

Public Comments
On
DRAFT
INTERMEDIARY
GUIDELINES
RULES, 2018

*Published by Ministry of Electronics & IT
Government of India*

Comments to the Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

Dr. V. Sridhar (vsridhar@iiitb.ac.in), *Dr. T.K. Srikanth*, *Dr. Janaki Srinivasan*
Professors

International Institute of Information Technology Bangalore (IIIT-B)

1. In Clause (3)(5) “.. provide such information or assistance as asked by any government agency or assistance ..” is very broad and could be potentially mis-used. The request should be from “an agency authorized by the Government and by an officer not less than .. [specified cadre level].. “ to take ownership and responsibility of such requests.
2. In Clause (3)(5), “.. or investigation or detection or prosecution or prevention of offence(s);” is again very broad and can be potentially mis-used. The offenses should be related to State’s interest as specified under clauses (3)(2)(i) and (3)(2)(k) and shall be modified to include such relevant offenses only.
3. In Clause (3)(5), “Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or assistance.”, though indicates “purpose limitations”, it has to be augmented with the following: “Such request shall be occasional and should not be concerned with entirety of electronic records but those that are specific to the intended purpose.” This will limit the scope of such requests and force the requesting entity/ officer to define the purpose of such request to be granular and not very broad.
4. In Clause (3)(9), “.. tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing ..”, imply that the intermediaries shall deploy automated or manual mechanism to look through the electronic records and decide on further action possibly based on the content of the message. While this shall be deployed by the intermediaries, the “proactive monitoring” could be used for intentional deletion or removal of messages by the intermediaries and might lead to discriminatory behaviour. It is possible that intermediaries could use humans to look at the messages for this purpose that might lead to biases creeping to segregation of messages. Further, automated mechanisms (algorithms) could have implicit biases depending on the way they were developed, and these could lead to bias in the classification of messages. One way to minimize such intentions on the part of the intermediaries is to mandate the intermediaries to publish the details of the mechanisms used for identifying, removing or disabling periodically so that these are transparent to the users at large.
5. What happens when an authorized request by the State is incorrect? How can the victim whose messages have been handed over by the intermediary to the State (police or government official) be compensated? There is no provision on such grievance redressal by the data subjects on the State either in the IT Act 2000 [amended 2008] or the Intermediary draft rules. This is precisely the reason why despite repeal of Section 66A of the IT Act by the Honorable Supreme Court, arrests are being made on that account

as recently reported by the Honorable Supreme Court itself. Except to file contempt proceedings in the courts, the data subjects who fall victims to such action by the State have no recourse. Hence we suggest a dispute appellate tribunal be formed, much similar to Telecom Dispute Settlement Tribunal (TDSAT) or Data Protection Authority as envisioned in the Data Protection Bill. This tribunal shall be an autonomous and independent body that looks in to disputes regarding State's request for information capture, transfer, interception. If the results of the dispute settlement are against the State, the associated requesting agency and the officer who ordered such request shall be punishable with the imposition of fines. If India includes this as part of the IT Act amendments, it will go a long way in protecting the interests of data subjects; make such State requests purpose oriented and occasional; improve trust of the data subjects over State surveillance; and be one of the first in the Worlds to include such legal provision.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)



ALL INDIA PROFESSIONALS CONGRESS

SOUTH MUMBAI CHAPTER

January 2019

Feedback on the (Draft) The Information Technology Intermediaries Guidelines Amendment Rules 2018

Rule	Provision	Feedback
3(2) (b)	<p>(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —</p> <p>---</p> <p>(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;</p>	<p>Regulation 3(2) (b) requires social media companies to prohibit content that is inter alia grossly harmful and obscene. These are ill-defined, subjective phrases and should be deleted. Pornography and invasion of privacy are already covered</p>
3(3) (f)	<p>(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;</p>	<p>The crossed out words (“ grossly offensive”) should be deleted since they are ill-defined and subjective:</p> <p>(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;</p>
5	<p>Regulation (5) When required by lawful order, the intermediary shall, within 72 hours of communication</p>	<p>This provision as it stands now, violates the fundamental right to freedom of speech and expression guaranteed by the Constitution under Article 19, but giving the government to</p>

	<p>provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised</p>	<p>silence anyone on social media by mere executive action. Safeguards need to be built in by making this subject to judicial approval. If required, a special judicial authority may be set up for this purpose. The UK has also set up a commission independent of the Executive for this purpose. Also, the power to trace out the originator of the message violates the right to privacy promulgated as a fundamental right under the right to life and personal liberty under Article 21 by the Supreme Court in Justice KS Puttaswamy vs UOI 2017</p> <p>Hence, we suggest that the following wording should be inserted (given in bold):</p> <p><i>Regulation (5) When required by lawful order, the intermediary shall, within 72 hours of communication provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.</i></p> <p>{ Addition }</p> <p><i>Each such order must be in writing, giving reasons, and must be backed by the approval of a court or appropriate judicial authority which may be attached in scanned copy where the request is sent by electronic means</i></p>
8	<p><i>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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the</i></p>	<p>The following changes are suggested to protect Right to freedom of expression under Article 19 of the Constitution. Before curtailing a fundamental right, the government must take judicial approval. Further, the government or even a court cannot decide what is decent or moral as it is a question of individual taste.</p>

	<p><i>Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.</i></p> <p><i>Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.</i></p>	<p><i>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 Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.</i></p> <p><i>Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.</i></p>
--	--	---

For further information, please contact:

aipcsouthmumbai@gmail.com or

<p>Mr Mathew Antony General Secretary AIPC Maharashtra</p>	<p>Mr Sanjiv Batra President AIPC South Mumbai Chapter</p>	<p>Mr Raghuvir Mukherji AIPC Fellow South Mumbai Chapter</p>
<p>Mob: 9870323964 Email: mma@indasda.com</p>	<p>Mob: 9821131431 Email: Sanjiv.b.batra@gmail.com</p>	<p>Mob: 9930183963 Email: raghuvir.mukherji@gmail.com</p>

Draft Information Technology [Intermediaries Guidelines (Amendment) Rules, 2018]

Background:

Online platforms are crucial drivers of innovation and growth in today's digital era. They act as a main access point in providing unprecedented access to information and other content through social networks, blogging sites, search engines, and video-sharing platforms, and further, aid in building closer ties between users and content through targeted advertising. The importance of the internet in facilitating access to information, is therefore in no doubt. However, it does have implication in the potential misuse of such online platforms and resulting in the increasing spread of illegal content such as child pornography, child abuse, trafficking of human beings amongst others and rising incidents of the spread of fake news.

The growing number of such incidents on an online forum not only undermines individuals' trust and confidence in the digital environment but also threatens or poses significant adverse impacts on economic and societal activities and cyber security. However, at the same time, the policies that govern intermediary liability for communications (content) made over the internet has a significant impact on user's rights including freedom of speech and expression and privacy rights. Therefore, there is a need to strike a balance between the needs of the government in implementing effective cyber security measures to ensure the security of networks and information systems and that of other stakeholders in creating an enabling environment for easy dissemination of information, protecting freedom of expression and ensuring individuals' right to privacy.

Comments/Suggestions to the Draft Rules:

1. Issue: Definition of Appropriate Government under Section 2(b) of the Draft Rules

Current Scenario: At present, the Draft Amendment Rules, 2018 defines 'appropriate government' to mean the definition provided in Section 2(e) of the IT Act, 2000 which makes a broad and uncategorized reference to the State Government with respect to matters enumerated in List II and any State Law enacted in pursuance of List III of the Seventh schedule of the Constitution, and the Central government in any other case. In this regard, the Draft Rules make it mandatory on intermediaries to take down or disable unlawful content on being notified by the appropriate government or its agency.

We believe that the scope of the definition 'appropriate government' is too vague and broad in its ambit which could have potential negative implications on the Freedom of expression enshrined in Article 19(1) of the Constitution of India.

Recommendation: Instead, we recommend the establishment or appointment of a designated 'Competent Authority' that may either comprise of law enforcement authorities or an administrative authority lawfully authorized to issue such takedown notices to intermediaries. This imposes responsibility on one specific body or a small class of competent authorities for specific sectors (that may be identified as Critical Information Infrastructures) and other internet intermediaries (like internet service providers) in reviewing and assessing cyber security contents

and ensuring the same does not fall within the contours of 'unlawful content'. The Competent Authority may include authorities like the Ministry of Information Technology, Ministry of Public Security, Ministry of National Defence, Ministry of Foreign Affairs etc.¹ We further recommend the appointment of a single point of contact (SPOC) to co-operate and co-ordinate with national competent authorities of other Countries where the cyber security incident has a cross-border impact.

In assessing similar frameworks on Intermediary Liability Guidelines especially in the European Union, this appears as a common practice. The European Commission's Communication on tackling illegal content online² and the EU's draft Regulation adopting a general approach on preventing the dissemination of terrorist content online³ requires Intermediaries to disable access to or take down illegal content online upon receiving notice from National courts of Member States or the national Competent Authority to be established by each Member State.

2. Issue: Removal of content or disabling access to content online by Intermediaries

Current Scenario: Intermediary liability relates to the legal accountability imposed on intermediaries with respect to content that is hosted and transmitted through its networks and online platforms. However, it is pertinent to point out that although intermediary liability requirements may be an effective measure in curbing the spread of illegal content online and the transmission of fake news via online platforms, it can also be used to control the dissemination of legitimate content as well through automated filtering methods. This creates an increased risk on the right to privacy because of the requirement of intermediaries to proactively monitor and filter its user's communications.

Although it is not disputed that such proactive measures (self-regulation) are required on the part of intermediaries to monitor, identify and remove or disable public access to unlawful information or content given the urgent need to curb the spread of child pornography, child abuse, trafficking of human beings, hate speeches, fake news etc., and given that the same measures have been proposed and adopted in other jurisdictions in recent times like in Germany⁴ and other EU Member States (having implemented the E-commerce Directive) as well as Russia,⁵ we believe that certain safeguards are required to be implemented in order to prevent over-removal of legitimate content by intermediaries.

Recommendation: Considering that the automated detection and filtering measures to be taken by intermediaries can affect the accuracy of the prompt removal of unlawful content and simultaneously result in accidental removal of legitimate content (over-blocking), we believe that

¹ The following are a few Competent Authorities established and appointed under the Cyber Security Laws of Vietnam, Singapore, China, Poland, Netherlands, amongst others.

² Communication from the Commission to the European Parliament, The Council, The European Economic And Social Committee and the Committee of the Regions on Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, COM (2017) 555 available at <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-555-F1-EN-MAIN-PART-1.PDF> at page 7.

³ Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online - general approach of 6th December 2018, available at <http://data.consilium.europa.eu/doc/document/ST-15336-2018-INIT/en/pdf>.

⁴ See Germany's Network Enforcement Act (NetzDG) (2018).

⁵ Wolfgang Schulz, Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG (2018) at 5, available at <https://www.hiig.de/wp-content/uploads/2018/07/SSRN-id3216572.pdf>.

there is a need to incorporate provisions into the Draft Rules to ensure that such content that is removed because of over-blocking be reinstated. The European Commission's Communication on Tackling Illegal Content Online⁶ contains provisions providing a user uploading data onto an online platform with an opportunity to contest the decision of removal of content by way of a counter-notice. If the counter-notice has reasonable grounds to consider that the content uploaded was not unlawful, the intermediary is required to reinstate the content onto its platform or allow the user to re-upload it without any prejudice to the intermediary's terms of service. Similarly, European Commission's regulation on the prevention of dissemination of terrorist content online provides for intermediaries to appeal against the removal order notified by the Competent Authority before the respective judicial authority.⁷

Special recommendation for 'notice and takedown' in copyright infringement actions:

With respect to infringement actions of copyrights and other proprietary rights, we recommend the adoption and incorporation of the 'Notice and Takedown' procedure as contained in section 512 of the Digital Millennium Copyright Act (DMCA)⁸ wherein a formal take-down notice is to be submitted to the intermediary containing the following:

- signature of claimant (owner of the works or individual acting on a right owner's behalf);
- identification of the work or works that the right owner claims have been infringed;
- identification of the material that is infringing and where that material is located;
- the claimant's contact information;
- a statement that the claimant "has a good faith belief" that the material used is unauthorized;
- a statement under penalty of perjury that the information given is accurate and that the actor is authorized to do so.

The claimant is required to write and provide notification to the designated agent who the ISP identifies on their server. On receiving such notification, the ISP must take down any content identified as potentially infringing and take reasonable steps promptly to notify the user that it has removed or disabled access to the material. The user on receipt of such notification has the opportunity to contest the claimant's allegation of infringement and consequent removal by sending a counter-notification. The counter notification must contain the following:

- the user's signature;
- information about the removed material along with its location;
- a statement under penalty of perjury that the user has a good faith belief that the material was removed or disabled due to mistake or misidentification;
- the user's name, address, and telephone number,
- statement that the user consents to the federal district court within their jurisdiction, and an acceptance of process.

An ISP that receives a valid counter-notification is required to forward the same to the claimant along with a statement that it will put the material back in ten (10) business days unless a court

⁶ Communication on Tackling Illegal Content Online, *supra* note 2 at 17.

⁷ Article 15, Communication on Tackling Illegal Content Online, *supra* note 2.

⁸ Digital Millennium Copyright Act, 17 U.S.C. § 512 (2012).

order is filed preventing the user from infringing any copyrights. An ISP that fails to hear from the notifying party can enable access to the material 10–14 business days later.

We believe that implementing such safeguards into the Draft Rules enhances transparency, respects due process, and ensures that the fundamental right to freedom of expression is not unreasonably restricted. The same is in line with the Manila Principles of Intermediary Liability in particular, Principle 5 which stipulates that all laws and content restriction policies and practices are to adhere to due process which includes providing the user content provider an opportunity to be heard before removal of content and a right to appeal against content restriction and removal orders.⁹ The right to appeal against the decision of the Competent Authority is also enshrined in Singapore's law on Cyber Security which provides the operator of a Critical Infrastructure to appeal to the Minister against the decision of the Commissioner¹⁰ and a second appeal to the Appeals Advisory Panel.¹¹

Further, as part of this transparency requirement, we believe it is to be made obligatory on the part of the government to regularly and publicly report the aggregate number of legal removal orders issued by them to the intermediary and the aggregate number of users affected by the same.¹² The same is in line with the Recommendation of the European Commission on the roles and responsibilities of internet intermediaries adopted on 7 March, 2018.¹³

3. Issue: Criteria to determine Cyber security incidents

Current Scenario: With respect to tackling cyber security incidents and ensuring security of network and information systems, we are of the opinion that the Draft Rules are not comprehensive enough in terms of determining the parameters or factors to be taken into account for identifying Critical Information Infrastructure as defined in Section 2(e) of the Draft Rules,¹⁴ determining the scope and parameters in determining 'adverse event' as contained in the definition of 'cyber security incident' in Section 2(f) of the Draft Rules, and the notification or reporting obligations of intermediaries on the occurrence of a cyber security breach.

Recommendation:

(i) Establishing parameters to identify Critical Information Infrastructure:

At the outset, we believe that the definition of cyber incident should be slightly modified to include any adverse event that results in the unauthorized disclosure of information apart from

⁹ Principle 5, Manila Principles on Intermediary Liability, Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation (2015) available at https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.

¹⁰ Section 17, Cybersecurity Act 2018 (Act. 9 of 2018).

¹¹ Id, Section 18.

¹² GNI Statement on Europe's Proposed Regulation on Preventing the Dissemination of Terrorist Content Online, available at https://globalnetworkinitiative.org/gni-statement-draft-eu-regulation-terrorist-content/#_ftn10.

¹³ Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries on 7 March 2018, Appendix to Recommendation at 1.2.3. available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.

¹⁴ Determining the factors to be taken into consideration in identifying Critical Information Infrastructure has not been addressed in the relevant provision under the IT Act, 2000 [Section 70(1)] either.

unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data under Section 2(f) of the Draft Rules.

Secondly, the European Union in its Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)¹⁵ prescribes certain criteria for the identification of operators of essential services to include:

- an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.¹⁶

We believe that the above parameters are to be taken into consideration in order to identify operators of Critical Information Infrastructure as defined under Section 2(e) of the Draft Rules wherein the Competent Authority would be required to provide a list of Critical Information Infrastructures (Eg: Transport, Information Technology and Telecom, Electricity etc.) that satisfy the criteria mentioned above for which reporting obligations and implementing necessary cyber security measures are triggered.

(ii) Parameters in determining ‘adverse event’ in the definition of ‘cyber security incident’ contained in Section 2(f) of the Draft Rules:

The Directive further specifies that the following parameters shall be taken into consideration in determining ‘adverse event’ causing significant disruptive effect in the provision of services of entities operating as Operators of essential services and Digital Service Providers:

- the number of users relying on the service provided by the entity concerned and affected by it;
- the dependency of other sectors on the service provided by that entity;
- the dependency of other sectors on the service provided by that entity;
- the market share of that entity;
- the geographic spread with regard to the area that could be affected by an incident;
- the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.¹⁷

These parameters have been successfully implemented in 24 EU Member States at present. Similar parameters have been utilized by countries in the Asia-Pacific Region such as Singapore¹⁸, China¹⁹ and Vietnam²⁰ in their domestic laws on Cyber security imposed on Internet Service Providers and other entities engaged in providing online services.

¹⁵ Article 5, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

¹⁶ Id.

¹⁷ Id.

¹⁸ See Cybersecurity Act 2018 (Act. 9 of 2018) passed on 5 February 2018 and entered into force on 31 August 2018.

¹⁹ See Cybersecurity law of the People's Republic of China ("Cybersecurity law") on June 1, 2017.

²⁰ See Law on Cybersecurity (Luật an ninh mạng) (the CSL 2018) to be in force on 1 January, 2019.

We believe that incorporating identical parameters into the provisions contained in the Draft Rules would render more clarity and structure into what amounts to an 'adverse event' that would give rise to a cyber security incident.

4. Issue: Reporting obligations of intermediaries on occurrence of cyber security breach

Current Scenario: The reporting obligations of intermediaries on cyber security incidents as contained in the Draft Rules merely requires intermediaries to report incidents and related information to the Indian Cyber Emergency Response Team. We believe that this provision is not comprehensive and is lacking clarity with no time period specified within which such notification is to be made, the contents of such notification etc. These obligations are crucial in minimizing or preventing cyber security incidents and need to be more substantively addressed.

