THE DRAFT INFORMATION TECHNOLOGY INTERMEDIARIES GUIDELINES (AMENDMENT) RULES, 2018

1. INTRODUCTION

The Ministry of Electronics and Information Technology (the "**MEITY**") released the draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018 (the "**Draft Rules**") on December 24, 2018. The Draft Rules intend to supersede the present Information Technology Intermediaries Guidelines Rules, 2011 (the "**Current Rules**"), which are currently in force.

Although the Draft Rules have been framed with the intention of curbing the misuse of online intermediaries, protecting the interest of online users and making intermediaries more accountable, we believe that there are certain *lacunae* and concerns, which need to be addressed.

The MEITY has invited public comments on the Draft Rules and we set out our key observations and recommendations below.

2. PROVISIONS OF THE DRAFT RULES

In the context of the Draft Rules, we would point out that an *intermediary* is defined to mean any person who on behalf of another person receives, stores or transmits records or provides any service with respect to such records and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, e-payment sites, e-auction sites, e-market places and cyber cafes[1].

A *user* is defined to mean any person who access or avails any computer resource of intermediary for the purpose of hosting, publishing, sharing uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary"[2].

We would also point out that *critical information structure* (the "**CII**") is defined to mean the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.[3]

2.1. Requirement to inform Users

Pursuant to Rule 3 (2) of the The Draft Rules, intermediaries are required to inform their users against hosting any material that may threaten the CII or public health or safety.

[1] Section 2(1) (w), Information Technology Act, 2000.

[2] Rule 2(1) (l), Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018.

[3] Rule 2(1) (e), Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018.

Our understanding is that Rule 3 (2) (k) of the Draft Rules requires the intermediary to display rules informing users not to host or publish any information that *inter alia* threatens CII.[4]

However, there are practical challenges associated with this. Users and intermediaries, at the time of uploading content, may not always be aware whether the content is likely to threaten the CII. Similarly, for any user to prove that information posted on an intermediaries' platform can potentially threaten CII will be challenging, and it will be difficult to obtain a court order to request the intermediary to take-down such content from its platform.

Intermediaries will also not be in a position to deploy technology based automated tools or other control mechanisms to pro-actively identify content that is likely to threaten CII and removing or otherwise disabling such content under Rule 3(9) of the Draft Rules.

We hence are of the opinion that the Draft Rules should:

(a) either objectively elaborate on the nature of information or content that is perceived as a threat to CII; or

(b) prescribe standards to determine whether any content is likely to threaten CII.

Rule 3 (2) (j) has been added in the Draft Rules and requires the intermediary to display rules informing users not to host or publish any information that *inter alia* threatens public health and safety.

This new requirement is very broadly categorized and leaves the nature of content that should not be posted online, open to the interpretation of the user. In *re Shreya Singhal v. Union of India*[5], the Supreme Court, citing *Grayned v. City of Rockford*, noted that the law on the subject of *vagueness* is clearly stated, highlighting that:

"*It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. Third, but related, where a vague statute 'abut(s) upon sensitive areas of basic First Amendment freedoms, it 'operates to inhibit the exercise of (those) freedoms.' Uncertain meanings inevitably lead citizens to "steer far wider of the unlawful zone'… than if the boundaries of the forbidden areas were clearly marked.' (At page 227-228)*".

[4] This inclusion in the list of content that cannot be hosted or displayed by users on an intermediaries' platform appears to be with the objective of curbing any potential attack on or breach of computer resource that could threaten the national security, public safety or economy.

[5] AIR 2015 SC 1523.

Therefore, it might be advisable to clarify in Rule 3 (2) (j) the exact nature of information that cannot be posted, by giving guidelines on restrictions under applicable law that applies in the context of the advertisement and media sector.

Similarly, the provision under Rule 3 (2) (i) of the Draft Rules is very broad and lacks clear boundaries, leaving open for interpretation as to what content should not be posted online.

Rule 3(2) (i) of the Draft Rules includes information that "*threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states, or public order, or causes incitement to the commission of cognizable offence or prevents investigation of any offence or is insulting any other nation.*"

In light of *re Shreya Singhal v. Union of India*,[6] Rule 3 (2) (i) of the Draft Rules should be streamlined in accordance with the reasonable restrictions on the freedom of speech under Article 19(2) of the Indian Constitution.

