15 January 2020

Shri Ravi Shankar Prasad
Union Minister for Law and Justice, Communications and Electronics and Information Technology,
Government of India

Cc: Shri Ajay Prakash Sawhney
Secretary, Ministry of Electronics and Information Technology (MeitY)
Government of India

Subject: Recommendations on concerns regarding the Information Technology [Intermediary Guidelines (Amendment)] Rules under the Information Technology Act

Honorable Minister Prasad,

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Electronics and Information Technology (MeitY) and Government of India, for leading the drafting process of "Information Technology [Intermediary Guidelines (Amendment)] Rules 2018 **(Draft Rules)**

AIC is an industry association comprised of leading Internet and technology companies and is committed to safe and open Internet. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter, Booking.com, Yahoo (Verizon Media).

We commend that the Government of India is reviewing the Intermediary Guidelines to align it with judicial precedents and global practices. However, certain key provisions of the Draft Rules fail to address crucial issues such as safe harbour protection available to intermediaries, privacy rights, and right to free speech of users. With India at the forefront of the global technology ecosystem, we find that this discussion around Draft Rules is timely and imperative. On behalf of the industry experts and our members, we write to you to express concerns around the effects of the proposed amendments to the Draft Rules. The proposed amendments create several concerns, many of which are raised in AIC's earlier submissions.

We also strongly urge the Indian government to share the most recent amended draft rules to ensure transparency in the proposals with industry stakeholders. We understand that imposing the obligations proposed in new rules would place a tremendous, and in numerous cases burden on many online intermediaries - especially new and emerging start-up community.

Accordingly, please find appended to this letter detailed comments and recommendations, which we would like Ministry of Electronics and Information Technology to consider as they prepare to publish the revised version of the proposed amendments to the Information Technology (Intermediaries Guidelines) Rules, and to protect India's Internet economy and users, by supporting the use of end-to-end encryption.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Thank you for your time and consideration. Importantly, we look forward to offer our inputs and insights directly through meetings and discussions.

Sincerely,

Jeff Paine | Managing Director
Asia Internet Coalition (AIC)

DETAILED COMMENTS AND RECOMMENDATIONS REGULATION OF INTERMEDIARIES

I. REGULATION OF INTERMEDIARIES

a. While regulatory regimes in Asia have been concerned over determining the nature of online content and whom to hold liable for such content, several countries have imposed liability on intermediaries for content uploaded on their platforms on the grounds of national security. The majority of ASEAN countries such as Thailand, Myanmar, Cambodia, Vietnam and the Philippines have enacted cybersecurity measures to enforce additional penalties on intermediaries that do not screen content. However, such measures have resulted in significant restrictions being placed on civil liberties owing to pre-censorship. Specifically, in India, pre-screening of content by an intermediary is not permitted under the law and principles upheld by the Indian judiciary in light of the constitutional guarantees of the freedom of speech and expression available to Indian citizens.

b. Legal regimes worldwide recognize that intermediaries must be given protection from legal liability that may arise due to any unlawful content posted by their users. To support this stance, countries across the world, and India provide intermediaries 'safe harbour protection' from any user generated or third-party content made available on its platforms. *Safe harbour protection refers to a legal exemption or immunity that allow intermediaries to host content as a neutral platform without being liable for any such content.* As an example of the tangible impact limiting safe harbour protections can have on an economy, a 2017 study by NERA Economic Consulting found that weakening intermediary liability safe harbour protections would cause the US economy to lose 4.25 million jobs and US$440 billion in GDP every 10 years – affecting SMEs the most.[1]

c. In this context, it is relevant to note that countries across the world draw from the *Manila Principles* for this purpose, which sets out standards and best practices for countries to follow, while structuring their regulations for intermediary liability. These include:

1. Intermediaries should be shielded from liability for third-party content uploaded on their platform;
2. Content must not be restricted unless there is an order by a competent judicial authority;
3. Requests for restriction of content must be clear, unambiguous, and follow due process;
4. Laws and content restriction orders must comply with the tests of legality, necessity, and proportionality; and
5. Transparency and accountability must be incorporated into the laws.