Recommendation: The European Commission's NIS Directive which has been successfully transposed into the domestic legislation of a majority of the EU Member States requires Operators of essential services and digital service providers to notify the Competent Authority or the Computer Security Incident Response Team (CSIRT) of the cyber incident within a period of time as stipulated by the governments of the respective Member States, and where appropriate, the competent authority may inform the public of a cyber security incident or require digital service providers to do so, where public awareness is necessary in order to prevent an incident or deal with an ongoing incident, or where disclosure of the incident is in public interest.²¹ We believe that such communication or disclosure to the public is also necessary in certain circumstances involving larger public interest.

While most EU Member States require the notification to be made 'without undue delay' to be determined on a case-to-case basis, other Member States such as the United Kingdom²², Germany²³, Ireland²⁴ require notification to be submitted within 72 hours. We suggest the inclusion of a similar time period or limiting it to within 48 hours from the time of determination of the cybersecurity incident.

The content of such an obligation as a general practice observed in most EU Member States (Eg: United Kingdom, Netherlands, Croatia, Germany, amongst others) and Countries in the Asia-Pacific region like China includes incorporating details of the description (nature and character) of the cyber security incident, the duration of the incident and the time at which it occurred, cause and source of the incident, potentially harmful consequences of the incident, cross-border impact (if any), remedial measures taken by the intermediary or proposed to be taken to mitigate the risk or prevent it from occurring, etc.

Therefore, we believe that a more detailed approach in the reporting requirements of intermediaries to the Indian CERT is required considering that such disclosure or notification requirements have not been suitably addressed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 as well.

²¹ NIS Directive, Article 16, *supra* note 15.

²² Section 12(6), The Network and Information Systems Regulation (2018 of 506).

²³ Section 8(b), German IT Security Law („IT-Sicherheitsgesetz“) of 25 July 2015. See, Cybersecurity 2019 (Germany) available at <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany> .

²⁴ Section 22(3), European Union (Measures for a High Common Level of Security for Network and Information Systems) Regulations, 2018.

We recommend that the reporting obligations of intermediaries include the following:

- Name of the relevant internet intermediary including the name and other contact details of the person familiar with the cyber security incident and authorized to act on behalf of the intermediary.
- Description of cyber security incident. This includes the category of the incident such as external attack (hacking etc.), data loss, disruption of software or hardware components, violation of internal IT Security Guidelines, internal causes, force majeure.²⁵
- How the cyber security incident was discovered?
- The duration and time of occurrence of cyber security incident.
- Cause of the cyber security incident.
- Impact/harmful consequences of the cyber security incident. This includes cross-border impact, if any.
- Remedial measures adopted or proposed to be adopted by the intermediary in resolving the cyber security incident.
- To which body/ competent authority the intermediary reported the cyber security incident to.

5. Issue: Due diligence required to be taken by Intermediaries:

Current Scenario: Section 3 of the Draft Rules prescribes certain due diligence measures to be undertaken by intermediaries in the discharge of their duties. Among these measures is the requirement to make available to the public the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person. We are of the opinion that this requirement is in accordance with best practises followed by other jurisdictions. This is in accordance with the Manila Principles of Intermediary Liability,²⁶ the Commission's Regulation on Tackling of Illegal Content Online²⁷ as well as the Recommendation of the European Commission on the roles and responsibilities of internet intermediaries.²⁸

However, we believe that the language used in determining the various due diligence measures required to be taken by intermediaries is very vague and subjective and goes beyond what is envisaged under Article 19(2) of the Indian Constitution in the usage of phraseologies such as "harassing", "disparaging", "hateful", "ethnically objectionable", "or otherwise unlawful in any manner" etc. It leaves much to the individual judgment of the censoring body (the intermediary in this case) and is too onerous and unreasonable an obligation to impose on intermediaries. We believe that a more objective guideline or criteria needs to be adopted on what kind of content stands prohibited on an online platform which can be ensured by intermediaries in carrying out their due diligence obligation. However, expecting internet intermediaries to filter content on their platforms based on the current parameters stipulated in Section 3 of the Draft Rules amounts to an excessive and unreasonable restriction of the fundamental right of freedom of speech and expression.

²⁵ See Annex 1 as per Section 4(6), German IT Security Law ("IT-Sicherheitsgesetz") of 25 July 2015.

²⁶ Principle 6, Manila Principles on Intermediary Liability, *supra* note 9.

²⁷ Communication on Tackling Illegal Content Online, page 16 available at <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-555-F1-EN-MAIN-PART-1.PDF>.

²⁸ Recommendation of the European Commission on the roles and responsibilities of internet intermediaries, *supra* note 13 at 2.2.

Recommendation: We recommend that the intermediaries should exercise due diligence by ensuring that both the takedown notice issued by the rights owner or the intermediary (as the case may be) and the counter-notification submitted by the user uploading data on the online platform (subscriber) are assessed and evaluated by the designated Competent Authority based on the parameters to determine 'unlawful' online content as contained in section 3(2) (a)-(k) of the Draft Rules. Accordingly, the competent authority should determine whether such content is to be removed by the relevant intermediary. Further, the burden of proof should lie on the individual alleging illegality of the online content.

6. Issue: Data localization requirement by intermediaries

Current Scenario: The Draft Rules require intermediaries having more than fifty lakh users in India to mandatorily have a physical presence in India by incorporating a company under the Companies Act, 1956 or 2013, having a registered office in India and appointing a nodal person of contact for 24x7 coordination with law enforcement agencies.

Recommendation: We believe that this data localization requirement is crucial as it enables storing of information and data domestically especially sensitive and personal data and data that is generated and collected by operators of Critical Information Infrastructures which facilitates easy access and quicker remedial responses in case of occurrence of a cyber incident. The same requirement has also been adopted and utilized in various other jurisdictions such as the EU Member States such as United Kingdom, Netherlands, Germany etc. wherein digital service providers are subject to their respective domestic Cyber Security Act and in compliance with the NIS Directive only if their main establishment is located within the territory of the concerned Member State, or have a representative appointed in the Member State in which they offer their digital services.²⁹ A similar provision is incorporated in the Cyber Security laws of Countries in the Asia-Pacific region like China,³⁰ and Vietnam.³¹

7. Issue: Data retention requirement by intermediaries

Current Scenario: The Draft Rules require retention of data for at least 180 days for investigative purposes or such longer period as required by the Court or lawfully authorised government agency.

Recommendation: We believe that the inclusion of such a provision is not unreasonable and is within permissible limits since the scope of what information is being retained has been restricted to only the alleged 'unlawful content' for the purpose of investigation. Data retention requirements have also been incorporated in cyber security laws of other Countries such as Vietnam wherein the law requires data retention for a minimum period of 12 months and extending up to 36 months depending on the kind of information.³² Although the Data retention Directive³³ was invalidated in the European Union, the same has been retained by EU Member States Germany, Romania and Czech Republic.

²⁹ See generally the Implementation Acts of various EU Member States available at <https://www.twobirds.com/en/in-focus/cybersecurity/nisd-tracker>.

³⁰ Article 37, Cybersecurity law of the People's Republic of China ("Cybersecurity law") on June 1, 2017.

³¹ Refer <https://vietnam-business-law.info/blog/2018/7/30/vietnams-new-cybersecurity-law>.

³² Article 26, Law on Cybersecurity (Luật an ninh mạng) (the CSL 2018).

³³ EU Directive 2006/24/EC on data retention was invalidated by ECJ on April 8, 2014.

MIT/79/012

Comments on the Draft Intermediary Guidelines (Amendment) Rules, 2018

Submitted to the Ministry of Electronics and Information Technology

Shrutanjaya Bhardwaj

B.A. LL.B. (Hons.), National Law University, Delhi (2017)
LL.M. Candidate, University of Michigan Law School (2019)
shrutlaw@umich.edu

4th January 2019

As per the [Ministry's website](#), these amendments are being proposed specifically to check the misuse of social media platforms for the spread of “fake news”. I have four submissions in this respect.

- I. Sub-rule (8) of Rule 3 is unconstitutional.
- II. Sub-rule (9) of Rule 3 is unconstitutional.
- III. Portions of sub-rule (2) of Rule 3 are unconstitutional.
- IV. The guidelines cannot constitutionally be applied to fake news.

These problems are discussed sequentially below.

I. SUB-RULE (8) OF RULE 3 IS UNCONSTITUTIONAL

Rule 3(8) reads as follows:

(8) 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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.

This provision is unconstitutional for two reasons. **Firstly**, it is ultra vires S.79(3)(b) of the IT Act. S.79(3)(b) authorizes the Government to direct the intermediary to take down information only when it is “being used [by an individual] to commit *the* unlawful act”. If the intermediary fails to comply, it incurs liability for the same unlawful act as committed by the individual. This shows that the Government is required to *identify* the precise unlawful act or offence that is being committed through the information which the Government wants removed. However, Rule 3(8) provides that the Government may direct the intermediary to take down any content as long as it is relating to one of the Art.19(2) grounds. Undoubtedly, the Supreme Court in *Shreya Singhal* did hold that any notification made under S.79(3)(b) must correspond to one of those grounds. But that is not enough – to comply with S.79(3)(b), the Government must also identify the precise offence or unlawful act being committed through the information.

There is another way to look at this. Art.19(2) permits the State to restrict speech only through a law. As per the Supreme Court's rulings in **Kharak Singh v. State of U.P., (1964) 1 SCR 332** and **Bijoe Emmanuel v. State of Kerala, (1986) 3 SCC 615**, the word “law” implies a statute or rules and

regulations having statutory force. This means that the State can validly restrict the freedom of speech only after it enacts a statute for one of the purposes specified in Art.19(2). Applying this principle to the guidelines in question, the Government may direct the intermediary to take down content only when such content violates a statute, statutory rule or statutory regulation. It must therefore identify such statutory provision etc. in its notification to the intermediary.

Secondly, this sub-clause makes no reference to the long list of prohibited information contained in Rule 3(2). Instead, it reproduces verbatim the grounds listed in Art.19(2) of the Constitution. This makes the provision vague.¹ Constitutional text, because of its very nature, contains broad principles which are meant to guide state action. These broad principles are mostly (and justifiably) couched in vague terms. But when the State proceeds to implement those principles, it must do so under a precisely drafted law. Note that one of the reasons why vague laws are unconstitutional is that they confer unfettered discretion on the implementing agency (in this case the Government). Sub-rule (8) is fraught with this danger. E.g., it empowers Government officials to censor content based on subjective notions of indecency and immorality.

For these reasons, Rule 3(8) needs to be reworded. A draft is suggested in the margin: suggested deletions are indicated through strikethrough, while suggested additions are marked in red.²

II. SUB-RULE (9) OF RULE 3 IS UNCONSTITUTIONAL

Rule 3(9) reads as follows:

¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, at para 79: “Quite apart from this, as has been pointed out above, every expression used is nebulous in meaning. What may be offensive to one may not be offensive to another. What may cause annoyance or inconvenience to one may not cause annoyance or inconvenience to another. Even the expression “persistently” is completely imprecise — suppose a message is sent thrice, can it be said that it was sent “persistently”? Does a message have to be sent (say) at least eight times, before it can be said that such message is “persistently” sent? There is no demarcating line conveyed by any of these expressions — and that is what renders the section unconstitutionally vague.”

² The intermediary upon receiving actual knowledge in the form of a court order, **or in the form of a notification** ~~on being notified~~ by the appropriate Government or its agency under section 79(3)(b) of Act, shall remove or disable access to **the information, data or communication link specified in the said court order or notification and residing in or connected to** ~~that unlawful acts~~ **relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence,** ~~on its computer resource,~~ **and the intermediary shall do so** without vitiating the evidence in any manner, **and** as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3;

Provided that the court order or notification, as the case may be, shall specify the unlawful act being committed and the legal provisions being violated through the information, data or communication link sought to be removed or disabled access to.

(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

Reading this provision with S.79(3)(b) makes its legal effect clear. Intermediaries would be held responsible for the spreading of unlawful content if they failed to place “appropriate” mechanisms and controls for its identification and disabling. This suffers from two constitutional problems. **First**, it is vague, as it does not specify what constitutes an “appropriate” mechanism. Since this is a penal provision and makes the intermediary liable, its vagueness would cause a chilling effect on speech by pushing intermediaries to be over-cautious in their approach and to censor more content than required. **Second**, this provision contravenes the ruling in *Shreya Singhal*, where the Supreme Court held that no obligation should be placed upon intermediaries to act *suo moto* in removing content (para 122):

“This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront.”

Third, the provision is probably unreasonable for assuming that automated mechanisms can be devised to combat unlawful content online. Leading social media companies have found it hard to engineer such tools.³ Therefore, and for the two reasons mentioned above, no requirement should be placed upon the intermediary to proactively curb unlawful content.

III. PORTIONS OF SUB-RULE (2) OF RULE 3 ARE UNCONSTITUTIONAL

This is an existing provision. Rule 3(2) lists several kinds of information that the intermediary must direct its users to not circulate. It was upheld by the Supreme Court in *Shreya Singhal*. However, one aspect seems to have been overlooked in that case. Art.19(2) permits restrictions to be placed on the freedom of speech only by way of a “law”, and “law” has been held to mean a statute, or a piece of subordinate legislation which may be traced back to a statute (see *Kharak Singh* and *Bijoe Emmanuel*). Many of the clauses under Rule 3(2) cannot be traced back to any legislation. E.g., parts of clause (f) have no legal basis after S.66A was struck down in *Shreya Singhal*. This alone renders them unconstitutional.

³ E.g., Facebook’s algorithms [have previously found it tough](#) to detect hate speech, though they are reportedly [making progress](#).

IV. THE GUIDELINES CANNOT CONSTITUTIONALLY BE APPLIED TO FAKE NEWS

Art.19(2) of the Constitution names nine grounds: sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency, morality, contempt of court, defamation, and incitement to an offence. *Shreya Singhal* stands for the proposition that any restriction on speech must correspond to at least one of these grounds.⁴ Fake news regulation, however, does not correspond to any of them. Let me briefly discuss four grounds which might seem to cover fake news.

“Public order” and “incitement to an offence” follow similar standards. This is because “public order” is interpreted as a ground to check incitement to imminent violence. Under both these grounds, speech is punishable only when it ceases to be mere discussion or advocacy and becomes incitement. The apex court discussed this in *Shreya Singhal*.⁵ The crucial difference between advocacy and incitement is a matter of listener autonomy: if the listener of my speech (or the recipient of my WhatsApp message) had enough time to deliberate on my speech and decide her course of action, I am not liable for any unlawful acts she performs. It is only when the speech/message resembles a “spark in a powder keg” that the speaker may be punished.⁶

On the other hand, “decency” and “morality” were both understood in *Shreya Singhal* as obscenity-related grounds.⁷ Although somewhat varying interpretations have been suggested by the Court on other occasions,⁸ it seems unlikely that these grounds would ever justify fake news regulation.

Hence, communication over social media platforms may not be regulated on the ground that it contains fake news. Fake news may be regulated *qua* incitement, *qua* defamation, *qua* hate speech, etc. (if it meets the respective standards), but not *qua* merely false information that falls short of these ideas. This means that the Intermediary Guidelines, just like all other laws, cannot constitutionally be applied to reach fake news *qua* fake news.

⁴ Para 15: “It is significant to notice first the differences between the US First Amendment and Article 19(1)(a) read with Article 19(2). ...Fourth, under our Constitution such restrictions have to be in the interest of eight designated subject-matters — that is, any law seeking to impose a restriction on the freedom of speech can only pass muster if it is proximately related to any of the eight subject-matters set out in Article 19(2).”

⁵ Para 13: “Mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart of Article 19(1)(a). It is only when such discussion or advocacy reaches the level of incitement that Article 19(2) kicks in.”

⁶ **S. Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574**, at para 45.

⁷ Para 50.

⁸ See **Ramesh Yeshwant Prabhoo (Dr) v. Prabhakar Kashinath Kunte, (1996) 1 SCC 130** for a discussion on decency; see **Navtej Singh Johar v. Union of India, 2018 SCC OnLine SC 1350** for a discussion on morality.



Freedom Publishers Union
Asia/Pacific Press Office - Mumbai Press Center
e: info@fpumail.net
w: www.freedompublishersunion.com

Submission to:
Ministry of Electronics & Information Technology
Government of India
e: gccyberlaw@meity.gov.in

January 24, 2019

To Ministry of Electronics & Information Technology;

Freedom Publishers Union understands and acknowledges the problems related to false and misleading information that have arisen in India, particularly over the duration of the past 12-24 months and specifically on the WhatsApp social platform. However, we cannot support the Government of India using these specific set of challenges as a means to justify further encroachment on civil liberties of the citizens of India through proposals to Section 79 of the IT Act which would force WhatsApp, and potentially other encrypted platforms, to decrypt secure data for the benefit of the Government of India, under the all too typically used reason of "national security".

We believe the proposals are a great concern and also believe that they are only the tip of the iceberg, as the Government of India attempts to further emulate the civil liberties encroachment and removal of basic freedoms of the citizens as has already been done, aggressively, and against the expert advice by digital rights organizations and activists, by Western democracies. The Government of India has already authorized increased powers to phone taps, which were then followed by further authorization for 10 government security and intelligence agencies to intercept sensitive internet data and seize electronic devices - All further evidence of the motivation of the Government of India to emulate the behavior of Western governments to increase mass-surveillance networks and increase government capabilities to 'legally' remove the freedoms and basic rights of citizens.

Although we welcome the opportunity on this occasion to make a public Submission, we do not believe that the Government of India has done enough on previous occasions in relation to what we consider quite important and invasive changes that do have real-world impact on the computer and internet usage habits of the citizens of India. It is of the political opinion of Freedom Publishers Union that the citizens should always be provided advanced notice of proposed changes and should always be provided with the opportunity for public Submission, where possible.

Data and messages that are encrypted is done so to guarantee and accommodate the right to privacy of users. Any attempt(s) to modify, break or bypass encryption technology is condemned by Freedom Publishers Union and a majority of the technology industry. Privacy is a right to be upheld, and not a right to allow for open abuse by law enforcement, intelligence or any other government associated agency. Furthermore, enabling the Government of India the ability to decrypt data would pose a significant threat to censorship of India's internet. Based on the expert advice we have sought, Freedom Publishers Union remains confident that internet censorship is not the intent of this specific proposal, however we warn that further imposition of censorship on India's internet could only be condemned, for adding to an already messy censorship regime the country suffers.