2.2. Notification of consequences of non compliance

Rule 3 (4) of the Draft Rules mandates intermediaries to send a monthly notification to its users reminding them about the consequences of non-compliance with the provisions of the rules and regulations, user agreement and privacy policy.[7]

In our view, there are 2 (two) important points to note here.

Firstly, the proposed requirement mandates a monthly notification to be sent *irrespective* of whether there are any changes to the privacy policy or the user agreement. This essentially means that intermediaries will need to set-up an automated notification for its users on a monthly basis.

From a user-experience perspective, a repetitive reminder on a monthly basis will, practically speaking, be ignored or deleted without being read. It may also create a deterrent for current and potential users from accessing or using the intermediary's computer resources, which may cause financial losses to intermediaries. Further, in future, if there is any amendment to the terms of use or privacy policy, this is likely to get lost in the frequent periodic automated notification to the users. Therefore, the intention of the proposal may not be effectively achieved. Instead, changing the periodicity of the notification may be more effective.

Secondly, a requirement of this nature poses a challenge for small scale start up intermediaries or intermediaries having a smaller user-base. This requirement will increase the financial burden for compliance. Therefore, in our view, it is important to impose such periodic compliance only on certain categories of the intermediaries, depending upon its annual revenue or number of users and such other considerations. The uniform imposition of compliance requirements will, rather ironically, create the opposite effect of what is intended; and an uneven playing field, which is against the principle of fair market economy, is the likely outcome.

[6] AIR 2015 SC 1523

[7] Rule 3(4), Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018.

2.3. The requirement to provide information

Rule 3 (5) of the Draft Rules incorporates several procedural changes. Generally, the requirement for providing assistance and information to government agencies in a time bound manner is a welcome measure as it serves broader public policy interests.

We set out our further specific comments in relation to Rule 3 (5) of the Draft Rules in the table below:

Changes to the Current Rules	INDUSLAW Comments
An intermediary is required to provide the information requested under a lawful order, within 72 (seventy two) hours from the communication.	No comments.
The intermediary is required to provide such information or assistance as asked for by any government agency or assistance for security of the State or cyber security; or investigation or detection or prosecution or prevention of offences; protective or cyber security and matters connected with or incidental thereto.	The provision to: '*provide such information or assistance as asked for by any government agency*' is too broad in nature and seems to be a standalone provision, giving the government agency wide powers to request any sort of information or assistance by way of a lawful order. The nature of information or assistance that a government agency can seek under this provision, is not qualified by specified grounds such as '*assistance for security of the State, cyber security*.' The Current Rules clearly stipulated the circumstances under which such a request could be made on an intermediary, through a lawful order. However, the proposed Rule 3 (5) has a very wide ambit. It appears to provide the appropriate government or its agency the right to: fish for information thereby exposing the private information of citizens to scrutiny; and draw on the technology expertise of the intermediary to help investigate a matter. The nature and extent of the assistance that can be requested from an intermediary is not clear. The Draft Rules should limit the nature of information that can be requested by a Government agency to the grounds specified in

Changes to the Current Rules	INDUSLAW Comments
	Rule 3(5) and the lawful order should specify the nature and extent of assistance that is expected from the intermediary. *Drafting Point:* On who can make the request, when the proposed Rule 3 (5) is read with Rule 3 (8) it appears that the intention is to restrict the right provided under Rule 3 (5) to a court order or a notice received from the appropriate government or its agency. However, this understanding is not clear from the standalone reading of the proposed Rule 3 (5) of the Draft Rules. The Current Rules gave this authority only to government agencies authorized with investigative, protective and cyber security activity. We would recommend that Rule 3 (5) be revised to clarify that the right vests with the appropriate government agencies, which are granted a lawful order.
Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance.	This requirement needs the request to state the purpose of the request. The request should also state the exact information that is needed from the intermediary, to enable the intermediary to strike a balance between complying with the lawful order while safeguarding the right to privacy of its users.
The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorized.	We understand that this provision was introduced pursuant to the government's commendable efforts to cease and curb the nuisance of fake news. The barbaric and distressing mob lynching caused due to recent social media messages and other social media news is indeed a menace to society. To that end this measure is commendable. However, in the present form, the requirement is not qualified by any requirement and appears to