According to Article 19 of the Universal Declaration of Human Rights, free expression online is a human right. It states: "Everyone has the right to freedom of opinion and expression; this right includes *freedom to hold opinions without interference* and to seek, receive and impart information and ideas *through any media and regardless of frontiers*."

The free flow of information is essential to creativity and innovation, and contributes to the economic growth for countries and companies alike. The Internet provides services that

[1] http://internetassociation.org/wp-content/uploads/2017/06/NERA-Intermediary-Liability-Two-Pager.pdf

empower users to create, share and receive information like never before – giving them more choice, power, and opportunity.

As an example, the United Nations' Joint Declaration on Freedom of Expression on the Internet recognizes the critical role of reasonable limits on liability, stating that "*intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression*."

d. In India, as per Section 79 of the Information Technology Act, 2000 (*IT Act*), an intermediary cannot be held liable for any third-party content made available or hosted by it, so long as it fulfils the following conditions:

1. The intermediary's role is limited to providing access to communication system over which content made available by third-parties is transmitted or temporarily stored or hosted; or
2. The intermediary does not initiate the transmission, select the receiver of the transmission or modify the information contained in the transmission with respect to exchange of electronic records or any service operating on it; and
3. The intermediary observes due diligence while discharging its duties under the IT Act and also observes any such other guidelines as the Central Government may prescribe.

e. In this regard, the Central Government issued the Information Technology (Intermediary Guidelines) Rules, 2011 (*Intermediary Rules*) outlining detailed procedures for the intermediaries to observe due diligence and guidelines under Section 79 of the IT Act. These procedures were revisited in the case of *Shreya Singhal* v. *Union of India* (*Shreya Singhal case*), where the Supreme Court (*SC*) ruled that the application of Section 79 of the IT Act and the Intermediary Rules must be in harmony with the requirements of due process.

In the Shreya Singhal case, Section 66A of the IT Act was struck down by the SC for being vague and arbitrary and hence not a reasonable restriction on the constitutionally guaranteed right to freedom of speech and expression. The SC ruled that Section 66A of the IT Act was not only overbroad but also consisted of ambiguous terms such as "grossly offensive", "menacing", "false", and "causing annoyance, inconvenience, danger". The SC also read down any obligation on intermediaries to pre-screen any content uploaded on their platforms. Accordingly, intermediaries are now required to remove or disable access to content *only* upon receiving actual knowledge of a court order or notification by the appropriate government / agency. Further, any request for taking down of content must be within the realms of the reasonable restriction grounds identified in the Constitution of India, 1950 (*Constitution*).

f. In the light of the above-mentioned international standards and national judicial precedents, AIC is of the view that the Draft Rules are likely to fall short of the extant legal jurisprudence in India and global standards and practices related to the regulation of intermediaries. In addition to interfering with the fundamental rights of freedom of speech and expression, and right to privacy as guaranteed under the Constitution, the Draft Rules impose burdensome obligations on the intermediaries, non-compliance of which is likely to result in intermediaries not being able to enjoy the safe harbour protections, provided under the IT Act.

RECOMMENDATIONS ON REGULATION OF INTERMEDIARIES

1. Public health advertising restrictions

The Intermediary Rules mandate intermediaries to inform its users not to upload content of several categories including content that infringes any patent, trademark, copyright or other proprietary rights; harms minors in any way; is obscene, pornographic, pedophilic, libelous, defamatory, etc. The Draft Rules have amended this provision to include two new categories of content, namely, content that *threatens*:

- public health or safety; including content that promotes cigarettes and other tobacco products, or consumption of intoxicants including alcohol and electronic nicotine delivery system; and
- critical information infrastructure in the country.

Since the Draft Rules do not provide any guidance for how any content may 'threaten' public safety, health or critical information infrastructure, the provision may be open to several interpretations, which in turn, may lead to unreasonable application of this provision in instances where online content may refer to the above-mentioned categories. Further, there is no definition of 'public health or safety' either under the IT Act or for that reason any statute per se.