The proposals, as Freedom Publishers Union interprets them, mirror elements of the recent changes which have been implemented in Australia which the Government claim will achieve the same intent of the proposals by the Government of India. We strongly condemned and opposed the Australian legislation, as did the technology industry. Therefore, we are in a position where we must also oppose any legislation of the Government of India which attempts to replicate legislation to the same relative effect as Australia.

It is currently unclear what level of cooperation WhatsApp and other affected technology companies will offer the Government of India, in response to any future changes to the law. Freedom Publishers Union urges the collective technology and software security industry to unite and push back against any changes that are approved by the Government of India.

Freedom Publishers Union will continue to advocate and educate our supporters and internet users on technical methods and software that can be used to increase their security through strong encryption that cannot be cracked and to bypass censorship. We do this not in defiance of any specific country's laws, but because an open internet and free flow of information free from censorship and government interference is a core principle of our philosophical founding.

Amit Gautam
spokesperson@fpumail.net



Foundation of Data Protection Professionals in India

[Section 8 Company limited by Guarantees]

[CIN No: U72501KA2018NPL116325]

Registered Office: No 37, “Ujvala”, 20th Main, BSK First Stage,
Second Block, Bangalore 560050

E mail: fdppi@fdppi.in; Ph: 08026603490; Mob:+91 8310314516

Date: 20th January 2019

Comments on the Draft Intermediary Guidelines 2018

The following are the comments from FDPPI on the draft Intermediary Guidelines 2018 released by the Government for public comments.

These take into account the contents of

- a) Section 79 as per the ITA 2000 amended in 2008 and notified on 27th October 2009
- b) Information Technology Intermediary Guidelines 2011 which is sought to be amended now
- c) Information Technology (Guidelines for Cyber Café) Rules, 2011
- d) Clarification issued by MEITY on 18/3/2013
- e) Advisory issued on Matrimonial websites on 6th June 2016
- f) Advisory issued on measures to curb online Child sexual abuse material on 18th April 2017

Apart from providing our views on the specific modifications now proposed by the Ministry, we would like to also provide some additional long term suggestions which may be considered as part of the current modifications.

General Comments

“Intermediaries” as defined in ITA 2000 are a very important segment of the economy as well as the security eco system of the nation. Regulating intermediaries is critical for Cyber Crime control as well as reducing the possible misuse of Internet by criminals, terrorists and foreign powers.

Intermediaries are also important from data protection requirements since they also control the BFSI, Health and Social Media sectors.

Therefore it is essential that Intermediaries are regulated effectively.

Since there are different types of intermediaries which may include Cyber Cafes, Matrimonial Websites, Mobile App companies, Mobile or Internet Gaming Companies, etc besides the more visible Fintech, Health care and Social Media companies, the umbrella regulations

have to be flexible enough to be supplemented by the additional sector specific guidelines. Otherwise the regulations would seek a lower common denominator or face legal challenge as unfair restrictions.

Keeping these requirements in mind, the following suggestions have been made which includes assigning the responsibility to the ssDirector General of IN-CERT to issue security guidelines as and when required for specified types of intermediaries and an “**Intermediary Dispute Resolution Policy**”.

Suggestions

Rule 2: to be modified to include the definition of “Intermediary Dispute Resolution Policy” (IDRP) as follows:

2(m) : “Intermediary Dispute Resolution Policy” (IDRP) means a policy as defined under rule 14 below of this notification.

2(n): “Intermediary Dispute Resolution Center” (IDRC) means an organisation that is registered with the MEITY for the purpose of resolving any disputes arising out of compliance related to Section 79 of ITA 2000/8 (Information Technology Act 2000) and the rules and regulations issued under an IDRP adopted by the organization.

2(1) to be modified as under

“User” means any person who avails the services of an Intermediary and conforming to the requirements under Section 79(2)(a) and 79(2)(b), of ITA 2000/8, which service includes, hosting, publishing, sharing, transacting, displaying or uploading information or views either on any computing platform including the mobiles.

Rule 3(1) to be modified as under:

The intermediary shall publish on the website where the services are offered to public

- a) Terms of Use of the services and an appropriate Privacy Policy
- b) Disclosure of ownership of the service.
- c) Disclosure of registration under data protection laws if any.
- d) Designated Grievance Officer as a single point of contact for the public and the Grievance redressal Mechanism applicable for resolution of any disputes.
- e) Any other information relevant for the provision of the service.

Rule 3(2) to be modified as under:

- A) **The terms of use** referred to under rule 1 shall include a notification to the users of the services of the intermediary that

The user shall use the services responsibly and shall take reasonable precautions

- i) not to use the services in a manner that threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or

- causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation
- ii) not to use the services in a manner that threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;
 - iii) not to use the services in a manner that threatens critical information infrastructure.
 - iv) Not to Impersonate another person or deceives and mislead about the origin of any message or communication
 - v) Not to cause harm to minors
 - vi) Not to cause infringement of intellectual property rights such as Copyright, Trademark or Patent
 - vii) Not to cause distribution of any content that contains a computer contaminant/virus/malware or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
 - viii) Not to cause a wrongful harm to any person

B) **The Privacy Policy** referred to under rule 1 shall be compliant with the data protection laws as applicable and ensure that identifiable personal data

- i) Shall be collected only to the extent necessary for the purpose of delivering the service,
- ii) Shall be processed in a fair and reasonable manner that protects the Privacy of the user, for purposes that are clear, specific and lawful and only for purposes specified or for any incidental purpose
- iii) Shall be retained only for the time required for fulfilling the purpose of collection unless otherwise justified by legitimate interest of the intermediary or for other legal obligations.
- iv) Shall be used otherwise in complete compliance of the data protection laws as applicable

C) **The Privacy Policy and Terms of Service** referred to under rule 1 shall be compliant with the security guidelines issued by the IN CERT as applicable to the intermediary or the category of activity to which the intermediary may belong.

Rule 4: to be modified as under:

- (4)
 - (a) The intermediary shall ensure that every user has a registered communication address through e-mail or a communication device that is verified for its correctness.
 - (b) An intermediary who provides an e-mail address or such other identity on the internet as a service, shall adopt such reasonable precautions as may be necessary to prevent impersonation.
 - (b) The intermediary shall inform its **users at least once every month, at the time of the user logging in to avail the service,** that in case of noncompliance with rules, regulations, user agreement and privacy policy for access or usage of the intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users and also remove noncompliant information.

(c) Where the user does not log in to avail the services for more than a month, a reminder as above shall be sent through E-Mail or as a message through a communication device at least once every year.

(d) Where the communication with the user through the E Mail or the communication device fails due to incorrect address of the recipient, the intermediary shall deactivate the user account until the user opts to re-activate the account.

Rule 6: to be modified

The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 **or such other security measures that may be prescribed under the data protection laws or by the Indian Computer Emergency Response Team (IN-CERT) as may be relevant.**

(P.S: Section 43A is expected to be deleted after PDPA 2018 becomes a law. Hence the Reasonable Security Practices and Procedure rules 2011 may be infructuous)

Rule 7: to be modified

The intermediary who has more than fifty lakh **registered users with identifiable location in India** or is one of intermediaries **specifically notified** by the government of India shall:

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;
- (ii) have a permanent registered office in India with physical address;
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.
- (iv) Register itself as an Intermediary with the IN-CERT with a self certified confirmation of compliance to this guideline **not later than three months** from the date of this notification with the details mentioned in para (iii) above and details of registration if any under any other law such as the data protection act if applicable.
- (v) Submit an annual confirmation about the continued compliance with updated information required to be filed under para (iv) above.

Rule 8: to be modified as under

- (a) The intermediary
 - i) 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 Act
 - ii) about any unlawful acts relating to Article 19(2) of the Constitution of India such as those in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States,

public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource, shall remove or disable access to that information without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.

(b) Further the intermediary shall preserve such information and associated records such period as may be required by the court or by government agencies who are lawfully authorised or on receipt of cancellation of the requirement by a subsequent order.

(c) Any deletion of the information under this rule without a confirmation from the relevant Court or the Government authority may be liable to be considered as destruction of evidence.

Rule 9: to be modified as under:

The Intermediary shall deploy such technology based automated tools or appropriate mechanisms, with appropriate controls, for **reasonably** identifying unlawful information or content on a proactive basis and flagging the content as **“Considered Inappropriate”**.

Such content flagged as “Considered inappropriate” shall be referred to the Grievance officer for the purpose for further action.

The Grievance officer shall record his/her views in writing and initiate further action as follows..

- (a) If the Grievance officer considers that the information is not to be flagged as inappropriate, he shall record his views as a “Compliance Note” and the information shall be retained with suitable tag as may be considered necessary and the compliance note shall be made available for any security audit by the regulatory authorities if required.
- (b) If the grievance officer concludes that the content is inappropriate, or he is unable to come to a conclusive decision to retain the same, he shall place the specific content under temporary obfuscation and refer it to the Competent Authority under Section 69 or 69A of Information Technology Act 2000 as may be relevant, for further instructions and act in accordance with the instructions received there from.
- (c) If the Competent authority does not confirm the removal of the information for a period of one week from the date of report, the information shall be reinstated.
- (d) If the competent authority confirms that the information shall remain removed, it shall be archived for legal requirement for a period not less than 3 years.

- (e) While placing any inappropriate content under temporary obfuscation or removal, the intermediary shall ensure that only the part of the content which is considered inappropriate shall be obfuscated or removed and not the entire content of which the objectionable aspect is a part.
- (f) Where there is any requirement for blocking of a large part of a content or removal of an entire URL, such decision shall be as determined by the competent authority.

Provided that this rule does not authorize the intermediary for decryption of encrypted information except under the requirement of an appropriate authority authorized under Section 69 of ITA 2000.

Rule 10: to be modified as under:

The intermediary shall initiate an effective Cyber Security incident report system that recognizes any event within its technical environment that is likely to cause harm to any user and report such cyber security incidents with relevant information to the Indian Computer Emergency Response Team within a reasonable time not exceeding 7 days from becoming aware of an incident.

Rule 11: to be modified as under:

The intermediary shall not knowingly deploy or install in or modify the technical configuration of the **user's** computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein **subject to it being installed only with the informed consent of the user.**

Rule 12: to be modified as under:

The intermediary shall institute an appropriate dispute resolution system and publish the details thereof in its website which shall include appointment of a Grievance Redressal officer whose contact details shall be provided on the website.

The Grievance Officer shall acknowledge the complaint and initiate action for redressal expeditiously and take such measures as may be necessary to resolve any Complaints received related to its service ordinarily within one month from the date of receipt of complaint.

The Intermediary may designate an appropriate "Ombudsman" to assist the user in resolving his complaint and also initiate action for "Mediation" and "Arbitration" as per the provisions of the relevant laws in India preferably through an Online Dispute Resolution system .

The applicable laws, the jurisdiction of supervisory Courts and place of offline arbitration shall be in India .

Rule 13: can be modified as under:

1. Since
 - a) there are certain advisories already issued subsequent to the issue of the Intermediary guidelines of 2011 which is presently being modified, and which are applicable to certain special categories of Intermediaries such as the need to block online Child Sexual Abuse Material, or comprehensive guidelines applicable to Cyber Cafes or Matrimonial Websites,
 - b) There would be other guidelines issued under the Proposed Data Protection Act or under E Commerce Regulations or other regulations, which may directly or indirectly be in conflict with these guidelines,
 - c) There may be other intermediary specific or sector specific due diligence guidelines that may be issued from time to time,

It is necessary to clarify as follows through modification of Rule 13 as follows:

- (i) Further to the general guidelines contained herein applicable to all intermediaries, specific advisories released in respect of special categories of intermediaries such as Online Child Sexual Abuse Material or on Matrimonial Websites or any similar notifications shall continue to be applicable even after the new guidelines come into force.
- (ii) The guidelines issued hereunder are only in the nature of minimal due diligence to be observed by intermediaries and does not restrict the legal responsibilities of the intermediary under any other Act including the Information Technology Act 2000 or such other relevant laws like Data Protection Act, Laws or Regulations related to E Commerce, Banking, Finance, Telecom, Health or Insurance information issued by the respective regulators etc.

Rule 14: to be introduced

Notwithstanding what is contained above, an intermediary at his sole option may opt to adopt the “Intermediary Dispute Resolution Policy “ (IDRP) as defined here under.

- a) The Intermediary Dispute Resolution Policy may be created and defined by a “Intermediary Dispute Management Center” (IDMC) that intends to specialize in resolving consumer disputes related to the use of Intermediary services and registered with the IN-CERT
- b) Any Intermediary can voluntarily associate itself to an “Intermediary Dispute Management Center” and adopt the Intermediary Dispute resolution Policy of that Center.

- c) The IDRP shall represent the basic commitment provided by the Intermediary for compliance of the Act and other legal obligations and may include intermediary specific policies as may be required.
- d) After adoption of IDRP the Intermediary may disclose the same in its terms and conditions and the Privacy Policy that it shall bind itself to the IDRP of the designated IDMC and that such IDRP shall also be binding on the users. It shall also inform the users that all disputes relating to the service shall be subject to the resolution through an Ombudsman/Mediator/Adjudicator as determined by the policy of the IDMC without any prejudice to the supervisory authority of any Court in India.
- e) Adoption of the IDRP as a means of defining the Terms and Privacy Policy and it may restrict its policy declarations to only the functional aspects of its service which will supplement the IDRP.
- f) Use of IDRP shall be purely voluntary on the part of the Intermediary.
- g) The IN-CERT will receive the necessary applications from intending IDMC s along with their self developed “Dispute Resolution Policy Disclosure Document” and upon satisfaction, shall list such an agency as an accredited IDMC. Such approvals will be provided by a committee headed by the Secretary MEITY and consisting of the Director General of CERT-IN with three co-opted members from the industry with adequate experience and reputation.

Rule 15: To be introduced:

Since the guidelines require certain technical changes to be implemented by the industry, it is preferable if a “Compliance Date” is fixed with a time of about 3 months given to the intermediaries to comply and report compliance.

Hence a Rule 15 shall be introduced stating

These guidelines will come into effect 3 months from the date of this notification.

For Foundation of Data Protection Professionals in India



Chairman



Shri Pankaj Kumar
Additional Secretary, Cyber Law
Ministry for Electronics and Information Technology
Government of India

23.1.2019

Dear Sir,

Subject: JUUL Labs' Comments/Suggestions on the Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018"

MIT/79/020

It is our honour to submit comments and suggestions on the Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018" (*Draft Guidelines*) prepared by the Ministry for Electronics and Information Technology (*MeitY*) and circulated for stakeholder comments on 24 December 2018.

JUUL Labs Singapore Holdco Pte Ltd. (*JUUL Singapore*) is a subsidiary of JUUL Labs UK Holdco Ltd which manufactures and sells vaping products. Vaping is an alternative for adult smokers looking to make a switch from combustible cigarette smoking. Being free from tobacco, JUUL vaping products have the potential to be a reduced harm alternative for adult smokers.

This is supported by the findings of various public health institutions and authorities. In its independent evidentiary review of the subject matter, Public Health England has categorically concluded that "Vaping poses only a small fraction of the risks of smoking and switching completely from smoking to vaping conveys substantial health benefits over continued smoking. The previous estimate that, based on current knowledge, vaping is at least 95% less harmful than smoking remains a good way to communicate the large difference in relative risk unambiguously so that more smokers are encouraged to make the switch from smoking to vaping."¹ Similarly, the National Academies of Sciences, Engineering and Medicine (NASEM) has concluded in relevant part that "there is conclusive evidence that completely substituting e-cigarettes for combustible tobacco cigarettes reduces users' exposure to numerous toxicant and carcinogens present in combustible tobacco cigarette" and there is substantial evidence that completely switching from regular use of combustible tobacco products cigarettes to vaping results in reduced short term adverse health outcomes in several organs systems."² As such, NASEM has concluded that "e-cigarettes pose less risk to an individual than combustible tobacco cigarettes" and "complete switching from combustible tobacco cigarettes to e-cigarettes would be expected to reduce tobacco-related health risk."³ Lead authors of the NASEM report on vaping, Drs. Eaton and St. Helen, also published a follow-on Evidence to Practice article, which recommended that, "if a smoker's initial treatment has failed or not been tolerated, or if the smoker refuses to use approved medications and counselling and wishes to use e-cigarettes to aid quitting, physician should encourage the smoker to switch completely to e-cigarettes. We agree with Public Health England that behavioural support should be provided to smokers who want to use e-cigarettes to help them quit smoking, and that health professionals should receive education and training in use of e-cigarettes in quit attempts."⁴

JUUL Singapore is contemplating entering the Indian market in order to sell and distribute its products within India to adult smokers. JUUL Singapore is supportive of responsible regulation in the category but is concerned that the proposed regulations will unnecessarily limit the ability for adult smokers to: (1) access information regarding certain class of products within the ENDS category, and (2) purchase specific products within the ENDS category.

¹ McNeill A, Brose LS, Calder R, Bauld L & Robson D (2018). Evidence review of e- cigarettes and heated tobacco products 2018. A report commissioned by Public Health England. London: Public Health England.

² The National Academy of Science, Engineering and Medicine, Committee on the Review of Health Effects of Electronic Nicotine Delivery Systems, Public Health Consequences of E-Cigarettes 11(2018)

³ Ibid

⁴ St.Helen, G. and Eaton, D., *Public Health Consequence of e-Cigarette Use*, 178 JAMA Internal Medicine, 984-86 (July 2018)



As such, JUUL Singapore has the following comments and suggestions on the Draft Guidelines:

A. Regarding Rule 3(2)(j) – Contents of rules and regulation, privacy policy or user agreement of intermediaries

Rule 3(2)(j) of the Draft Guidelines requires intermediaries to include in their rules and regulations, privacy policy or user agreement the condition that users of the intermediary not host, display, upload, modify, publish, transmit, update or share any information that “*threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder*”.

1. ENDS outside the scope of the Drugs and Cosmetics Act, 1940

The Draft Rule 3(2)(j) proposes that ENDS can be promoted through an intermediary to the extent that is approved under the Drugs and Cosmetics Act, 1940 (*DC Act*). However, the Drugs Consultative Committee (*DCC*) in its 48th Meeting held on 24 July 2015, held that “*E-cigarettes are not covered under the definition of the term ‘drug’ and therefore do not come under the purview of Drugs and Cosmetics Act, 1940. E-cigarettes therefore cannot be regulated under the provisions of the said Act.*”⁵ In 2018, the Central Government issued an Advisory which also acknowledged that ENDS are not, as of now, regulated under the DC Act.