Changes to the Current Rules	INDUSLAW Comments
	provide an omnibus right to demand the tracing of any information. This effectively means that: the security provided by end-to-end encryption from a data privacy standpoint is diluted if this provision is enabled, which means that the data from a technology standpoint will be exposed to higher cyber security risk; there is potential for the breach of the fundamental right of speech of Indian citizens, and there is an enhanced onus on intermediaries to have accurate and updated identification records of each user of the platform, in a manner that can be shared with those relevant government agencies. Therefore, in light of the above, we suggest that the above requirement to trace out the originator of information should be specifically limited to the information and details listed under Rule 3 (2) of the Draft Rules. Further, it is should clarified that intermediaries should be liable to trace out such information, only upon obtaining a lawful order, and not otherwise.

2.4. **On the ground requirements**

Under the Draft Rules, it has been stated that an intermediary who has more than 5 million (50 (fifty) lakh) users in India or an intermediary who has been specifically listed pursuant to a notification of the Central Government should:

(a) be a company incorporated under the company law of India;

(b) have a permanent registered office in India with a physical address; and

(c) appoint a nodal person in India to act as the point of contact and an alternate senior designated functionary, who would be responsible at all times to coordinate with the law enforcement agencies to ensure the intermediary complies with their order or requisitions, as the case may be.[8]

In our view, the requirement for being registered as a company in India and having a permanent registered office in India could prove to be financially as well as logistically burdensome for certain intermediaries, especially small scale start up intermediaries having more than 5 million (50 (fifty) lakh) users.

In addition, it might also deter foreign intermediaries from doing business in India, as there will be additional statutory compliances and costs in doing so.

Although the revisions in the Draft Rules make it easier for the Indian courts to exercise jurisdiction over intermediaries situated outside India, we would point out that the Information Technology Act, 2000 (the "**IT Act**") *already* provides for cross border jurisdiction.

The IT Act applies to *any* offence committed outside India as long as it involves a Computer[9] or a Computer System[10] or a Computer Network[11] located *within* India. Further, the concern in relation to protecting the personal data collected by intermediaries with over 5 million (50 (fifty) lakh) users will be addressed to a large extent under the provisions of the Personal Data Protection Bill, 2018, once it is enacted into law, given its proposed extra-territorial scope and application.

Arguably, the requirement of a permanent registered office in India with a physical address may place a higher burden on intermediaries than the requirements under the Personal Data Protection Bill, 2018, which has been severely criticized for its provisions with respect to data localization.

With regard to the appointment of a nodal person in India, it has not been specified as to which kind of 'orders or requisitions' of the law enforcement bodies the nodal person is required to ensure compliance of, and under which law or rules and therefore, there is a need to bring in clarity in the language of the provision. There should be more clarity on the fact that the nodal person should ensure compliances of orders or requisitions of certain kinds, for example, orders relating to unlawful acts relating to Article 19 (2) of the Indian Constitution.

---

[8] Rule 3(7), Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018

[9] Under the IT Act-computer means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

[10] Under the IT Act-computer system means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

[11] Under the IT Act-computer network means the inter-connection of one or more computers or computer systems through- (i) the use of satellite, microwave, terrestrial line, wireless or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers or communicated device whether or not the inter-connection is continuously maintained

2.5. Removing or disabling content

Rule 3(8) And Rule 3(9) of the Draft Rules require that an intermediary shall, upon receiving actual knowledge in the form of court order, or on being notified by the Government or its agency, no later than 24 (twenty four) hours, remove or disable access to material which may be lawfully restricted under Article 19(2) of the Indian Constitution, including the interests of the sovereignty and integrity of India, the security of the nation, friendly relations with other countries, public order, decency and morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource, without impairing the evidence of such content.

The requirtments under the Draft Rules are compared with the Current Rules in the table below, along with our further thoughts.