Since the *Shreya Singhal* case specifically observes that any restriction on free speech and expression must be within the contours of the Constitution, this provision can potentially amount to an unreasonable restriction on the freedom of speech and expression guaranteed under the Constitution.

Advertising restrictions should be kept separate from restrictions on other forms of content. Since intermediaries are merely a neutral platform on which parties interact, it may not be appropriate to cast an obligation of compliance of specific statutes, which is the role of the advertiser to comply. We recommend that the provision should focus on 'advertising' and not 'promotion of content' along with being limited by the laws that govern tobacco, alcohol and drugs in other areas.

2. Content take down

The Draft Rules impose an onerous obligation on intermediaries to take down content upon receiving a court order or notification by an authorized government agency within 24 hours of actual notice. However, the Draft Rules fail to provide any checks and balances to ensure that such requests are used in a just manner. The time limit of 24 hours is insufficient as it does not allow intermediaries to analyse the take down request or seek any further judicial remedy. This again, is in contradiction to the SC's ruling in the *Shreya Singhal* case as it does not ensure due process, as is required by the law. While this Rule is based on the ruling of *Shreya Singhal* case, the requirement of disabling content within 24 hours is much beyond the scope of the decision and in fact counters the freedom of expression aspect presented in the judgement.

The Draft Rules also increases the period of retention of records from 90 to 180 days or *such longer period as required by government agencies or courts*. However, the provision does not formulate sufficient safeguards to ensure that the power to extend the period of retention of data is used by government agencies in a fair, just, and transparent manner.
Fixed turn-around times raise significant implementation challenges, especially for companies with only a few employees working daytime shifts and the risk of excessive takedowns that run counter to the fundamental rights of citizens. In addition, an intermediary is often incapable of determining without further information which may push companies to remove content without reviewing it sufficiently.

Section 69A of the IT Act and the rules notified thereunder already provide for a procedure, with specific safeguards, for restricting or blocking content or access to such content upon receiving a court order. The obligation on intermediaries to proactively screen and take down content under the Draft Rules place intermediaries outside the ambit of intermediaries, therefore, denying them the opportunity to seek safe harbour protection under the provisions of the IT Act.

In situations of an emergency, where the content relates to public wrongs and meets the criteria / grounds laid down in Sec 69A of the IT Act, it may be tenable to impose a certain median time lines, but for content that relates to private disputes/wrongs and has a free speech element such as defamation, it would be unreasonable to impose such a strict timeline for intermediaries to act.

In all instances, the provision should also contain "Stop the Clock" provisions by listing out a set of criteria (such as seeking clarifications, technical infeasibility, etc.) under which the time limit would cease to apply to allow for due process and fair play in enforcing such requests.

3. Increased retention Period for a period of 180 days

A regulatory requirement to preserve content must meet the test of proportionality and reasonableness as laid down by the SC in the *Puttaswamy* decision. Further, the sub-rule should be consistent with the principle of data minimisation that runs as a common thread across the proposed Personal Data Protection Bill. These tests should define both the scope of content that is required to be preserved and the time period for which it should be preserved. The proposed amendments to the sub-rule go beyond these tests especially insofar as the time period of 180 days is concerned. Also data retention rules must comply with the principles of legality, necessity and proportionality.

Granting the power to 'appropriate government' or 'its agency' to seek preservation of data goes beyond the stated purpose for such requests that is for 'investigation purposes'. These should ideally be limited to "authorised law enforcement agencies."

Retain 90 Day Period: Intermediaries have been complying with the request for preservation of records pursuant to a valid lawful request subject to the condition that the record exists in its system as on the date of the request, which is also extended from time to time based on the lawful request. Further, the amendment could also clarify how this retention period would operate for users outside of India who also exercise their right to delete personal data pursuant to other foreign laws.

