuswamy*.[6]

3. Blocking Order

Rule 3(8) of the Draft Rules requires an intermediary to remove or disable access to unlawful acts relatable to Article 19(2) of the Constitution of India within 24 hours of receiving a (i) court order, or (ii) notification by the appropriate government or its agency. We foresee the implementation of rule 3(8) to lead to legal and practical difficulties below.

3.1 Absence of Procedural Safeguards

The IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("**Blocking Rules**") read with section 69A of IT Act provide the extant framework for blocking access to information consequent to an administrative action. Under the Blocking

[4] S.O. 6227(E) dated December 20, 2018
[5] Rule 21 of Interception Rules and Rule 6 of Cyber-Security Monitoring Rules.
[6] Reported as (2017) 10 SCC 1

Rules, Central Government appoints a "Designated Officer", who shall not be below the rank of a Joint Secretary. If a person requests blocking of information, such request must first be made to a nodal officer of the concerned organization. Upon satisfaction of the nodal officer, the blocking request is forwarded to the Designated Officer. Thereafter, the request is examined by a committee comprised of the Designated Officer and Joint Secretary level representatives from Ministry of Law and Justice, MHA, Ministry of Information and Broadcasting and the Indian Computer Emergency Response Team. A reasoned blocking order is passed after giving an opportunity to the originator of information or the intermediary to represent their case. Such order is amenable to appeal before the High Court under Article 226 of the Constitution of India. In contrast, rule 3(8) does not offer any such procedural safeguards of reasoned orders or pre-decisional hearings to originator of information or intermediaries. If rule 3(8) is enacted as-is, it would by-pass the procedural safeguards enshrined in the Blocking Rules and be contrary to the rules of natural justice.

4. Automated Blocking

Rule 3(9) of the Draft Rules mandates intermediaries to deploy technology based automated tools or mechanisms, with appropriate controls, for proactively identifying and blocking public access to unlawful information. Implementation of rule 3(9) is fraught with the following complications.

4.1 Contradictory Obligations

Section 79(2)(b)(iii) of the IT Act stipulates that an intermediary will not enjoy immunity under section 79(1) if it *selects* or *modifies* the information contained in a transmission. By employing technology based automated tools, an intermediary would engage in censorship and shall therefore select information which it chooses to transmit or modify information to ensure that unlawful information is not transmitted. It is noteworthy that in complying with rule 3(9), the intermediary shall violate section 79(2)(b)(iii) and lose its immunity under section 79(1) of IT Act. This anomaly must be resolved before the Draft Rules are finalized.

4.2 The Shreya Singhal Verdict

Rule 3(4) of the 2011 Rules had provided intermediaries the power to exercise discretion in blocking content. However, this power was made "*non-operative*" by the Supreme Court in Shreya Singhal vs. Union of India[7]. By mandating intermediaries to pro-actively identify and block information, rule 3(9) of Draft Rules runs contrary to the diktat of the Supreme Court of India.

4.3 Automated Tools Incapable of Ascertaining Legality

Improved functioning of automated tools requires huge volumes of data. Datasets may themselves possess bias, because of which, automated tools are prone to commit errors. Further, determination of what constitutes lawful information and what doesn't is a nuanced and complex process. Differing contexts provide different meanings to the same expression. For instance, an algorithm used by Twitter to weed out "*hate speech*" has been known to wrongfully remove

[7] Reported as (2015) 5 SCC 1

harmless statements because it could not identify the context in which the statements were made.[8] While instances of child pornography, nudity, and sexual abuse are easy to detect and remove, instances of political speech are not. Given the complexities of the task at hand, human intervention is necessary for accurate analysis of an information's legality.

4.4 No Redressal Mechanism

Auto-blocking by automated technologies does not disclose precise reasons for blocking of information. This results in denial of an adequate grievance redressal mechanism as an aggrieved person cannot assail the reasons for auto-blocking. Also, rule 3(9) does not prescribe means wherein wrongfully blocked content can be restored. Therefore, auto-blocking would occur sans a hearing. Additionally, intermediaries who want to comply with Draft Rules for retaining their immunity may engage in over-cautious blocking. Without an adequate redressal mechanism, auto-blocking will have an obvious impact on freedom of speech and expression.