There is, therefore, an inconsistency in expecting regulation for ENDS products under the DC Act, when ENDS products lie outside the scope of regulation of the said Act. Should Rule 3(2)(j) be enforced, it would create an absurdity in the law by prescribing an impossible event.

It is a well-known principle of interpretation that an amendment in the law must not lead to an absurdity in the interpretation of pre-existing laws.⁶ To that extent, Rule 3(2)(j) is not sound in law and must be suitably amended to remove references to ENDS entirely.

2. Over-regulation of product promotion

Restrictions on promotion and advertisement of consumer products already exist under laws and regulations such as the Consumer Protection Act, 1986 (*CPA*), the Advertising Standards Council of India (*ASCI*) and other sector-specific legislation. All these existing frameworks operate to prohibit false and misleading advertisements, including advertisements that give a false impression of the qualities or characteristics of a product, or make false claims about the efficacy or utility of a product, or are false and misleading in any other respect. Thus, to the extent that promotional material for ENDS adheres to these pre-existing regulations and guidelines, the content should not be further regulated.

Honest and scientific information regarding consumer products, which is verifiable as per the standards laid down under the existing laws and regulations, should be made available to the public to increase consumer awareness and to facilitate informed decision-making among consumers. Information asymmetry regarding available products takes away the right of the consumer to know what is available in the market and to make informed product choices.

The lack of information regarding a potential reduced harm alternative to combustible, tobacco-based cigarettes will also be a negation of the Rights of the Consumer under the CPA. A consumer is entitled to be assured of access to a variety of goods at competitive prices. A consumer is also entitled to information regarding goods and services in order to be protected against unfair trade practices. Making information about diverse products available to consumers is the only way to ensure such access. The absence of honest and scientific information regarding electronic vaping products will deny consumers the opportunity to access a potentially reduced harm alternative to tobacco-based cigarettes. Consumers will also be denied of the opportunity to convert from combustible, tobacco-based cigarettes to a potentially reduced harm alternative. Further, hiding information about

⁵ Please find the report of the 48th DCC Meeting [here](#).

⁶ See for example: *Shamarao V. Parulekar vs. The District Magistrate, Thana, Bombay and Ors.*, AIR 1952 SC 324.



products facilitates a scenario where misinformation will thrive, hurting the interests of both the consumer and the industry.

The freedom to carry on any trade or business is a Fundamental Right and has the full protection of the Constitution under Article 19(1)(g). Subordinate legislation in the nature of guidelines cannot abrogate the Constitution. In fact, any such abrogation of a Fundamental Right will render the guidelines void to that extent under Article 13(2) of the Constitution. To the extent that the Draft Guidelines contradict Article 19(1)(g), they will be rendered null and void in the law. Similarly, to the extent that the Draft Guidelines restrict speech under Article 19(1), they will also be found null and void vis-à-vis Article 13(2).

3. Electronic vaping products are a distinct class of products

It is important to note that, while ENDS products have been categorized in the Draft Guidelines as a single category, the ENDS category in fact includes many different types of differing products, which are not comparable and should not be grouped together for regulatory purposes.

Some ENDS products are a purely recreational or lifestyle choice, such as e-hookahs and e-shisha. On the other hand, electronic vaping products such as JUUL are a potentially reduced harm alternative that are used by adult smokers seeking to make a switch from combustible cigarettes, and are potentially useful in combustible tobacco cessation efforts.

Recent reports from the Public Health England, American Cancer Society, Cancer Research UK, Royal College of Physicians and National Academy of Sciences, Engineering and Medicines have stated that vaping is a less harmful alternatives to combustible smoking. Further, as mentioned above, Public Health England has categorically stated that vaping at least 95% less harmful than smoking and they are actively promoting it as a tobacco cessation product. In fact, Public Health England's evidentiary review, it was found that an upper bound estimate for 2017 reveals that 57,000 people succeeded in quitting smoking altogether on account of vaping. The restrictions proposed under the Draft Rules will deny adult smokers the opportunity to access information and products, which could help them in making informed decisions and switching to a potentially safer alternative.⁷

4. Recommendation

It is recommended that Rule 3(2)(j) be modified to not introduce additional restrictions on advertisements or promotional material for ENDS products that are in compliance with pre-existing laws and regulations.

In the alternative, it is recommended that Rule 3(2)(j) be modified to exclude electronic vaping products from the category of ENDS products.

B. Regarding Rule 8 – Intermediary to remove information under Article 19(2)

Rule 8 of the Draft Guidelines empowers the intermediary to “*remove or disable access to unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.*”

1. Contradictory to the Shreya Singhal Judgment

In 2015, the Supreme Court held in the case of *Shreya Singhal vs. Union of India* that neither discussion nor advocacy of an issue can be grounds to attract Article 19(2) of the Constitution. Accordingly, Section 66A of the

⁷McNeill A, Brose LS, Calder R, Bauld L & Robson D (2018). Evidence review of e- cigarettes and heated tobacco products 2018. A report commissioned by Public Health England. London: Public Health England.; See also <https://www.cancer.org/healthy/stay-away-from-tobacco/e-cigarette-position-statement.html>; <https://scienceblog.cancerresearchuk.org/2016/04/28/reducing-the-harm-of-tobacco-could-e-cigarettes-be-part-of-the-solution/>; Royal College of Physicians. *Nicotine without smoke: Tobacco harm reduction*. London: RCP, 2016; The National Academy of Science, Engineering and Medicine, Committee on the Review of Health Effects of Electronic Nicotine Delivery Systems, *Public Health Consequences of E-Cigarettes* 11(20

IT Act was struck down as unconstitutional. By seeking to remove promotional material from the internet, the Draft Guidelines are attempting a subversion of the law laid down by the Supreme Court.⁸

2. Delegation of Governmental Powers to Private Bodies

In essence, Rule 8 of the Draft Guidelines delegates constitutional powers to non-legislative, non-governmental bodies. Empowering private bodies to exercise power under Article 19(2) of the Constitution is ultra vires the delegation of power framework since the Legislature is empowered to delegate power only to administrative bodies, not to private bodies.⁹ Rather than providing specific directions on the scope of the intermediary's powers and duties, constitutional powers are being delegated to intermediaries, who are private bodies, and not accountable to the people in any way for their actions. This gives rise to tremendous scope of misuse and abuse of power, random and unfettered abrogation of the freedom of speech and expression, and will severely curtail the freedom of trade and commerce.

The Supreme Court has held that "*When the Constitution entrusts the duty of law-making to Parliament and the Legislatures of States, it impliedly prohibits them to throw away that responsibility on the shoulders of some other authority.*"¹⁰ In the present case, the entity on whose shoulders the Legislature is delegating this responsibility is not even an appropriate authority under the Constitution but a private body not accountable to the public in any way.

3. Excessive delegation

In applying the test of "excessive delegation", apart from considering the breadth of the discretion conferred by an Act to promulgate delegated legislation, the courts also examine the procedural safeguards contained in the Act against misuse of power. A completely unlimited blanket power where there is neither any guidance to the delegate, nor any procedural safeguards against improper exercise of power by the delegate, can be held invalid as excessive delegation.¹¹ In the present scenario, no procedural safeguards have been provided to users of the intermediary services against the removal of their content by intermediaries. Thus, it is submitted that, Rule 8 of the Draft Guidelines is bad in law.

3. Recommendation

The power to judge whether certain speech or expression is ultra vires Article 19(2) is a power that has been intrinsically granted to the courts. Courts are empowered to exercise due procedure and provide reasoned orders to hold find certain forms of speech and expression to be within the scope of 19(2). The power of courts cannot be usurped by intermediaries and private bodies, nor can speech be restricted arbitrarily. In light of these considerations, we recommend that Rule 8, being unnecessary, be reconsidered and diluted to the extent that intermediaries only provide logistical support in removing content that courts have, after the application of due procedure and through a reasoned order, found to be within the scope of Article 19(2).

C. Regarding Rule 9 – Automated Tools to Remove Content

Rule 9 of the Draft Guidelines provides intermediaries the power to "*deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content*".

1. Arbitrary Removal of Content without Application of Mind

Allowing automated tools to identify and remove information and content will lead to arbitrary removal of content and information which will result in a violation of both Article 19(1)(a) and Article 19(1)(g). Such an action will be the same as taking executive action without due application of mind, which is prohibited in the law. An automated tool which is identifying certain keywords on the internet and deleting content on such basis will end up removing not just promotional material but also educational information and information that has been put out

⁸ AIR 2015 SC 1523.

⁹ This position has been adopted by various High Courts. See for example: *Md. Abdur Raquib and Anr vs. Secretary, West Bengal Madrasah Education Board and Ors*, AIR 1994 Cal 122.

¹⁰ *Kishan Prakash Sharma and Ors. vs. Union of India (UOI) and Ors.*, AIR 2001 SC 1493.

¹¹ *Kishan Prakash Sharma and Ors. vs. Union of India (UOI) and Ors.*, AIR 2001 SC 1493.



in the interest of the public. This will result in complete arbitrariness and chaos in the exercise of free speech as well as conducting trade and commerce.

2. Recommendation

It is recommended that Rule 9 be amended in a manner that the automated tools only identify keywords, but the analysis and actual removal of content be carried out after due application of the human mind.

Conclusion

It is our humble submission that the Draft Guidelines be amended according to the above suggestions and recommendations. To this end, we will be happy to assist in any additional drafting exercises, or further input, as may be required.

Kind regards,

A handwritten signature in black ink that reads "Ken Bishop".

Ken Bishop
Vice-President, International Growth,
JUUL Labs

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Cc:

- Shri Pankaj Kumar, Additional Secretary, Ministry of Electronics and Information Technology (MeitY)
- Shri Gopalakrishnan S., Joint Secretary, Ministry of Electronics and Information Technology (MeitY)
- Shri Rakesh Maheshwari, Scientist G and Group Coordinator, Ministry of Electronics and Information Technology (MeitY)
- Shri Dhawal Gupta, Scientist D, Cyber Laws and E-Security Division, Ministry of Electronics and Information Technology (MeitY)

Enclosure

Detailed Comments and Recommendations

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

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

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 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:

1. Rule 3(2) – 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. Rule 3(8) – 24 Hours for 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. Rule 3(8) – 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. Rule 3(9) – 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 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 foolproof 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

² <https://indiankanoon.org/doc/127517806/>

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 age³. 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

1. Rule 3(4) – 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. Rule 3(5) – 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.*

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” A similar, parallel proviso should be inserted under sub-rule (5).

3. Rule 3(5) Enabling traceability of originators

Rule 3(5) includes 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. Rule 3(7) – 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 MeitY 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 of submission

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



ITU-APT Foundation of India

28 January 2019

MIT/79/022

**Secretary,
Ministry of Electronics and Information Technology,
New Delhi-110003**

Subject: IAFI SUBMISSIONS ON DRAFT INFORMATION TECHNOLOGY [INTERMEDIARIES GUIDELINES (AMENDMENT)] RULES, 2018

Dear Sir,

ITU-APT Foundation of India (IAFI) is a non-profit, non-political registered society, and has been working for the last 15 years in India with the prime objective of encouraging involvement of professionals, corporate, public/private sector industries, R&D organizations, academic institutions, and such other agencies engaged in development of the Indian Telecom sector in the activities of the International Telecommunication Union (ITU) and the Asia Pacific Telecommunity (APT).

The digital revolution that has been taking place over the past decade has transformed the way that society conducts itself in terms of communication, business, trade etc. Internet service providers have been responsible for increasing the access of the public to the Internet and its myriad benefits, which has seen rich dividends when we observe the growing Indian population that is now digitally connected. On the other hand, digital service providers have capitalised on the growing Internet access to provide a number of platforms and services with numerous features and functionalities to the Indian people. In other words, the combination of internet access as well as services have led to the stupendous growth of digital enterprises in the country.

In this context, the subject of safe harbour for intermediaries is a critical issue, as it allows digital service providers to continue to provide their service, innovate and grow, without being restricted by unwanted legal regimes. Safe harbour is the pivot on which intermediaries operate, as it allows them to claim immunity from illegal or unlawful activities conducted on their platforms as long as they take adequate action on such activities when notified appropriately.

Any efforts to curtail this protection would halt the progress made in the arena of digital services and hurt the digital economy. It would isolate Indians from the technological developments taking place across the world, including the fourth industrial revolution.

With this background, IAFI is deeply concerned about the Draft Information Technology [Intermediaries Guidelines (Amendment)] Rules, 2018 (“Proposed Rules”) amending the Information Technology (Intermediaries Guidelines) Rules, 2011 (“Intermediaries Guidelines”), under the Information Technology Act, 2000 (“IT Act”).

Our detailed submissions are set out below.

Rule 3(2)

Rule 3(2) of the Intermediaries Guidelines prescribes that the intermediaries’ rules and regulations, terms and conditions or user agreement should inform the users to not share, upload or otherwise publish certain categories of information. The proposed rule 3(2) expands the list of disclaimers that intermediaries must provide to their users.

These provisions are framed in a way that make their ambit highly unclear and ambiguous. There is no clarity on which content would be construed to be ‘threatening’ to public health as no clear thresholds are mentioned. By the language of this amendment, even innocent expression related to the above-mentioned subjects, such as critical information infrastructure, could be targeted as being violative of this law.

As has been settled in the Supreme Court’s judgment in the case of *Shreya Singhal v Union of India* (“Shreya Singhal”), vague restrictions on the right to free speech and expression do not qualify as reasonable restrictions as provided for under Article 19(2) of the Constitution. In this case, the Supreme Court struck down Section 66A of the IT Act because it criminalised information on ‘unconstitutionally vague’ grounds such as ‘causing annoyance’, ‘inconvenience’, etc. A similar principle could be applied in the present case, and cause it to be declared as unconstitutional.

In light of the above judgment, the proposed amendment relating to Rule 3(2) should be removed.

Rule 3(4)

The proposed rule 3(4) mandates that intermediaries inform their users that their non-compliance with the rules and regulations, user agreement and privacy policy could lead to termination of their access or usage rights *on a monthly basis*.

The requirement to inform users of this aspect of the usage conditions and not any other aspect is arbitrary, and is also onerous for the intermediaries. Intermediaries will have to repeatedly provide this information to their users, which might result in warning fatigue, thereby creating no public good. Thus, this imposes an additional obligation on intermediaries without resulting in any corresponding benefit for users. Additionally, if the objective here is user awareness, then a broad-based approach will be counter-productive as various intermediaries have been already undertaking project and

programs to make users more aware about the rules and regulations of the platform. Furthermore, technical feasibility and over all user experience also need to be taken in to consideration.

Rule 3(5)

The proposed Rule 3(5) prescribes that intermediaries must provide information or assistance in certain situations. The provision states that intermediaries must “provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto.”

We believe that this provision suffers from the following problems:

- (i) Lack of clarity: The proposed rule does not clearly formulate the obligation of intermediaries. It is not clear whether the government agencies can seek assistance relating to the grounds mentioned above or any others. Similarly, it is not clear whether any government agency can make such requests or only those that are authorised.
- (ii) Time period: The time period of 72 hours has been given to intermediaries to provide the requested information or assistance. We believe that this time period is arbitrary and should be removed, as it would not allow intermediaries to process the request adequately and seek review from the concerned government agency if required.
- (iii) Mode of communicating request: The proposed rule allows government agencies to make requests for information or assistance in writing or through electronic means. Electronic means refers to a wide variety of communication channels and would lead to the intermediaries having a high burden of checking every mode available for such communication. We believe that a specific channel of communication, which is by means of writing, should be employed for such sensitive and critical communication.

Rule 3(7)

The proposed Rule 3(7) prescribes certain liabilities for intermediaries who have more than fifty lakh users in India or have been specifically notified by the government of India. These liabilities extend to incorporation in India, establishment of permanent registered office, and appointment of persons of contact for 24x7 coordination with law enforcement agencies.

We believe that the safe harbour provisions contained in Section 79 of the IT Act are not wide enough to allow the prescription of local incorporation, and therefore, the proposed rule 3(7) is beyond the scope of the parent IT Act. As such, it does not stand the scrutiny of delegated legislation.

Further, the proposed rule creates a highly onerous burden on global intermediaries, who would not find it financially feasible to incorporate in every country of operation. Such liabilities are likely to drive these service providers away from India, thereby hurting the Indian consumers who use and consume the services provided by them.

Rule 3(8)

The proposed Rule 3(8) provides that intermediaries must remove or disable access to unlawful acts upon actual knowledge of a court order or on being notified by the government or its agency within 24 hours.

We believe that this provision suffers from the following problems:

- (i) Lack of procedural safeguards: This proposed rule creates no safeguards which would guide the government agencies in their exercise of the power to remove or disable access. As a result of this, this power may be used unsparingly and without due cause, causing injustice to the users associated with the information and records in question.
- (ii) Time period: The time period of 24 hours provided to intermediaries to comply with the take-down orders is highly inadequate as it will not allow them to appropriately respond to the requests or seek review from the government in a timely manner.
- (iii) Preservation of records: The proposed rule also mandates that the information and associated records may need to be stored indefinitely as required by government agencies, for which no procedural checks are provided.

On the whole, Rule 3(8) is framed without any due process, and thus should be removed.

Rule 3(9)

The proposed Rule 3(9) makes intermediaries liable to “deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

It is critical here to refer to section 79(2) of the IT Act, which states that the intermediary does not –

- (i) Initiate the transmission,
- (ii) Select the receiver of the transmission, and
- (iii) Select or modify the information contained in the transmission.

It is clear from the above provision that intermediaries are considered as neutral and passive bodies that only provide the platform or service. This view has been concretised in the *Shreya Singhal* case, which categorically read down any obligation on intermediaries to judge the lawfulness of any content shared on their platforms. Within this context, the proposed rule 3(9) contravenes not just the spirit of intermediary protection, but also the Supreme Court’s judgment in *Shreya Singhal*.


In addition, it should also be noted that the exercise of monitoring and censoring by intermediaries will infringe upon the fundamental right of users to express themselves freely.

In conclusion, IAFI would like to respectfully submit that the Proposed Rules would have the effect of negating safe harbour for intermediaries and expose them to excessive regulation. The restrictive provisions and onerous liabilities are likely to prove discouraging for the growth of digital services in India, thereby prematurely halting the growth of the digital economy that we have come to witness in the last few years. However, we do understand that some of the concerns raised by Ministry of Electronics and IT are important and needs to be addressed but same cannot be achieved within the

scope of Section 79 of the Information Technology Act, 2000. Thus, we are of the opinion that much more rigorous consultation with stakeholders and intermediaries should be conducted for the overall review of the Information Technology Act, 2000.