4. Proactive filtering

The *Shreya Singhal* case clarifies that intermediaries can only act as a facilitator of transmission of content on its platforms and must not pre-screen any content uploaded by users to judge the lawfulness of such content. However, the Draft Rules now impose an obligation on intermediaries to proactively screen content on its platforms, which goes against the SC's ruling. This provision is also likely to be seen as an interference with the right to freedom of speech and expression as any content uploaded by users will be subject to constant monitoring. In addition to curbing free speech, if intermediaries are required to pre-screen content, the nature of intermediaries is largely changed from being a neutral facilitator to an adjudicator of content, which may not be feasible for intermediaries to carry out.
The provision of intermediaries requiring to proactively monitor content being uploaded by users under the Draft Rules is also in contravention to the SC's decision in the *K. Puttaswamy* v. *Union of India case* (*Puttaswamy case*) as it fails to meet the tests laid down in the decision.[2] Therefore, any monitoring of content by the intermediary is intrusive to an

[2] https://indiankanoon.org/doc/127517806/

individual's freedom of speech and expression and right to privacy and may pose a serious challenge to digital rights available to users worldwide.
Given the massive volume of content shared online, platforms will have to take a 'better safe than sorry' approach – which in this case would mean 'take down first, ask questions later (or never).' These threaten not only to impede legitimate operation of (and innovation in) services, but also to incentivize the removal of legitimate content. This is one of the reasons why laws and policy principles have generally not required platforms to proactively monitor and filter all content; for instance, the United Nations' Joint Declaration on Freedom of Expression on the Internet affirms that "intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression."

It is also worth noting that 'Unlawful content' is a highly subjective expression and not capable of precise interpretation or determination by any reviewer. Internet is available on a worldwide basis and its content is available in multiple languages, dialects and vernacular / slang – which of these terms will be objectionable or offensive is impossible to determine in a fool proof manner. Further, the rule envisages such AI technologies to have 'appropriate controls', which only renders the scope of the rule even more subjective, wider, open-ended and almost impossible to comply with.

This proposed amendment in the draft rules goes against established international case laws and India's commitments under various international covenants, which include:

- UN Rulings such as General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights (ICCPR) issued by the UN's Human Rights Commission (July 2011).
- Joint Declaration on Freedom of Expression and the Internet (2011) issued inter alia by the UN Special Rapporteur on Freedom of Opinion and Expression.
- It is also submitted that the legal and regulatory framework in other jurisdictions does not support making 'proactive monitoring' of content whether by automated or by human means, as a pre-condition for intermediaries to avail of safe harbour protection.

Within Indian law, the changes in draft rules are also in direct conflict with the mandatory provision of the Section requiring intermediaries to abstain from selecting or modifying transmission to avail exemptions from liability. Rule 9 goes against the statutory intent as outlined in Sec 79 (2)(b) that entitles an intermediary to statutory protection only if it does not select or modify the information contained in the transmission.

On another note, developing and implementing technology based tools to pre-screen content is an extremely complex engineering task and can be very onerous to implement even by established intermediaries. For start-ups and relatively smaller intermediaries, it is an extremely high burden and may even result in killing innovation and investment in the sector, especially if its linked to their ability to avail of the statutory immunity to which they are entitled.

The lack of clarity, technical infeasibility (especially for smaller players) and lack of good Samaritan Principles are all reasons why this provision should be removed, or decoupled with the due diligence guidelines that would form the basis for an intermediary to avail of its statutorily granted defence of safe harbour.

If retained, the provision should include a carve out that an online platform should not be penalized to the extent it may make voluntary efforts to implement proactive filtering (good Samaritan Provision). This is crucial, as it allows companies to go above and beyond the requirements where appropriate, including voluntary efforts without engaging in pre-censorship.

II. RIGHT TO PRIVACY

a. On 30 June 2014, the United Nations High Commissioner for Human Rights (*OHCHR*) published its report on the right to privacy in the digital age.[3] The OHCHR recognises the relationship between online service providers and surveillance and the increasing trend of privatised surveillance, noting:

"*There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation*".

b. Recently, in one of the most landmark judgments pronounced in India, the SC upheld the right to privacy as a fundamental right under Part III of the Constitution of India in the case of *Puttaswamy case*. The SC observed that any legislation or action that restricts the right to privacy of an individual is required to fulfil the tests of legality, necessity, and proportionality. However, we observe that the Draft Rules fail to regard the decision of the SC by imposing several obligations on the intermediaries, which may result in an unreasonable restriction on the right to privacy of individuals.