5. Incorporation of an Indian Company

Rule 3(7) of the Draft Rules obligates intermediaries with more than 50 lakh (5 million) Indian users, or those specifically notified by the GoI to: (i) be incorporated under Companies Act, 2013, (ii) have a permanent registered office in India and (iii) appoint a nodal contact person for 24*7 coordination with law enforcement agencies. Needless to say, implementation of this rule would cause the following difficulties.

5.1 Fifty Lakh Users

Rule 2(l) of Draft Rules defines the term User to mean "any person who accesses or avails any computer resource of intermediary" for the purpose of "hosting, publishing, sharing, transacting, displaying or uploading information or views". Therefore, any person who accesses an intermediary's computer resource, even once, shall become a User. India has 50 crore (500 million) internet users.[9] Any mildly popular foreign intermediary could attract 50 lakh Indian users (1% of India's total internet users) to utilize their computer resources. Accordingly, local incorporation requirements shall trigger for a majority of foreign intermediaries. This may cause foreign intermediaries to refrain from providing their services in India, consequently impairing the Indian internet user experience.

5.2 Compliance Costs

Under rule 3(7) of Draft Rules, it is not enough for a foreign intermediary to establish a Project or Branch Office in India. The foreign intermediary shall necessarily have to incorporate an Indian company and observe compliances under Companies Act, 2013. Apart from increased compliance costs, the Indian company will be taxed in India. The resultant taxation and corporate compliances are an additional burden on foreign intermediaries.

---

[8] Yeung, Karen, Algorithmic Regulation: A Critical Interrogation (May 23, 2017). TLI Think! Paper 62/2017; Regulation & Governance, Forthcoming; King's College London Law School Research Paper No. 2017-27. Available at SSRN: https://ssrn.com/abstract=2972505, (last accessed on February 13, 2019)

[9] Internet Usage in India, Available at https://www.statista.com/topics/2157/internet-usage-in-india/, (last accessed on February 14, 2019)

5.3 Recommendation

The intent behind rule 3(7) is to ensure that foreign intermediaries cooperate with government agencies. Interception Rules and Blocking Rules ensure compliance from foreign intermediaries by mandating them to appoint a nodal officer for handling requisitions.[10] Similarly, Draft Rules can limit the requirement to appointment of a nodal officer only. Compliance with such requirement can be ensured through penal provisions, which after an impartial hearing, may include blocking orders against the intermediary itself. Such a mechanism would achieve the objectives of the Draft Rules and ensure that foreign intermediaries are not overburdened with onerous compliances.

6. Conclusion

While the intent behind the Draft Rules is laudable, they need streamlining, especially in context of the existing legal framework. It is documented that lesser compliance requirements would increase expected profit for successful Indian start-up intermediaries by 5%.[11] If the Draft Rules are given effect in their present form, it would disrupt India's intermediary start-ups and affect foreign intermediaries. Any regulation of intermediaries must be through a consultative process by recognizing that intermediaries exist and operate in diverse spheres. Due-diligence obligations for social-media sites, e-commerce sites, internet service providers, small and large intermediaries etc., must be commensurate with the purpose that they serve and without disrupting their overall functionality. Unfortunately, the Draft Rules treat intermediaries as a homogeneous unit, imposing uniform onerous obligations across the board. Such blanket approach is unsustainable and discourages culture of innovation. Meity will be best advised to revise the Draft Rules in order to keep them industry-friendly and coherent with the existing legal regime.

Author
Nikhil Issar

[10] Rule 13 of Interception Rules and Rule 14 of Blocking Rules
[11] Oxera, February 2015, "The economic impact of safe harbours on Internet intermediary start-ups". pp.2, available at https://www.oxera.com/wp-content/uploads/2018/07/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf, (last accessed on February 14, 2019).