We will be happy to provide any further information of elaboration of our proposals. Ms. Aarush (+91 999 979 7700/ +91 997-134-9028/ info@itu-apt.org) GM, IAFI can be reached for any further information.

With warm regards,



**Bharat B Bhatia
President
Mobile: +91-9810173737**

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Introduction

Technology especially the Internet is a major disruptive force that is changing everything and turning every model known and unknown on its head.

At a basic level it is connecting the average citizen to information and data and empowering them in an unprecedented way. This puts all Institutions under pressure to change and adapt.

While it is my belief that intermediaries must be liable for unlawful and illegal content on their platforms, the approach to regulating Intermediaries should be carefully thought through - should **not be a one-size-fits-all approach**, nor should it be a brute force approach that causes unintended censorship and fettering of free speech and innovation.

The internet has played a key role in connecting people across the globe, enabling collaboration and allowing access to information and news on an unprecedented scale. The internet has also created opportunities for mischief makers, lawbreakers, terrorists and a whole new group of people bent on misusing the power and span of the Internet, to create disharmony and violence. The need to address this is urgent as more and more Indians get online with almost 60 Crore Indians and growing.

Safe Harbor and Intermediary Liability in a Changing World

Way back in 2007, as a member of Standing Committee on Information Technology working on Fiftieth Report on 'Information Technology (Amendment) Bill, 2006', I had anticipated the growth of Technology intermediaries and its ramifications for the real world. I had suggested that intermediaries will have to be made accountable at some point of time. I am enclosing a relevant section from that report.

Information intermediaries are no longer the companies they were when intermediary liability laws first developed, and the role of platforms in society is changing. Technological change driving much of the industry is the scale of

content and the velocity and speed of amplification of content on platforms. With the emergence of modern cutting-edge technologies like Artificial Intelligence (AI) and other tools, the intermediaries have significantly higher capabilities of preemptively filtering the unlawful content than they were in the previous years. Hence my contention that intermediaries **must no longer enjoy the safe harbor exemption** and must be made responsible for the content on their platforms to some extent. *How to regulate them and to what extent can be the subject of discussion and debate.*

Different Regulations for Different Information Intermediaries

I repeat again - While I agree that intermediaries must be liable the approach should not be a one-size-fits-all approach, nor should it be a brute force approach that causes unintended censorship and fettering of free speech.

Therefore, intermediaries must be treated differently based on their capacity and means to filter the content. The following could be the suggested categories and redefinition of intermediaries in this context.

1. Internet access and service providers (ISPs)
2. Data processing and web hosting providers which Transform data, prepare data for dissemination, or store data or content on the Internet for others
3. Internet search engines and portals which Aid in navigation on the Internet
4. E-commerce intermediaries and online aggregators which enable online buying or selling
5. Social Media and Messaging Platforms like Facebook, Twitter, WhatsApp etc (which are also described as Participative Networking Platforms and aid in creating content and social networking including Internet publishing and broadcasting platforms but do not themselves create or own the content being published or broadcast)

Proactive takedown of Unlawful Content and Traceability

The intermediaries of today are not “mere conduits” as they were in early days of internet. Intermediaries today make conscious decisions about their design to yield certain kinds of content; they closely study their users and enable micro-target advertisements at them or sell user data to others. They can leverage the knowledge they acquire about users to potentially influence their behavior. In summary they exercise significant power and influence and current regulations vis-à-vis these platforms lag their power and influence especially to be misused. Hence exempting intermediaries of this scale and capability under safe harbor regime is to stay within a bubble of unaffordable innocence.

I accept that the concern is not unjustified that the proactive obligation to remove “unlawful” content could lead to over-censorship. However, there are ways for regulations to address this. It is also necessary to ensure more competition amongst such platforms and not allow one platform to dominate the market and therefore have users multiple choices and options.

While deploying technology tools to curate the content may not be the silver bullet to curb misinformation and unlawful content, it still would be a good step towards altering the current free-for-all culture that exists in many of these platforms. It must be recognized these platforms are no longer simple technology innovations but entities that exercise tremendous influence and power that could be used positively but can also be deployed to cause harm and disruption in societies and communities in our country and around the world.

Conclusion

Technology and innovation and the change they represent is meant to be for public and societal good. But when the same is misused with intention of harm, crime, division etc. the technology intermediaries and the Government must close ranks and act decisively and robustly to ensure that our country, our democracy and our way of life doesn't get disrupted by those who wish to do so.

50

**STANDING COMMITTEE ON
INFORMATION TECHNOLOGY
(2007-2008)**

FOURTEENTH LOK SABHA

**MINISTRY OF COMMUNICATIONS AND
INFORMATION TECHNOLOGY
(DEPARTMENT OF INFORMATION TECHNOLOGY)**

**INFORMATION TECHNOLOGY (AMENDMENT)
BILL, 2006**

FIFTIETH REPORT



**LOK SABHA SECRETARIAT
NEW DELHI**

August, 2007/Bhadrapada, 1929 (Saka)

Auditing of Electronic Records

7. The Committee note that according to the representatives of the industry auditing of electronic records is desirable as per the global practice to provide some legal sanctity to these records and check frauds that are constantly occurring in corporate India. The DIT, while concurring with the appropriateness of the suggestion, have regrettably passed on the onus to the industry to find out more details regarding the global practices and standards in this regard. The Committee disapprove such an attitude of the nodal Department as they themselves should have done all the spade work in this regard. However, after interaction with the industry representatives, the Committee feel that auditing of electronic records is a pressing need in the present scenario when more and more data and records are not only being generated digitally but even the existing ones are being digitalised for excellent retention value and easy storage and retrieval. During the course of the examination, the Committee could comprehend that even DIT are not fully clear about the status of digitally generated records, albeit they being official government documents. The Committee, therefore, desire that a suitable clause be inserted in the Bill to make auditing of electronic records mandatory so that electronic records both in terms of information system and information security are accorded clarity, authenticity and legal sanctity.

Definition and role of Intermediary and liability of network service providers

(Clause 4 and Clause 38)

8. Section 2 (w) of the IT Act defines 'intermediary' with respect to any particular message as any person who on behalf of any other person receives, stores or transmits that message or provide any service with respect to that message. The Committee note that Clause 4 sub-clause (F) of the Bill now seeks to define the term 'intermediary' as any person who on behalf of another person receives, stores or transmits electronic records or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes. It also seeks to explicitly exclude 'body corporate' as referred to in Section 43(A) of the principal Act as an intermediary. The Committee also find that Clause 38 of the Bill proposes to substitute the entire Chapter XII of the principal Act whereby the intermediaries are absolved of liability in

certain cases. In some other situations, the culpability of the intermediaries has been fixed. To exercise further control over the intermediaries, Clause 38 also stipulates that they shall observe such other guidelines as the Central Government may prescribe in the matter under sub-section 4 of Section 79. After carefully going through the various proposals, the Committee are constrained to point out that the definition and role of intermediaries sought to be made through the amendments are not very clear, particularly with regard to the exclusion of body corporate referred to in Section 43 (A) of the Bill. They, therefore, desire that the Department should reexamine Clause 4 (F) of the Bill so that there is no scope for ambiguity while interpreting the definition and role of the intermediaries.

9. The Committee observe that under the existing provision of the IT Act, 2000 the network service providers are made liable for all third party content or data. But under the proposed amendments, the intermediaries/service providers shall not be liable for any third party information data, or communication link made available by them, except when it is proved that they have conspired or abetted in the commission of the unlawful act. The Department's reasoning for not making the intermediaries/service providers liable in certain cases is that a general consensus was arrived at, while discussions were going on the amendments to the IT Act, to the effect that the intermediaries/service providers may not be knowing what their subscribers are doing and hence they should not be penalised. The Committee do not agree with this. What is relevant here is that when their platform is abused for transmission of allegedly obscene and objectionable contents, the intermediaries/service providers should not be absolved of responsibility. The Committee, therefore, recommend that a definite obligation should be cast upon the intermediaries/service providers in view of the immense and irreparable damages caused to the victims through reckless activities that are undertaken in the cyber space by using the service providers' platform. Casting such an obligation seems imperative, more so when it is very difficult to establish conspiracy or abetment on the part of the intermediaries/service providers, as also conceded by the Department.

10. What has caused further concern to the Committee, in the above context, is that the Bill proposes to delete the words 'due diligence' as has been existing in Section 79 of the principal Act. The Department's logic for the proposed removal of the words 'due diligence' is the intention to explicitly define the provisions under Section 79 pertaining to exemption from liability of network service

providers. The Department have further contended that the words 'due diligence' would be covered under the guidelines which the Central Government can issue under sub-section 4 of Section 79 of the principal Act. The Committee do not accept the reasoning of the Department as they feel that removing an enabling provision which already exists in the principal Act and leaving it to be taken care of by the possible guidelines makes no sense. They are in agreement with the opinion of some of the investigating agencies that absence of any obligation to exercise 'due diligence' would place some of the intermediaries like online auction sites/market places in an uncalled for privileged position thereby disturbing the equilibrium with similar entities that exist in the offline world. The Committee also feel that if the intermediaries can block / eliminate the alleged objectionable and obscene contents with the help of technical mechanisms like filters and inbuilt storage intelligence, then they should invariably do it. The Committee are of the firm opinion that if explicit provisions about blocking of objectionable material/information through various means are not codified, expecting self-regulation from the intermediaries, who basically work for commercial gains, will just remain a pipedream. The Committee, therefore, recommend that the words 'due diligence' should be reinstated and made a pre-requisite for giving immunity to intermediaries like online market places and online auction sites.

Contraventions of serious nature (Clause 19)

11. Section 43 of the IT Act, 2000 provides for payment of compensation not exceeding rupees one crore as penalty for damages to computer, computer system, etc. It enlists eight situations under Clauses (a) to (h) where the damages are liable to be paid. The Committee note that the amending Bill proposes that the marginal heading of Section 43 be changed from 'Penalty' to 'Compensation'. An additional Clause [(i)] relating to destruction/alteration, etc. of information in a computer resource has also been added. While agreeing with the additional Clause, the Committee tend to share the apprehensions of some of the investigating agencies regarding gravity of contraventions enumerated in Clauses (c) to (i). These contraventions are of serious nature and may have calamitous consequences in many cases, more so where Intellectual Property Right (IPR) or related aspects and security matters are involved. They, therefore, feel that merely a compensation not exceeding one crore rupees may not suffice. The Committee, therefore, desire that Clauses (c) to (i) of Section 43 be made cognizable offences punishable with

Dear Sir/Madam,

We are grateful to the ministry for having published the Draft Information Technology (Intermediary Guidelines Amendment) Rules, 2018 (hereinafter, "Proposed Amendment") and for having initiated a public consultation process on them.

In this letter, we outline some information about Change.org, the impact the Proposed Amendment is likely to have on our activities and why we think the Proposed Amendment requires a serious rethink.

About Change.org

Change.org is the world's largest petition platform with over 220 million users globally. Our mission is to empower people everywhere to create the change they want to see, and our vision is a world where no one is powerless.

In India we have over 1.5 crore (15 million) users who have used Change.org to start or sign petitions on the most pressing issues in their lives and communities. Change.org is a non-partisan, open platform that empowers *anyone* to campaign on *any* issue, regardless of their political views -- as a result, there is an extremely wide range of petitions available to sign on the website. There are petitions about political, social, and economic issues, alongside petitions about entertainment, sports, and popular culture; Change.org is a perpetual snapshot of what Indians are working hard to change at any given moment.

As a company, we don't take a position on specific issues or petitions. This means that a politician or CEO who is addressed as the recipient of a Change.org petition can trust that it represents the voice of people from a great diversity of backgrounds, rather than one constituency or advocacy group.

Change.org users' impact

The impact of Indians using Change.org has been tremendous. Below are just a few of the inspiring stories of the Indians who have used Change.org to start and win successful petitions.

Subarna Ghosh www.change.org/Safebirth

Twenty years ago, Mumbaikar Subarna Ghosh experienced a forced c-section. The unnecessary surgery left her scarred for life, both physically and emotionally. She quit her job as a journalist and started researching on women's childbirth experiences. After

change.org India

meeting other mothers who had similar experiences, started a campaign to decrease the high number of dangerous, unnecessary cesarean deliveries in India. [Her campaign](#) was supported by over 3lakh people and the online space became a forum where thousands of India women shared their own stories. Subarna met the [Union Minister for Women and Child Development](#) and handed over the petition to her. Because of Subarna's campaign, the Union Health Ministry sent a directive to all the states to curb down unnecessary caesareans. The [Union Health Ministry also mandated](#) that all hospitals empanelled under the CGHS have to declare their caesarean section rates to the public. Subarna is also part of a Maharashtra State committee on C-sections, and has started her own organisation.

Priyanka Gupta www.change.org/SingleParentPassport

In India, children of single mothers were often unable to obtain passports due to complicated rules requiring recognition of the father. Priyanka Gupta, a single mother, started a [Change.org campaign](#) to simplify the rules and recognize single mothers as sole guardians in passports.

Priyanka's petition also spurred several single women to share their stories and generated significant national media attention. Minister Maneka Gandhi [responded](#) to the campaign by contacting the Ministry of External Affairs. A joint committee was set up with WCD and MEA reconsidering the rules for single parents. In December 2016, the MEA then announced new simplified passport rules recognizing single parents as sole guardians in Indian passports. The WCD Ministry officially [announced this victory on Priyanka's petition](#)

Insia Dariwala www.change.org/EndTheIsolation

In end of 2017, Insia Dariwala, a filmmaker from Mumbai, started her campaign asking the Women and Child Ministry to [Order an in-depth study on male child sexual abuse in India #EndTheIsolation](#). The Women and Child Development Minister [sent this DM response](#) on her petition. She promised to ensure that India's child protection laws were gender neutral. The media picked up this [impact story as headlines](#). Insia is working with the Ministry in executing this research which will hopefully form the foundation of many policy changes in years to come. Months later, the Ministry of Women and Child Development followed up on this campaign by urging all states to extend [equal compensation for boy survivors of child abuse](#).

Impacts of the Proposed Amendment

Change.org qualifies for and requires protection as an intermediary under Section 79 of the Information Technology Act, 2000 and is governed by the Information Technology [Intermediaries Guidelines] Rules, 2011. The Proposed Amendment therefore has a direct impact on Change.org and its operations servicing its India userbase.

Change.org notes with serious concern the chilling effect that the Proposed Amendments are likely to have on Indian citizens in general and the Indian users of Change.org in particular. Change.org also is of the opinion that some of the provisions in the Proposed Amendment lack precision and certainty that a compliance standard typically requires.

Chilling Effect

All Indian citizens have a constitutionally protected fundamental right to free speech. It is also their right and legitimate expectation that such constitutional protection extends to their online speech.

The importance of freedom of expression is something that users of Change.org value highly, in their use of a platform where anyone can engage in bringing people together to effect change on issues that matter to them. Change.org's interests are aligned with the interests of its users in not only upholding and promoting their free speech online, but also ensuring that any measures that cause any uncertainty, consequently having a chilling effect on the exercise of the right to free speech are counteracted.

Accordingly, Change.org recommends that the following provisions in the Proposed Amendment be removed or further modified as suggested herein.

- The proposed amendment to Rule 3 on the obligations of the intermediary (e.g Change.org), particularly the addition of item (k) under Sub-Rule (2) that in effect provides that the users may not post any information "*that threatens critical information infrastructure*" is too vague as a standard. For instance, several legitimate campaigns such as [this one](#), which brings to the fore security concerns (whether real or otherwise) of India's Aadhaar database, which is currently classified a CII could be repelled because of the Proposed Amendment. Change.org suggests that this item may perhaps be amended to state "*threatens to compromise or tamper with.*"
- The proposed amendment to Sub-Rule (5) of Rule 3 and the addition of

change.org India

Sub-Rule (8) effectively authorising “*any agency*” of the State to require information and cooperation from intermediaries, including turning over personally identifiable information of their users is overbroad. It is suggested that such powers be vested only with certain enumerated list of agencies and with each of them only for specific purposes. To prevent misuse, it is further suggested that such powers be vested only with certain designated high ranking officials of those agencies.

- The proposed to addition of Sub-Rule (8) that obliges the intermediaries to, in effect, police the content based criteria such as “*sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence*” lacks necessary precision and certainty. Change.org understands and acknowledges that such criteria repeat a similar enumeration in Article 19(2) of the Constitution. However, Change.org is of the view that such broad criteria to test the constitutionality of legislations, typically by a judicially trained mind, cannot be applied for the purpose of routine operational compliance. It is suggested that this change be done away with.

Automated Content Control

The requirement to deploy technology and automated tools for content control such as “*proactively identifying, removing and disabling*” content (proposed addition of Sub-Rule 3(9)) is a grave threat to freedom of expression. Users have a legitimate expectation from platforms such as Change.org that the content control decisions are clearly reasoned by human beings, who are best equipped to make such complicated decisions.

A fully automated decision making on content access and control, even if the technology were to evolve beyond its present-day limitations in the near future, requires a serious rethink. Firstly, developing effective technology will not always be practical for small start-ups that host user-generated content. Furthermore, maintaining and improving such technology to adapt and meet changing patterns of Internet use and abuse requires further significant investment. Finally, there are few providers of such tools in the market that platforms could integrate into their own. These factors make the regulatory mandate to use such tools completely untenable.

Regulatory Burden

The Proposed Amendment places significant barriers and regulatory burden on a several non-partisan intermediaries including Change.org that empower Indian citizens to have their voice heard in the process of public reason on several key issues.

For instance, the provision in Sub-Rule (4) casts a duty on the intermediaries to inform their users effectively reminding them of the limitations to their rights “*at least once every month.*” This is not only too frequent and may cause user fatigue, but also may end up not achieving the objective as users may get into the habit of not carefully noticing the contents of such frequent communication.

The proposed turn-around-time (TAT) of 72-hours in Sub-Rule 3(5) and 24 hours respectively in Sub-Rule 3(8) do not distinguish the requests based on priority or purpose. It is suggested that these provisions should recognise a gradation of priority and urgency among requests and fix maximum TATs accordingly. For instance, the 24-hour turn-around threshold may be retained in the case of a national security related need and perhaps a two-week TAT in the case of a defamation related request. In the case of Sub-Rule(5), Change.org urges the ministry to also consider having separate TATs for acknowledgment of the request and the furnishing of the requested information.