RECOMMENDATIONS ON RIGHT TO PRIVACY

1. Periodic user intimation of applicable laws and ToS.

The Draft Rules amend the Intermediary Rules to specify that intermediaries are required to inform their users, *once every month*, that non-compliance with the rules and regulations, user agreements and privacy policy may lead to termination of services.

This seems to be an unnecessary, additional obligation on intermediaries as such information is already provided for in the user agreements that are easily available and accessible to users on the intermediary's website. While this is not cost-effective for several companies as it increases compliance related expenses, users may not appreciate excessive information provided by the intermediaries at such intervals leading to notification fatigue.

There are various ways in which a user can be informed of their obligations to comply with TOS and the choice should be left to intermediaries to determine the most appropriate way to do so, depending on the product/ service offered by the intermediary. An over-prescriptive approach should be avoided.

2. 72 Hour compliance for all requests

The Draft Rules require intermediaries to provide, within 72 hours of receiving a court order or notification by an authorized government agency, information and assistance if it *concerns the security of the State or cyber security or for investigation, detection, prosecution or prevention of any offence, and for protective or cyber security and any other incidental matters*.

[3] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

This provision is not only devoid of the specific instances where any government agency can seek information and assistance from intermediaries, but also goes against due process of law as intermediaries are compelled to share information without reasonable or justifiable grounds/causes. This provision fails to meet the three-pronged test upheld in Puttaswamy case.

Additionally, the Draft Rules mandate intermediaries to provide information or assistance to government agencies *within* 72 hours of a lawful order. However, the time frame of 72 hours seems to be arbitrary as 72 hours may not be sufficient time to respond to such requests.

The 72 hour response timeline should be dropped, as it can be technically unfeasible, especially for start-ups and MSMEs and also procedurally impossible to comply with for foreign requests for data governed by Mutual Legal Assistance Treaties (MLAT). Instead, the law should state such actions should be carried out expeditiously, with perhaps the inclusion of a narrowly but clearly defined emergency/urgent action provisions which can contain the 72 hour action provision for cases where there is an imminent threat to life, national security reasons and other grounds in the nature of those under Section 69A of the IT Act. There could be a graded classification of subject matters, with a requirement to respond to requests for information relevant to such content categories in a time bound manner.

In all instances, the provision should also contain "Stop the Clock" provisions by listing out a set of criteria (such as seeking clarifications, technical infeasibility, etc.) under which the time limit would cease to apply to allow for due process and fair play in enforcing such requests. An appropriate provision in this regard could be added to the provision, which could read "Provided that in cases where such court order or notification is not clearly actionable, the intermediary may seek further clarity and should endeavour to disable the content upon the order or notification being so clarified in accordance with law".

3. Enabling traceability of originators

The draft rules have a provision stating that the intermediary shall enable tracing out of originators of information on its platform, as may be required by government agencies who are legally authorised.

The provision does not define traceability, especially in the context of basic subscriber information already collected by various online platforms. This lack of clarity leaves the door open for conflicting interpretations during enforcement proceedings as well as judicial interactions under the rule. The implications of the expression, 'enable tracing' is not clear. It could mean enabling traceability by the government or by the intermediary in response to a government request.

The Rule casts an obligation of traceability requirement which means that in encrypted services, an intermediary is required to break the same and provide details. However, such broad obligation to enable tracing out of such originator of information may conflict with foreign laws in cases where the originator is based outside India. For context, an originator is defined under the IT Act as "*a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary*".

The lack of clarity, technical infeasibility (especially for smaller players), potential for breach of privacy via surveillance and subjectivity in enforcement are all reasons why this provision should be removed.