Current Rules	Draft Rules	INDUSLAW Comments
The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information….	The intermediary upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency under section 79 (3) (b) of IT Act…	The Draft Rules proposes to codify the evolving jurisprudence on this subject. Hence, in accordance with the interpretation of the Indian judiciary of the safe harbour principles in Section 79 of the IT Act and the Current Rules, the Draft Rules impose an obligation on intermediaries to take action only upon receiving a court order or a notification from a regulatory authority. This safeguards intermediaries from excessive responsibility or liability. The requirement for taking down content by an intermediary only on receiving a court order is commendable, protecting the interest of both the intermediary and its users, since it is not practical for an intermediary to examine *all* uploaded content to evaluate whether it is liable to remove or disable access.
Under the Current Rules, the intermediary can be requested to take down information that is in contravention of Rule 3(2).	Under the Draft Rules, the request to take down can be made pursuant to a court order or by notification from appropriate Government or its agency relation to unlawful acts relatable to Article 19(2) of the Indian Constitution.	While this change is in keeping with the freedom of speech and the reasonable restrictions on this freedom under the Indian Constitution, the grounds for take down are not very clear. The Current Rules recognized a *take-down* request for content that was invasive of another's privacy, racially or ethnically

Current Rules	Draft Rules	INDUSLAW Comments
		objectionable, or which was generally unlawful in any manner. It appears that these grounds are still available to obtain a court order and request a *take-down* of content. However, the Government notification under Rule 3(8) will be for specific unlawful acts in relation to Article 19(2) of the Indian Constitution. In our view, there is a need to clarify that the Draft Rules require an intermediary to take down content in violation of Rule 3(2), upon receiving a court order, to ensure that the Draft Rules are not perceived as limiting the grounds to approach the court for a *take-down* order under Article 19(2) of the Indian Constitution.
Rule 3(4) of the Current Rules also covered a request for take down of content that infringed intellectual property.	The Draft Rules do not seem to cover this.	This is a departure from the existing jurisprudence. The Indian judiciary has repeatedly distinguished *take-down* requests for *intellectual property infringement* from other *take-down* requests, and held that for online IP violations, a notice directed to intermediaries regarding the actual infringing content along with details of the IP rights in question is sufficient to warrant removal of the infringing content. There is no requirement of a court or executive order for actual knowledge to be constituted under Section 79 (3) (b) of the IT Act. Therefore, in light of the above, it is important that intermediaries should have the power to address *take-down* requests for intellectual property infringement, in the absence of a court or executive order, unless the intermediary reasonably and in *good faith* believes that they are not in a position to assess actual intellectual property infringement from the *take-down*

Current Rules	Draft Rules	INDUSLAW Comments
		notice; and would require an court or executive order to take down the content.
The duration to respond was 36 (thirty six) hours.	The response time has been brought down to 24 (twenty four) hours.	This change to the Draft Rules is fine, given the grave implications of the intermediary not acting in a timely manner.
The time period for preservation of records was 90 (ninety) days for investigation purposes.	The time period for preservation of records has been increased to 180 (one hundred and eighty) days, or for such longer period as may be required by the court or by government agencies who are lawfully authorized.	This change is fine, however, it will mean that intermediaries will have to incur additional costs in preserving and safeguarding user data and records for a longer period, to ensure that there is no misuse or unauthorized access to data during this period.

It should be noted that under the provisions of the Draft Rules, an intermediary is under an obligation to deploy technology based automated tools or such appropriate mechanisms, having appropriate controls, to proactively identify, remove or disable public access to unlawful information or content.[12]

The requirement to install automated tools has been previously discussed under the Supreme Court's judgment in *Sabu Mathew George vs. Union of India*[13]. However, under the Draft Rules, there is no clarity on the manner in which these automated tools will identify unlawful information or content. The Rules fail to define the term '*unlawful information or content*', the absence of which will create ambiguity and inconsistency amongst the intermediaries.

Therefore, in our view, the use of such automated tools may arbitrarily, excessively and disproportionately *pre-censor* information and content, having a detrimental effect on an individual's right to free speech, defeating the intention behind the Supreme Court's judgment in *Shreya Singhal vs. Union of India*[14]

While we acknowledge the need to set out certain standards and specifications with respect to the use of automated tools to ensure uniformity in the digital space, the risk of over-censorship is still a danger.

[12] Rule 3(9), Draft Information Technology (Intermediary Guidelines (Amendments) Rules, 2018.

[13] 2017(1) RC R (Civil) 175.

[14] 2015X AD (S.C.) 586.

Authors: Suneeth Katarki | Namita Viswanath | Aditi Verma Thakur | Ashi Bhat | Ivana Chatterjee

Date: February 12, 2019

Practice Areas: Technology Media & Telecommunications | Government & Regulatory

DISCLAIMER