Change.org, with more than 50 Lakh Indian users would qualify for being governed by the provisions of Sub-Rule 3(7) in the proposed amendment. It is suggested that it be clarified that the 24x7 need is only an on-demand basis and that the contact information of the nodal officer would only be registered with the specific enforcement agencies and not made public, in the interests of the privacy of such person.

Thank you,

Nida Hasan

Associate Country Director,

Change.org India

nida@change.org



**COMMENTS AND SUGGESTIONS ON THE DRAFT OF THE
INFORMATION TECHNOLOGY [INTERMEDIARY GUIDELINES
(AMENDMENT) RULES] 2018**

Submitted to

Ministry of Electronics and Information Technology

Submitted By

BananaIP (BIP) Counsels

Contact Person: Ashwini Arun

Email ID: contact@bananaip.com

CONTENTS

S. No.	TITLE	PAGE NO.
1.	INTRODUCTION	3
2.	DETAILED COMMENTS AND SUGGESTIONS	4
	Rule 3(2)	4
	Rule 3(4)	5
	Rule 3(5)	7
	Rule 3(7)	9
	Rule 3(9)	11
	Rule 3(10)	12
	Rule 3(12)	13
3.	GENERAL COMMENTS AND SUGGESTIONS	15
4.	ABOUT BANANAIP COUNSELS	16

INTRODUCTION

The Ministry of Electronics and Information Technology (MEITY) issued a [notification](#) on 24th December 2018 publishing the draft Information Technology (Intermediary Guidelines) Rules 2018 to replace the rules notified in 2011. The notification, published on the MEITY website, invited comments and suggestions on the draft rules. We are submitting our recommendations and suggestions to the Ministry, and await positive changes in the proposed rules.

We appreciate the Ministry's recognition of the widespread misuse of social media platform to spread fake news, and the Ministry's resolve in drafting these rules to strengthen the legal framework to make intermediaries more accountable under the IT Act, 2000.

We have noticed that certain provisions of the proposed rules are ambiguous and insufficiently detailed and hence suggested a few changes.

Rule 3 (2)

Such rules and regulations, **privacy policy** terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

- (a) belongs to another person and to which the user does not have any right to;
- (b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
- (c) harm minors in any way;
- (d) infringes any patent, trademark, copyright or other proprietary rights;
- (e) violates any law for the time being in force;
- (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
- (g) impersonates another person;
- (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
- (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.
- (j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;**
- (k) threatens critical information infrastructure.**

Comment

The Rule does not contain any provision requiring the intermediary to prohibit the user from hosting, displaying, uploading, modifying, publishing, transmitting, updating or

sharing any information which is false, fake, untruthful, misleading, and intended to deceive. The failure to incorporate such a provision, or the decision to leave to the intermediary the incorporation of such a provision in the user agreement, is completely inconsistent with the stated purpose of the amendment in the Rules, i.e. to “strengthen the legal framework and make the social media platforms accountable under the law”. This is particularly inconsistent as these Rules were framed in response to a motion to call attention to the “Misuse of Social Media platforms and spreading of Fake News” and intended to convey the “resolve of the Government” to address the issue.

To address this issue, the Rule may be amended to include the following:

Such rules and regulations, **privacy policy** terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a)....

(k)...

(l) is false, fake, untrue, misleading, and intended to deceive the recipient of the information. Explanation: A recipient is any legal or natural person who has lawful access to the information.

Rule 3 (4)

The intermediary shall inform its users **at least once every month**, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.

Comment

The Rule vaguely states that the intermediary should inform its users regarding the consequences of non-compliance with its policies “at least once a month”. It does not state the mode or manner of providing this information or notice to the user.

The Rule does not impose any liability/obligation on the intermediary to take express consent from the user at any time, including when the intermediary updates its policies. Thus, it does not specify whether a mere notification on the intermediary’s platform is sufficient, or whether the intermediary is required to make the user proceed with using the platform only after clicking on “I Agree”.

It is recommended that the Rule be amended to require the intermediary to provide express notice to users on the platform itself and through the communication channel chosen by the user. The Rule should also require the intermediary to take express consent from a user whenever he/she first accesses the intermediary’s services, and at each instance when the intermediary updates or amends its policies. This will make the intermediary’s functioning more transparent and make its policies more accessible to the user, and will ensure that users are better informed about the policies they are required to comply with.

The Rule does not impose any obligation on the intermediary to terminate the account or usage rights of a user who does comply with the intermediary’s policies. The Rule also does not require the intermediary to take any specific action against users who repeatedly violate the intermediary’s policies.

It is recommended that the Rule be amended to require the intermediary to take action against users who repeatedly and frequently violate the intermediary’s policies. Such an amendment will also restrict the intermediary from abusing its discretion to not act against users for its own commercial benefit.

Further, the Rule also does not specify whether the intermediary has the right to terminate only specific usage rights of a non-compliant user, or impose any obligation on the intermediary to terminate only certain specific usage rights. For instance, a user who repeatedly violates the intermediary's policies while publishing information may only be barred from publishing content and not from accessing content published by other users.

It is recommended that the Rule be amended to allow the intermediary to terminate the user's access to certain services based on the previous violations by the user. This will give the intermediary greater autonomy, while still requiring appropriate action on its part, and will also not be unjust towards the user.

Rule 3(5)

When required by lawful order, the intermediary shall, **within 72 hours of communication**, provide such information or assistance **as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto.** Any such request can be made in writing **or through electronic means** stating clearly the purpose of seeking such information or any such assistance. **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.**

Comment

- The Rule requires an intermediary to provide the requested information or assistance only in the following cases:
- asked for by any government agency or assistance concerning security of the State or cyber security

- investigation or detection or prosecution or prevention of offence(s)
- protective or cyber security and matters connected with or incidental thereto.

This list of circumstances is narrow and restrictive, despite the open-ended clause specifying “matters connected with or incidental thereto”, and does not cover all instances/cases in which the intermediary’s assistance may be required. For instance, in cases of IP infringement, invasion of privacy or defamation, the intermediary’s assistance may be required to determine the source of the infringement and the channels of transmission.

It is recommended that the Rule be amended to include the other circumstances in which the intermediary’s assistance may be required, and that a more flexible timeline be allowed for assistance in circumstances not already specified in this Rule.

The Rule does not define or clarify what the term “protective” means, in the context of “protective or cyber security and matters connected with or incidental thereto.”

The Rule does not clarify the meaning of the term “Communication” when requiring intermediaries to provide the required information within 72 hours. Specifically, the Rule does not state whether the limit of 72 hours applies to the communication of the lawful order or the communication of the request for information by the government agency to the intermediary.

It is recommended that the Rule clarify the meaning of the term ‘Communication’ and the associated time limit, such that intermediaries have 72 to provide the information after the request of the authorised government agency has reached the intermediary.

The Rule requires an intermediary to enable tracing of the originator on the platform as required by an authorised government agency. However, the Rule does not clarify whether the intermediary is required to trace the information in all forms or only in a

single form. The information in question may be found in various forms (text, image, video, etc) on the intermediary's platform, and the original originator for each form might be different or not linked to the originators in other forms.

For instance, information which is likely to incite violence or which disparages persons of a particular religion or community, may be present in the form of a message/comment (text), a screenshot of the text (image), or a recording of a person reading the text (audio and/or video). In such cases, the intermediary may not be technologically equipped to trace the originators in each form.

It is recommended that the Rule be amended to clarify the extent to which the intermediary is required to enable tracing of the originators, and whether the tracing extends to all forms in which a specific piece of information may be shared.

Rule 3(7)

The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;
- (ii) have a permanent registered office in India with physical address; and
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.

Comment

A user as defined in the Intermediary Rules, means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing,

transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary.

The Rule requires that an intermediary which has more than 50 lakh users in India comply with certain conditions. This pre-condition raises the following issues:

- The broad definition of the term “user” may lead to past users of the intermediary being included for the purpose of determining whether the intermediary has 50 lakh users, thus leading to a misleading calculation.
- The Rule provides no guidance on how the number of users is to be calculated, i.e. whether this number is measured through number of active current users, number of unique visitors to the intermediary’s platform, number of downloads/installs (for a mobile platform), or any other metric.
- The Rule does not specify a time limit within which an intermediary is required to comply with the specified conditions after reaching 50 lakh users.
- The Rule has not specified how the number of users is to be calculated, it does not specify whether an intermediary is required to comply with these conditions the first time it reaches 50 lakh users, and whether it has to continue complying with these conditions irrespective of a future drop in the number of users.
- The Rule does not specify how the term ‘in India’ is to be interpreted.
- The Rule does not specify any reasoning through which the number of 50 lakh users has been determined as the prerequisite for having to comply with the conditions mentioned.

It is recommended that the Rule be amended to clarify how the number of users is to be measured, the time within which the intermediary is required to comply with these conditions after reaching the specified number of users, and how the Rule will apply to intermediaries with vast fluctuations in the number of users.

It is also recommended that the Rule be amended to impose these conditions on intermediaries with less than 50 lakh users, as this number is too high to include other platforms which have a wide userbase but are not required to comply with this Rule.

The Rule does not specify the minimum qualifications required for the “nodal person of contact” or the “alternate senior designated functionary.”

It is recommended that the Rule clearly specify the minimum qualifications of the nodal person of contact and the alternate senior designate functionary, either in terms of objective qualifications like age and education, or in terms of seniority within the organisation of the intermediary.

Rule 3(9)

The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

Comment

This Rule imposes a positive obligation on the intermediary to monitor all content made available on its platform, to enable it to identify and remove all unlawful information or content. However, the Rule does not define the meaning or scope of the term “unlawful information or content.” The Rule does not clarify whether “unlawful information or content” implies any content in contravention of Rule 3(2)

Further, the Rule does not state how an intermediary may determine which content is unlawful. The question of whether content is defamatory, whether it violates the intellectual property or privacy rights of a third party, whether it harms minors or is likely to incite violence, or whether it violates any other laws in force is a question of both fact and law. Any such question may be properly decided only by a competent

court of law, not by an intermediary. The imposition of such an obligation on the intermediary not only unreasonably burdens the intermediary, but also leaves a judicial/quasi-judicial determination to a corporation. The Rule does not lay down any standards which the intermediary may employ to determine which content is unlawful, not does it impose any obligation to strictly adhere to those standards and not remove lawful content.

It is recommended that this Rule be deleted from the Draft Rules, as it neither addresses the problem of fake news, which these Rules seek to address, not does it provide any clear guidance to either intermediaries or third-parties on how unlawful content is to be handled.

Rule 3(10)

The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team (I-CERT).

Comment

This Rule requires the intermediary to report cyber security incidents and share information related to such incidents with the Indian Computer Emergency Response Team. However, the Rule neither defines what constitutes a cyber security incident, not does it specify the time within which the intermediary is required to report such incidents to the I-CERT.

It is recommended that the Rule be amended to clarify the meaning of the term 'cyber security incident', and specify the time within which the intermediary must share reports and information related to such incidents with the I-CERT, based on the magnitude and seriousness of such incidents.

Rule 3(12)

The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule (3) can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

Comment

This Rule requires an intermediary to publish information on how users or third-parties may contact its Grievance Officer, and requires the Grievance Officer to redress a complaint within one month from the date of its receipt.

The Rule does not clarify the process through which an intermediary is required to handle a complaint. The Rule does not impose any obligation on the intermediary to display its policy of handling complaints and the required information, to make a form available for submitting complaints and other necessary information, to investigate the complaints in a certain manner depending on the nature of the complaint, to take any action based on the complaint (including removing or disabling access to the content in question), or even to respond to the complaint within a specified time, with or without the details of any action being taken based on the complaint. The Rule does not specify how the intermediary is required to investigate a complaint, what are the minimum qualifications of the person in charge of handling complaints, and what are the minimum qualifications of the Grievance Officer. The Rule does not specify whether the intermediary is required to immediately acknowledge the receipt of complaints, and the time within which it is required to request any other information which it requires in order to act on the complaint. The Rule also does not specify which types of complaints the intermediary is required to address immediately, as some complaints (for instance,

related to privacy violations) may be time sensitive and thus requiring removal of the content within a few hours.

The Rule also does not impose any obligation on the complainant to submit a complaint containing all necessary information, including the link to the content in question. The Rule does not specify a time within which the complainant is required to submit such information after receiving a request for the same from the intermediary.

The Rule fails to address situations in which a complainant does not submit all necessary information despite repeated and timely requests from the intermediary, or situations in which an intermediary does not act on a complete complaint within the specified time, and instead delays its response by asking for unnecessary information.

It is recommended that the Rule be amended to include a framework which every intermediary is required to adhere to while handling complaints. It is recommended that this policy require the intermediary to display its own complaint redressal policy in accordance with the Rules, and handle complaints accordingly. Accordingly, it is recommended that the Rule should prescribe the process to be followed for investigating complaints, for acknowledging complaints and communicating developments in the investigation to the complainant, and the action to be taken based on the investigation.

It is recommended that the Rule be amended to require the complainant to submit certain information, in the absence of which the complaint will not be treated as complete and valid, and the intermediary shall be under no obligation to address such complaint. It is further recommended that the Rule be amended to impose a time limit only after the intermediary receives all the information specified in the Rule, and that the amended Rule impose different time limits based on the nature of the complaint, and allow a shorter window to address time-sensitive complaints.

GENERAL COMMENTS AND SUGGESTIONS

Many intermediary entities function as e-commerce platforms within the meaning of the term under the FDI Policy in E-commerce (2018), or as data fiduciaries within the meaning of the term under the Personal Data Protection Bill, 2018.

The Draft Intermediary Rules do not address issues arising when intermediaries operate as data fiduciaries and e-commerce platforms. To address issues arising therein, it is recommended that the Rules be amended such that:

- An intermediary will be required to allow users to delete their accounts and all personal data in the possession of or under the control of the intermediary.
- An intermediary will not be allowed direct involvement in the activity for which it is an intermediary platform, in order to create a level-playing field for all entities. For instance, e-commerce entities shall not be allowed to sell their own products, and content aggregators shall not be allowed to also create content of the same genre.
- An intermediary will not be allowed to promote specific products or content except in accordance with objective, measurable criteria like frequent consumption or a highly rating by bonafide users. The intermediary will be allowed to run advertisements purchased by advertisers, including for promoting products/content searched by the user.
- An intermediary will not be allowed to determine the price of a product/service on its own, as this may lead to favourable pricing for specific products, which also may contribute to a non-level playing field.
- An intermediary will be required to take more stringent measures to monitor the nature of not only content on its platform, but also the nature of the users, to avoid fake reviews, ratings, likes, and other measures of the popularity of products, services and content.

ABOUT BANANAIP COUNSELS

BananaIP Counsels is a renowned, premier intellectual property (IP) firm based in Bangalore. Its attorneys have extensive experience advising intermediaries and representing individuals and companies in their interactions with intermediaries.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

THE INDIAN MUSIC INDUSTRY

266, Kaachwala Bldg. 2nd Floor, Dr. Annie Besant Rd., Opp. Old Passport Office, Worli, Mumbai -400 030
 Tel. : +91 22 6660 8349 / 8350 • Website : www.indianmi.org

29th January 2019

Shri Pankaj Kumar,
 Additional Secretary,
 Cyber Laws & E-Security Division,
 Ministry of Electronics and Information Technology
 (Government of India)
 Electronics Niketan, 6, CGO Complex,
 Lodhi Road, New Delhi - 110003

Subject: Comments on the Draft of Intermediary Guidelines, 2018

Dear Mr. Kumar,

The Ministry of Electronics & Information Technology (Ministry) has recently issued *The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018* (2018 Rules). We, the Indian Music Industry aka IMI, on behalf of our Members, seek to make certain remarks. IMI represents the business and trade interests of Indian recorded music companies on a pan-India basis. IMI is affiliated with the International Federation of the Phonographic Industry (IFPI), an organisation representing the interests of the recording industry worldwide. IMI Members hold an extensive repertoire of protected intellectual property, including copyright protected works.

One of the major concerns of IMI is reducing piracy in India. Piracy has severe negative effects to the global creative copyright industry, including in India. According to Shridhar Subramaniam, president of Sony Music India, music piracy causes a loss of ~ INR 1500 Cr. to the Indian recorded music industry, annually.¹ According to the IFPI – IMI Digital Music Study 2018, 76% of Indian internet users pirated music online in the previous three months.² There has been an increase in the content consumption in line with the increased penetration of

¹ Dialogue 2018 – Vision 2022

² IFPI – IMI Digital Music Study 2108. Page 3. <http://indianmi.org/be/wp-content/uploads/2018/10/Digital-Music-Study-2018.pdf>

smartphones and cheaper data charges in India.³ A report estimates that large pirate websites operating in India can earn up to USD 4 million annually.⁴

Digital piracy is also a national security threat. Websites hosting pirated content often surreptitiously install malware on users' computers that collects personal information which is subsequently misused. Pirate websites have been linked to forms of cyber-crime, fraud and terrorism. Furthermore, these websites often also display prohibited advertisements.

IMI welcomes the introduction of the 2018 Rules as it provides an opportunity to modernise the intermediary liability law in India. In addition to some general remarks, IMI has specific concerns relating to Rule 3(3) regarding safe harbour and the removal of Rule 3(4) of the 2011 Rules, as well as recommendations relating to Rule 3(9) in the 2018 Rules, all of which are elaborated below.

General remarks

The Information Technology Act 2000 law defines "intermediary" broadly: "with respect to any particular electronic message, any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message".

The breadth of this definition means that care must be taken in relation to the 2018 Rules such that liability privileges and/or other benefits and obligations of the regime are not applied to types of service for which they are not intended.

In addition, naturally, intermediary liability limitations only make sense if the underlying liability for the relevant wrongful or tortious act is clearly established. As regards to copyright infringements, it is essential that the 2018 Rules set out clear rules on primary and/or secondary liability for intermediaries that engage or whose services are used in copyright infringing activities.

³ E&Y FICCI Media and Entertainment Industry Report 2017. Page 188

⁴ FICCI – SIPI – VeriSite. Badvertising: When Ads Go Rogue. Page 5.
https://www.creativefirst.film/show_pdf/74

The Scope of Online Intermediary Liability Privileges (aka Safe Harbours)

Any intermediary safe harbours should be limited to technical, automatic and passive intermediaries and on the condition that they operate in the manner expected of a diligent economic operator to prevent the availability of infringing content on their platforms.

Safe harbours were introduced to protect service providers that provide essential technical infrastructure for the internet so that it could develop without an unreasonable burden of liability. With the benefit of safe harbours, the online sector has grown exponentially.