Alternatively, the provision should provide clarity on terms such as 'enable tracing', define criteria of what would be 'sufficient' when it comes to user information that can be collected by providers and limit the scope of requests that can be made under the rule to prevent 'one to many' matching of content.

4. Local incorporation and presence

The Draft Rules specify that if any intermediary has 50 lakh (5 million) or more users, or is specifically notified by the government, such an intermediary is required to have presence in India (by way of incorporation and having a registered office in India) and appoint officers in India for interacting with law enforcement agencies on the clock.

Such a requirement will adversely affect companies that currently do not have any registered office in India, however, offer their services to users in India. With increase in compliance costs that come with incorporation of a company in India, companies across the globe including start-ups may have to reconsider targeting users in India. Consequently, users in India may not be able to avail a variety of services required for carrying out day-to-day communication, online transactions, and trade/business related tasks.

This proposed provision requiring local incorporation and physical offices will also have a huge repercussion on taxation, foreign direct investment and other legal perspective along with negatively impacting economic growth. This also seems to be a further step towards a forced data localisation. The pressing issues with these provisions are:

- Intermediaries are covered by the IT Act. The current scope and applicability of the IT Act (Section 1) does not prescribe the persons to whom the IT Act is applicable to be established or registered in India (including IT service providers and intermediaries), as is the case for various statutes applicable to other sectors (for eg, insurance companies under the Insurance Act or access.
- This new criteria will disrupt the business activities of sectors in India who are dependent upon the intermediary services. Further, mandating that all intermediaries must necessarily have a registered presence in India, would mean that certain established intermediaries that are conducting their business in complete compliance with applicable local laws may now fall foul of restrictions under the FDI policy and may be required to wind up their service offerings, significantly affecting the ease of doing business in India.
- The eligibility criteria of fifty lakh users is relatively low and can impose an unreasonable burden on start-ups/smaller intermediaries who would not have the ability or infrastructure to comply with the requirements under this amendment (and consequently impacting innovation and start up growth in India).
- The vague and arbitrary nature of this provision also leaves various open questions that need clarification. Some of these are: the criteria of determining the number of users of an intermediary service, enforcement mechanisms for entities such as international websites and the infeasibility of blocking entire tracts of the Internet (eg: Wikipedia) that can fall afoul of these requirements.
- The global nature of the Internet has democratized information which is available to anyone, anywhere in an infinite variety of forms. The economies of scale achieved through globally located infrastructure have contributed to the affordability of services on the Internet, where several prominent services are available for free. Companies are able to provide these services to users even in markets that may not be financially sustainable as they don't have to incur additional cost of setting-up and running local offices and legal entities in each country where they offer services. Therefore, these new rules will harm consumer experience on the open internet, increase costs to an extent that offering services / technologies to consumers in India becomes financially unviable

Given that the intended objective of this rule is to ensure that in the event of an emergent legal issue, there is a locally available representative of an intermediary (nodal point of contact) to play a coordinating and facilitative role with law enforcement agencies and officers for the purpose of compliance to their orders/requisitions made in accordance with provisions of law or rules. These could ensure that the process of review is timely and effective, without placing onerous

burdens on a vast majority of intermediaries. The provision could also provide criteria for notifying intermediaries, methodology to determine metrics such as number of users and enforcement mechanisms to ensure effective enforcement and clarity in day to day operations for all relevant actors.

CONCLUSION

With India being on the forefront of technological development and innovation, any legislation that regulates intermediaries ought to take cognizance of the prevailing procedure established by law, judicial precedents, and global practices. The Draft Rules, to a large extent, disregard several principles upheld by the SC and the provisions of its parent legislation, the IT Act. To ensure that companies in the Indian market enhance the services offered to users, any regulation affecting the privacy of users and their rights to exercise their freedom of speech on such platforms cannot be shadowed by additional, onerous obligations on intermediaries. We request the Ministry of Electronics and Information Technology to review the Draft Rules keeping in mind the needs of the industry and rights of the users in order to enable better access to online services.

-End