However, in recent years safe harbours have been relied upon by entities that bear little resemblance to essential infrastructure providers – these include so called user upload services (such as YouTube) that actively curate, promote and monetise content their users upload on their platforms. This deprives copyright holders of fair revenues and gives these services an unfair advantage over other digital music services which license directly from right holders. This market distortion, known as the ‘Value Gap’, has been recognised by the EU, where draft legislation to clarify that active user upload services are (i) engaging in copyright restricted acts and (ii) cannot benefit from safe harbours for the content they make available, is at an advanced stage.

In terms of the specific drafting, IMI proposes that Rule 3(3) of the 2018 rules should include the words “*or otherwise provide access to*” after “*host or publish*” in line 1. A further sentence at the end of Rule 3(3) should clarify that the exemption applies only if all such activities of the intermediary are of a technical, automatic and passive nature and that it does not apply to any service playing an active role in respect of content on or passing through its service.

Additionally, to ensure that all intermediaries are required to comply with the due diligence obligations set out in the 2018 Rules, IMI proposes that the safe harbour provision at section 79 of the Information Technology Act 2000 should be amended to read “...*if he proves that the offence or contravention was committed without his knowledge AND [replacing OR] that he had exercised all due diligence...*”



The removal of the notice and take down provision

IMI is extremely concerned that the deletion of Rule 3(4) of 2011 Rules from the 2018 Rules will facilitate digital piracy in India. Rule 3(4) of the 2011 Rules mandates intermediaries to take down any content falling within Rule 3(2) pursuant to a notice given by an affected person. Thus, IMI Members can issue a notice to intermediaries to remove infringing content as specifically listed in Rule 3(2)(d) of the 2011 Rules (replicated in the 2018 Rules).

As per the 2018 Rules, infringing content can only be removed pursuant to a court order or a government direction. In the 2018 Rules, content falling within Rule 3(2) can only be removed pursuant to Rule 3(3)(b) of the 2018 Rules. Rule 3(3)(b) of the 2018 Rules provides a safe harbour protection to intermediaries only if they remove infringing content pursuant to a court order or a government direction. Rule 3(3)(b) of the 2018 Rules does not allow IMI Members to issue a notice to the intermediaries to remove infringing content.

Effective notice and take down is an essential remedy for the creative industries to try to limit the distribution of infringing content posted online. This is especially the case in respect of content made available prior to its commercial release date ("pre-release" content). Every minute that pre-release content remains online undermines the investment made in producing, developing and marketing content protected by copyright. By way of example of the scale of the need for notice and take down, in 2017, the international music industry body IFPI sent over 11 million individual URL take down notices to over 6,700 different websites requesting the removal of content which infringed copyright.

Accordingly, safe harbour legislation must include a specific obligation to take down content if the intermediary becomes aware of facts or circumstances, or should reasonably have been aware of facts or circumstances, from which the infringing activity is apparent. This type of "red flag" knowledge should not only arise from a take down notice sent by a right holder but should be characterised by reference to steps a diligent economic operator would be expected to take in the circumstances. In addition, "notice and take down" should mean "notice and stay down": on receipt of a notice, service providers should be obliged to take reasonable steps to ensure that all other copies of, or URL links to, infringing content: (a) are also removed; and (b) do not appear in the future. This is an appropriate and proportionate obligation which could be effected using existing, affordable technologies.

The 2018 Rules will lead to greater availability of infringing content owing to the additional time, resources and cost required in obtaining the requisite court order or government direction, as required under Rule 3(3)(b) of the 2018 Rules. Thus, the 2018 Rules as currently drafted will increase the availability of infringing content exponentially in India. The additional hurdle imposed in having to obtain a court order or government direction is particularly critical in cases of a new release of a copyright work (including pre-release content, described above) because the bulk of the monetisation happens within the first few hours, days and weeks of the release of the sound recording.

IMI firmly believes that the proposed 2018 Rules must re-introduce the deleted Rule 3(4) of 2011 Rules. According to footnote 1 of the 2018 Rules⁵, Rule 3(4) of the 2011 Rules is to be deleted pursuant to the judgment given by the Supreme Court in *Shreya Singhal v. Union of India* dated 24.03.2015. The judgment in *Shreya Singhal v. Union of India*, however, only dealt with offensive messages falling within Rule 3(2)(b)⁶ of the 2011 Rules and the consequent punishment under Section 66A of the Information Technology Act, 2000. The judgment does not deal with hosting of infringing content on the internet. As seen above, the 2018 Rules in its existing form will dramatically increase digital piracy in India. The deletion of Rule 3(4) of the 2011 Rules in 2018 Rules gravely harms the interests of IMI Members, as well as the whole of the creative content industry. Consequently, Rule 3(4) of 2011 Rules, deleted in the proposed 2018 Rules, should be reintroduced.

The obligation to deploy automated tools to identify and remove content

The introduction of an obligation in sub rule 3(9) of the 2018 Rules to deploy automation tools to identify and remove unlawful content is positive step forward for the intermediary regime. Such automated tools are already commercially available at affordable cost and widely utilised by service providers.

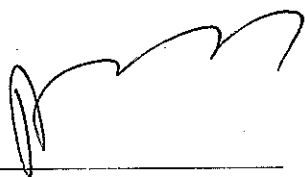
⁵ Footnote 1 of the 2018 Rules states that: "This sub-rule has been modified as per Supreme Court Judgment in the matter of Shreya Singhal Vs UOI dated 24.03.2015."

⁶ The intermediary shall observe following due diligence while discharging his duties, namely: Such rules and regulations, privacy policy or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that: is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

IMI has two recommendations in relation to Rule 3(9). Firstly, IMI believes that the provision would be clarified (and the creative industries would immensely benefit) if the rule explicitly specified that 'unlawful content' under Rule 3(9) includes *inter alia* content which infringes intellectual property, for example, by adding the words "of the type specified in sub rule 3(2)" at the end of the Rule 3(9) provision. Secondly, IMI is concerned that intermediaries may escape legal liability owing to the lack of an enforcement provision for Rule 3(9) in the 2018 Rules. IMI strongly believes that the 2018 Rules must make intermediaries liable for each and every violation of Rule 3(9) as well as every other rule of the 2018 Rules.

Despite our concerns, as noted above, the 2018 Rules are a positive first step towards the modernisation of intermediary law in India. IMI would welcome an opportunity to make an in-person representation of its concerns before the Ministry and/or to provide further written information in relation to any questions arising.

Yours sincerely,



Blaise Fernandes

President & CEO

The Indian Music Industry

Comments on draft amendments to the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 submitted to the Ministry of Electronics and Information Technology.

We wish to draw the attention of the Ministry to three issues:

1. Intermediaries are required to prohibit publication of certain types of content on their platform such as those threatening public health or safety. This may violate the right to free speech under Article 19(1)(a) of the Constitution.
2. Intermediaries are required to deploy automated tools for identifying and removing access to unlawful information or content. The requirement under this provision may be contrary to the reasoning of the Supreme Court in a recent judgement.
3. Intermediaries with more than fifty lakh users must incorporate a company in India. It is unclear as to how the number of users will be calculated for the purpose of the rule. Therefore, an intermediary will find it difficult to determine whether it is required to set up a company in India under this provision.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
(Published by MeitY)

1. Prohibition of content in the user agreement or privacy policy

[Rule 3(2)]

Rule 3: The intermediary shall observe following due diligence while discharging his duties, namely: --

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, privacy policy or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that –

...

(j) threatens public health or safety...

Issue: Intermediaries are required to prohibit publication of certain types of content on government request. This may violate the right to free speech.

The Rules provide that the intermediary must prohibit publication of certain types of content in its user agreements. The Draft Rules prohibit a new category of information which threatens 'public health or safety'.

This may violate Article 19(1)(a) of the Constitution which guarantees the right to free speech and expression. As provided under Article 19(2), this right may be restricted on six grounds, including in the interest of public order, or national security.

The new category of information which threatens 'public health or safety' may not meet the requirement of Article 19(2). The Supreme Court has clarified that threat to public safety (which has been read to include public health) cannot be a ground to restrict the freedom of speech. The Court stated that any restriction placed on the freedom of speech must relate to the grounds specified under Article 19(2).¹ In another judgement, the Supreme Court has clarified that a restriction on speech, in order to be reasonable, must be narrowly tailored so as to restrict only what is absolutely necessary.²

2. Requirement of intermediaries to proactively identify and remove unlawful content

[Rule 3(9)]

Rule 3: The intermediary shall observe following due diligence while discharging his duties, namely: --

(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

Issue: Intermediaries must deploy technology-based automated tools for identifying and removing access to unlawful content. The requirement for intermediaries to identify ‘unlawful’ content may be unreasonable.

The Draft Rules provide that intermediaries must deploy technology based automated tools for identifying and removing access to unlawful information or content. This provision may be contrary to the reasoning of the Supreme Court in a recent judgement.²

In 2015, the Supreme Court examined Section 79(3)(b) of the Information Technology Act, 2000. This provision required intermediaries to remove or disable access to certain types of content on the basis of user requests. The Supreme Court stated that it would be difficult for intermediaries to judge the legitimacy of each item given high volumes of content. It read down the provision to say that content needs to be removed or disabled only if: (i) it is done on the basis of the order of a court or government, and (ii) the order relates to one of the restrictions under Article 19(2) of the Constitution (such as state security and public order).²

The Draft Rules require intermediaries to develop automated tools to identify and remove access to ‘unlawful content’. This requirement is similar to the above provision which was read down by the Supreme Court.

3. Requirement of intermediaries to register in India if there are more than 50 lakh users

Rule 3: The intermediary shall observe following due diligence while discharging his duties, namely: --

(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;

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

(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.

Issue: Intermediaries with more than fifty lakh users must incorporate a company in India. It is unclear how the number of users will be calculated for the purpose of the rule. Therefore, Intermediaries will find it difficult to comply with this provision.

The Draft Rules provide that certain intermediaries must be incorporated in India, under the Companies Act, 2013. These are intermediaries with more than fifty lakh users or those notified by the government. The rule does not clarify how the number of users will be calculated. For example, the number of users of an intermediary may be calculated through different methods such as the number of registered users on the intermediary's platform, the number of daily active users, or the number of installations. In the absence of a clear methodology to determine the number of users, it may be difficult for an intermediary to judge whether it has crossed the fifty lakh threshold, and is therefore required to set up a company in India.

-
1. Secy., Ministry of Information & Broadcasting, Govt. of India vs. Cricket Assn. of Bengal 1995 AIR 1236.
 2. Shreya Singhal vs. Union of India AIR 2015 SC 1523.

MIT/79/030

General Comment:

[According to the invitation](#) for the comments/suggestion on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 the proposed amendments are aimed at strengthening the legal framework to make social media platforms more accountable under the law in response to a calling to attention motion on ‘misuse of social media platforms and spread of fake news’. DEF recognises the vital need to curb the misuse of social media to curb the spread of misinformation and disinformation channelised towards the incitement to violence in various parts of India. However, the intermediary guidelines have a broad mandate which cater to a wide range of intermediaries working in the digital space and not just to social media companies whose platforms are used for the distribution and propagation of misinformation and disinformation. As a result of this, it is important to carefully evaluate the causal, incidental, and eventual relationship between the objective and intent, the strategy, and the potential unintended consequences and knock on effects on current civic and economic practices in the digital space. Due to DEF’s presence on the ground working with communities towards reducing information poverty and improving social and economic equity in underserved areas by enabling access to information and communication technologies for development, it recognises that the reception and virality behind the spread of rumours that has led to violent action in different parts of India is underpinned by a complex web of social dynamics. Therefore, increasing the conditions under safe harbour requirements for intermediaries in themselves would not be enough to address the issue in terms of its causal and enabling factors since there needs to sustained effort in engaging with the root causes of the problem. This has been one of the learnings from the misinformation sensitisation workshops conducted by DEF with support from local district administrators and law enforcement across 11 states in India.

Intermediaries provide infrastructure or service which is used by end-users as per their own communication requirements. Safe harbour provision exists to provide conditional immunity from liability for third-party content and exemption from general requirement to monitor content. This arrangement is indispensable for protecting constitutionally guaranteed fundamental rights so as not to delegate law enforcement functions of taking evaluative decisions restricting citizens’ activities to private actors. With the proposed amendments, India is inching closer towards a stricter liability regimes by expanding the conditional requirements needed to qualify for safe harbour. A stricter liability regime that imposes greater obligations on intermediaries and proactive censorship requirements onto them undermines the expanded democratic potential and agency that digital media had afforded an ordinary individual. Moreover, definitional issues around terms such as “grossly offensive or menacing in nature”; “threatens public order”; “threatens public health or safety” should be resolved to avoid vagueness and achieve clarity. In order to ensure that ultimate objectives of aiding law enforcement to respond to the sensitive situations efficiently at a given time do not result in collateral damage and false positives, it is important to have clearly defined due process and safeguards in place with judicial oversight that lend transparency and accountability and ensure that only unlawful content, determined by a court of law, is restricted through intervention based on actual knowledge.

This general comment is followed by a discussion on the specific points of the proposed amendments such a traceability, automation and proactive monitoring, and the need for harmonisation with international standards and practices.

Specific Comments:

Traceability: Contention, contradiction, and evidence from the ground

Context: The past couple of years have seen an alarming [rise](#) in cases of lynchings and mob violence resulting out of rumours and misinformation spread via social media platforms like WhatsApp. The anonymity and the potential for virality afforded by social media obfuscate the detection of the actual perpetrator of the message. In a given locality gripped by violence-mongering rumours, traceability is understandably a prime law enforcement concern. Rule 3(5) of the proposed amendments aims to cater to this purpose. However, the said Rule contains a number of contradictions and could be interpreted to be sufficiently overbroad so as lead to its potential misuse. The Rule mentions a timeframe of 72 hours within which intermediaries would need to provide ‘information or assistance’ when *required by lawful order* by any government agencies *who are legally authorised*. However, this Rule does not mention the agencies and the rank of officials who would be legally authorised to issue lawful order mandating information and assistance from intermediaries. Clear delineation of due process is essential to foster accountability and transparency. While sensitive situations like lynching and mob violence demand expediency, it also calls for compliance with due process. Licensing [agreements](#) under The Indian Telegraph Act, 1885 for Internet Service Providers (ISPs) who can be classified as access providers already require ISPs to put systems in place that enable lawful monitoring and interception of communication by the Indian Government and they are also required to monitor content that communications that can be objectionable, obnoxious, malicious, or a nuisance. This is apart from their required compliance with provisions for data retention, disclosure, and provision of services towards aiding lawful monitoring and interception by government. Apart from this the license holders are also obligated to block Internet sites, URLs (Uniform Resource Locators), and/ or individual subscribers as identified and directed by the Licensor from time to time. Further, [the Gazette notification of 20 December 2018](#) under s. 69(1) of the Information Technology Act, 2000 authorising 10 police and intelligence agencies to “intercept, monitor, and decrypt” all information on any computer resource in the country.

Analysis: The above concurrent developments and pre-existing regulations highlight an enmeshing of regulatory regimes that seem to work at cross-purposes and to the detriment of the users’ fundamental freedoms and civil liberties. This is due to the lack of clarity on the grounds of balancing fundamental freedoms and public order and safety. Both the stated objective and the intent of amendments to the existing intermediary liability regimes stems from the need to regulate the proliferation of viral misinformation on the social media platforms. However, the proposed amendments will cover all types of intermediaries within its purview like payment gateways, advertisers, search engines and even access providers like ISPs who are already regulated under a licensing regime with its given set of compliances. In the absence of a surveillance law, the lack of clearly specified guidelines and procedures widen the ambit for abuse since the purposes for which information can be requested can range from security of the State to detection, prevention, and prosecution of crime and cyber security and matter connected or *incidental* thereto. The wide scope and ambit of Rule 3(5) without clear legally established tests or safeguards, and grievance redressal mechanisms in tandem with Gazette notification of 20 December 2018 mentioned above highlight the need for the much needed legal framework for state surveillance to ensure such powers are used for *bona fide* purposes only with clearly defined security safeguards and obligations on state agencies with the need for an effective review mechanism and judicial oversight as mentioned in the [Srikrishna Committee Report](#).

Recommendations: Define parameters to classify services provided by intermediaries rather than intermediaries themselves. As a result of the transmutable nature of the internet a particular intermediary may provide a number of different services. For example, Facebook is a social media platform that also sells advertising space. Once parameters of service have been so defined, regulations should be tailored with respect to that particular category keeping in mind already pre-existing sectoral regulations. Further, any demands made on intermediaries should follow clearly defined guidelines of due process along with obligations on state agencies for which it is important for the government to delineate the legally authorised agencies and rank of officers along with a process that allows for review of decisions taken. Ultimately, it is important to mandate judicial oversight for state intervention because courts are the best placed to judge the lawful/ unlawful nature of a content and necessity and proportionality of a proposed intervention. Apart from legal and regulatory frameworks to respond to societal challenges posed by viral misinformation, it also important to build individual and institutional capacity for resilience. DEF has been working on the ground with communities and local administration and law enforcement around the country by conducting workshops on misinformation and disinformation in partnership with WhatsApp. Conducted with the support of the District Collector's office and Superintendent of Police, 4500 stakeholders at the local and community-level have been trained between September 2018 and January 2019 across 11 states in India including police officers, local administrative officers, teachers, NGO representatives, local entrepreneurs, students, and self-help groups. While conducting the workshops DEF came to know of existing local efforts already being undertaken by local administration and law enforcement. For example, the Police Department of Seoni, Madhya Pradesh regularly organises workshops for their personnel to understand cyber-crimes better. During one of the workshops, teachers in Palghar, Maharashtra who confessed to sharing misinformation are educating other teachers, students, and local community members. Law students in Jaipur, Rajasthan pledged to become agents of change and reach out to people voluntarily in order to spread awareness about misinformation and disinformation. Pre – and post – assessment of the workshops revealed that the percentage of respondents who hardly verified their WhatsApp forwards fell sharply by 10.4% and the percentage of respondents who are most likely to verify their information increased by 20.9%.

Automation and the delegation of enforcement

Context: Rule 3(9) of the proposed amendments state that “(t)he Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content”. According to the Supreme Court judgement in the case of Shreya Singhal v Union of India [(2015) 5 SCC 1], an intermediary's proactive intervention is absent in s. 69A of the Information Technology Act, 2000 read with the Information Technology (Procedures and Safeguards for for Blocking for Access of Information for Public) Rules, 2009. A blocking order can only be passed by a Designated Officer after complying with 2009 rules or by a Designated Officer following a Court Order.

Analysis: Automated tools require large amounts of data to train. Bias in the data, historical or otherwise, as well as human bias creeps into the analysed outcome. Determination of what constitutes lawful and unlawful, especially in matters as nuanced, complex, and critical as those affecting fundamental rights such as freedom of expression and association online, cannot be authoritatively decided anywhere but in a court of law. Therefore, deploying such technologies to determine what is unlawful information or content becomes an exercise in building a pervasive system of myriad discriminations and prejudices that can have chilling effect on the democratic potential of the online space. While instances of child pornography, nudity, and sexual abuse are easy to detect and remove, instances of political speech are not. Moreover, delegating enforcement of online information and content to automated technologies and by translation private entities are incompatible with international standards of practice. Automated technologies have an endemic ‘black-boxing’ problem

where it is virtually impossible to trace the source and cause of a decision taken which undermine an aggrieved party's right to a due process. Furthermore, asking private entities to deploy such technologies to proactively identify and remove public access to unlawful information or content is tantamount to delegation of law enforcement to private actors. Private entities cannot be the arbiters of what constitutes lawful; this falls under the purview of the judicial system. Moreover, at the threat of losing safe harbour provisions, private entities would tend to err on the side of caution resulting in serious negative impacts on an individual's freedom of expression and association online. Further, proactive intervention of intermediaries in altering the status of the information or content they are hosting without actual knowledge might go against the very definition of qualifying as an intermediary and especially even more so as per the Supreme Court judgement issued in the case of *Shreya Singhal v The Union of India* [(2015) 5 SCC 1]. According to the latter, an intermediary can only remove content (a) upon receipt of court order that has found a particular content to be illegal within the course of court proceedings and (b) upon notification from an authorised government agency.

Recommendation: Rule 3(9) should be removed in its entirety because of implicit bias and black boxing inherent in automated decision-making, the lack of legal basis for delegation of law enforcement to private entities, and the lack of legal basis for proactive policing by intermediaries.

Harmonisation with international standards

Context: India's intermediary liability regime provides safe harbour protection for intermediaries which are conditional upon the fulfilment of certain obligations. This is [distinguished](#) from two other models: (a) broad protections and (b) strict liability regime. The former protects intermediaries from a wide range of third party content except in the cases of criminal activity or clearly defined categories of law. The latter holds intermediaries completely liable for third party content and require active monitoring and intervention by intermediaries. India's regime so far has been in-between these two extremes and closely reflecting The European Union E-Commerce Directive and US Digital Millennium Copyright Act. The argument against cumbersome intermediary liability regimes stems from concerns about 'collateral censorship', thereby undermining the expanded democratic space offered by digital media. As per the 2011 Joint Declaration on Freedom of Expression, 'liability should only be incurred if the intermediary has specifically intervened in content, which is published online'. It further states that 'ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and take-down'. Similarly in 2011, the Special Rapporteur on Freedom of Expression criticised States' attempts to force intermediaries to undertake censorship on their behalf and that intermediaries should only implement restrictions on users' fundamental rights and civil liberties upon judicial intervention. He further recommended transparent procedures to be adopted by intermediaries when required to take restrictive measures and keep the focus of such measure restricted to the specific content in question. The notice and take-down approach that is characteristic of conditional intermediary liability regimes like that of India have been criticised on the basis of lacking a clear legal basis. This is a result of unclear and complex notice and take-down provisions and their inherent arbitrary nature since they do not go through an independent judicial determination process on the (un)lawful nature of a given content. This is further exacerbated by a lack of due process available for appeals by the affected parties.

Analysis: Rule 3(9) of the proposed amendments have moved India closer to the stricter end of the spectrum by demanding proactive censorship. This in effect delegates the censorship to automated decision-making to be deployed by private entities, thereby holding serious implications for implicit bias, discrimination, and chilling effect. Rule 3(5) continues the trend of notice and take-down regime without any provision for judicial oversight. Moreover, the lack of differentiation between services provided by different intermediaries, there is a resultant entangling of sectoral regulatory regimes and

policy priorities with the proposed amendments thereby resulting in complex compliance processes for intermediaries who would then implement the highest restriction available in order to retain their safe harbour protection leading to an adverse effect on civic and democratic participation online.

Recommendations: In order to develop a progressive legal and regulatory regime that can balance justice, fairness, equity, and security in extending both liberty and security to its citizens India must work towards harmonising and emulating international standards and best practices. This would entail establishing clear guidelines, obligations, and due process on authorities in order to facilitate transparency and accountability towards fulfilling both expediencies of law enforcement as well as safeguarding long cherish constitutionally protected individual rights and liberties. Apart from establishing clear legal and regulatory frameworks like clarifying authorised government agencies, rank of authorising officers, and creating provisions for judicial oversight it is also important to work towards building capacity at the local administration and law enforcement level to respond to newer social exigencies created by proliferating technological penetration and the newer challenges thrown up by them. It important that any restriction sought to be placed by intermediaries on third-party content is based on narrowly defined legal tests and principles.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)



MIT/79/031

January 30, 2019

Comments by the Information Technology Industry Council on the Proposed Amendment to the Information Technology Intermediaries Guidelines

The Information Technology Industry Council (ITI) is pleased to respond to the Ministry of Electronics and Information Technology of India's proposed amendments to the Information Technology Intermediaries Guidelines (hereinafter, "the amendment").

ITI is the premier voice for the global information and communications technology industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. We advocate on behalf of our members for policy and regulatory environments that foster innovation and maximize all the benefits that ICT companies provide, including economic growth, job creation, and the tools to solve the world's most pressing social, economic, and environmental challenges. We work closely with our partners in government, international organizations, the business community, and civil society to achieve these objectives. One of the core elements of our mission, in every economy in the world, is to position our companies to be genuine partners of governments.

The internet has provided a platform for the development and deployment of a great variety of innovative content, applications, and services. Online platforms and intermediaries have played an incredible role in driving innovation and growth in the economy, creating market opportunities and access for businesses of all sizes. A critical aspect of any regulation focused on intermediaries is to clearly define the scope of the law and the types of services that fall within it. There is no common or clear-cut understanding of the concept of online platforms or intermediaries, so it is important for MEITY to make clear how various obligations in the amendment apply to various internet services, online marketplaces, cloud service providers, and content providers, depending on the nature of specific online platforms, fall into scope. A "one size fits all" approach would not be efficient, and regulations should recognize the different business models and functions.

We appreciate the recognition by MEITY of the role that platforms have played in driving innovation and growth in the economy, creating market opportunities and access for businesses of all sizes. In pursuing this initiative, we recognize that MEITY must carefully consider how to ensure that it protects important public interests. Neither we nor the companies we represent question the right and responsibility of governments to regulate in the public interest, whether to protect people's personal information, avoid inappropriate content, or prevent anti-competitive market behavior. Our companies succeed because of the trust and confidence of our customers, and so we have a strong interest in working with our Indian colleagues to advance these interests in a manner that is consistent with our shared commitment to open and non-discriminatory trade and investment environments. Similarly, we are sensitive to the idea that several of the proposed changes to the regulation of platforms could have significant consequences on the internet ecosystem and the ability of these companies to promote the growth and innovation that have

Global Headquarters
1101 K Street NW, Suite 610
Washington, D.C. 20005, USA
+1 202-737-8888

Europe Office
168 Avenue de Cortenbergh
1000 Brussels, Belgium
+32 (0)2 886 8764

@ info@itic.org

itic.org

fueled economic activity and innovation throughout India and the rest of the world. Any amendments to the IT Act must strive to keep in mind the rights of the users, including their right to free expression; feasibility of proposed changes by all companies in scope, and the demands of law enforcement. Further, the ongoing debate on privacy in India may be challenged by specific proposed changes in the amendment. We believe that any efforts to amend the IT Law should be consistent with user and business expectations on privacy, while also facilitating responsible actions by intermediaries and providing flexibility to adopt new technologies.

In our review of the proposed amendment, we note the following issues that could serve as significant barriers for companies providing intermediary services and may actually have the opposite effect as intended by the amendment.

- **Amendment 3(4) - New obligation to notify all users on a monthly basis about Terms of Service (ToS) and relevant Indian laws, and expansion of required terms in ToS:** There is a vague prohibition on content that "threatens public health or safety." The "public health or safety" restrictions are wider than laws that govern content expressed through other mediums -- for example, an intermediary would need to prevent any content that "threatens public health or safety", whereas such rules do not necessarily exist for other platforms or content providers. Additionally, the broad nature of this provision pertaining to "any content" could prove problematic in a variety of contexts, leading to unintended censoring of user content.

Additionally, frequent notifications can lead to notification fatigue, making them less useful. Companies often have robust contract management processes, and these should not be mandated to follow a certain pattern. Instead of focusing on the frequency of informing users, intermediaries should focus on easy accessibility and understanding of these terms.

- **Amendment 3(5) - Expanded obligation to assist any government agency with any request within 72 hours (including requests to disclose user information):** This is an overly broad and unduly burdensome obligation to provide subscriber information and content data without appropriate safeguards, such as those found in India's pending data protection legislation. The text also does not account for the possibility that company policy or legal obligations to users may prevent it from providing the government with certain information. Further, in many circumstances a company may only *process* certain information and not *retain* it, which would make it impossible for a company to comply with such requests. The 72-hour timeline is also not protected by any 'stop the clock' measures that would pause the timeline if there are legitimate reasons (such as a need to ask for clarification on scope of request or to provide missing information) that prevent the request from being fulfilled in 72 hours.

It is important that the modalities of notification and what constitutes a legal and lawful request be unambiguously clarified. Without such details, corporate entities would find it difficult to offer necessary assistance, as what constitutes assistance will be linked to the request and change on a case to case basis.

Any timelines for assistance are dependent on the nature of assistance sought and information available. In addition, companies must review and assess their legal obligations under contract with users and may need clarifications from agencies. Therefore, the amendment should provide for flexibility in terms of timelines for response. While businesses may acknowledge the

request within a certain specified time, the actual time taken to share information, if possible, should be case dependent.

Therefore, the amendment should provide for suitable exemptions for intermediaries, especially where there may already be existing legal obligations. We further recommend publication of guidelines on the process to be followed by companies on receiving requests.

- **Amendment 3(5) - New requirement for intermediaries to ensure that 'originators of information' can be 'traced out' as required by government agencies.** These terms are not clearly defined in the proposal and could require modification of technical architectures, breaking end-to-end encryption, mandating a great collection and retention of user and metadata information. The IT Act already contains specific provisions relating to surveillance, such as s.69 and s.69B, with corresponding delegated legislation.

Additionally, the lack of clarity leaves the door open for conflicting implementations as well as interpretations during enforcement proceedings and judicial proceedings and does not offer criteria by which an intermediary can gauge their compliance with the rule, adding to the uncertainty of operating in India as an online service provider. The amendment also does not specify, the time period for increased retention and collection period.

These requirements to trace the originator of information could result in violation of contractual terms and conditions related to data privacy and access to enterprise data. This can have a long-term impact on how India is perceived as a destination for technology business operations. We urge MEITY to consider the impact of mandatory requirements of tracing the originator on privacy and contractual terms, especially for entities who operate in B2B scenario. We further recommend guidelines on the process to be followed be made available.

- **Amendment 7 - New local presence requirement:** The amendment would require that intermediaries with more than 5 million users must "be an entity incorporated under Indian laws," "have a permanent registered office in India with physical address," and "appoint a locally present nodal officer for coordination with law enforcement." These requirements are not necessary in order to drive compliance with Indian law and would be detrimental to the growth of companies inside and outside India. Intermediary services act as both the catalyst and platform for small business growth and enhanced participation in international trade. The global reach of the internet enables easy communication and access to business partners, customers, information, and collaborators regardless of location in a way that was never possible before. Policies that require companies to open a physical office in any country in which they seek to do business impose unnecessary, expensive, and inappropriate requirements on digital companies. This move could also have a disproportionate impact on startups and micro, small, and medium enterprises (MSMEs), which may not be equipped with the infrastructure to comply with the requirements. We encourage MEITY to remove this language and recognize that intermediaries can already conduct their business in complete compliance with applicable laws without establishing a registered local presence.
- **Amendment 8 - Imposition of 24-hour limit for all content takedown and removal requests from a government agency or court:** This diverges from the earlier practice of acknowledging requests in 36 hours and removing them in 30 days. As with the 72-hour timeline above, this is burdensome and technically challenging for companies, and there is no protection by any 'stop

the clock' provisions in cases where more information or clarity is needed about a request. The amendment should also include safeguards for appeal and discussion to prevent misuse. We recommend that the timeline to remove or disable access to content be increased and made more flexible on a case dependent basis.

- **Amendment 9 - New monitoring requirements:** The amendment proposes that intermediaries must deploy automated mechanisms "for proactively identifying and removing or disabling public access to unlawful information or content." These requirements are problematic for multiple reasons. First, they are vague in scope. The proposal refers to "unlawful content," but this term is not clearly defined in the amendment and would be subject to the interpretation of individual companies that are not typically in a position to determine whether content is unlawful. A similar reference to "appropriate controls" would render the amendment even more subjective and difficult to comply with.

Proposed monitoring and removal of information could impact the privacy of clients. Certain types of proactive monitoring and removal of content goes against the expectation of an intermediary, and the notion of safe harbor accorded to them. Various judicial pronouncements in India have also held that intermediaries are not required to proactively monitor, review, or edit content, which is a criteria for intermediaries to qualify for a safe harbor under the IT Act. Further, for entities such as cloud service providers, deploying automated tools to monitor content, could be a violation of contractual terms and conditions.

We would therefore recommend removal of this provision as a mandate, or exemptions should be carved out for types of intermediaries where such monitoring is against the business model and places an undue burden on such entities.

Further, this requirement should be coupled with a 'good Samaritan' protection that provides a safe harbor when a provider engages in direct proactive monitoring. Also, "unlawful" should be narrowly defined, so that it is not subject to individual company or enforcement interpretation.

Finally, given the large volume of content shared online, platforms faced with a proactive filtering requirement will often take a 'better safe than sorry' approach and take down content that is anywhere near the line of illegality, resulting in the removal of a significant amount of legitimate content and speech.

* * * * *

ITI appreciates the opportunity to present our views on this matter. We stand ready to support MEITY in clarifying policy considerations with respect to online intermediaries that allow India to advance its legitimate public policy goals in a manner consistent with innovation, job creation, and economic growth.

Sincerely,



Ashley E. Friedman
Senior Director, Policy



**Amnesty India submission to the
Ministry of Electronics and Information Technology, Government of India
on the draft Information Technology (Intermediary Guidelines) Rules 2018**

30 January 2019

Following the call of the Ministry of Electronics and Information Technology for comments and suggestions on the draft Information Technology (Intermediary Guidelines) Rules 2018, published on 24 December 2018, Amnesty India welcomes the opportunity to make the following submission.

The draft Rules would significantly change the nature of intermediary liability in India. Amnesty India is deeply concerned that the draft Rules, if implemented in their current form, would run counter to India’s national and international obligations to safeguard human rights, in particular the right to freedom of expression and the right to privacy.

The draft Rules would amend and replace the Information Technology (Intermediaries Guidelines) Rules, 2011, which were notified under Section 79 of the Information Technology Act, 2000, which provides conditional ‘safe harbour’ immunity from liability to Internet intermediaries.¹ The Ministry has stated that the drafting of the 2018 Rules followed concerns raised in Parliament about “misuse of social media platforms and spreading of fake news”.²

Amnesty India shares several of the government’s concerns about the prevalence of disinformation, hateful expression, harassment and abuse online, often directed at women and members of minority groups. However the draft Rules in their current form run the risk of restricting legitimate expression, chilling free expression, and violating the right to privacy, while stopping short of strengthening transparency requirements for Internet companies.

This submission analyses some of the provisions of the draft Rules in light of India’s obligations under international human rights law and standards on freedom of expression and privacy.

¹ The draft Rules are available at http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

² Press Information Bureau, “Draft IT rules issued for public consultation”, 24 December 2018. Available at <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>

CONCERNS AND RECOMMENDATIONS

I. Censorship of legitimate expression

Vague and overly broad terms

Rule 3(2) states that intermediaries³ shall inform users to not host or publish “information” that falls under certain categories, including information which “is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful”.

Other categories include information which “communicates any information which is grossly offensive or menacing in nature”, or which “threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states... or is insulting any other nation.” Rule 3(3) requires intermediaries to themselves not publish such information.

Rule 3(9) also states that companies shall proactively identify and remove “unlawful” information or content. None of these terms are defined anywhere in the Rules or in the Information Technology Act, 2000.

Concerns:

The draft Rules retain much of the ambiguous language used in the Information Technology (Intermediaries Guidelines), 2011. Amnesty India is concerned that the Rules use vague and overly broad terms to identify expression that can be restricted, going well beyond both Indian and international human rights standards on freedom of expression.

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) – to which India is a state party – applies equally to online expression. While governments can impose restrictions on the right to freedom of expression, these restrictions must meet certain well-established conditions under international law.⁴ Firstly, they must be prescribed by law

³ The draft Rules adopt the definition of ‘intermediary’ used in the Information Technology Act, 2000, which states: “‘intermediary’ with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message”. This could conceivably cover internet service providers, web hosting providers, social media platforms, search engines, VPN providers, payment gateways, online aggregators and e-commerce companies. The Act is available at <http://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf>

⁴ The UN Human Rights Committee, which oversees the implementation of the ICCPR, describes these standards in greater detail. See Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34. Available at <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

which is clear and accessible, and distinguish between lawful and unlawful expression with sufficient precision and clarity.

Secondly, they must protect certain specific legitimate interests: the rights or reputations of others, national security or public order, or public health or morals. Thirdly, they must be necessary and proportionate to achieve that purpose, and must be the least intrusive measure among those available. Restrictions must be consistent with all other human rights recognized in international law, and not impair the essence of the right affected.

Many of the terms used in the draft Rules are not sufficiently clear or narrowly defined. Terms such as “unlawful”, “grossly harmful”, “harassing”, and “insulting any other nation” lack clarity and precise definition, and make it difficult for Internet users to predict what expression will be restricted. The vagueness and over-breadth of these terms can end up restricting legitimate exercise of the right to freedom of expression, and have a chilling effect – leading to people exercising self-censorship for fear of having their content removed.⁵

Similar concerns had led India’s Supreme Court to strike down Section 66A of the Information Technology Act in 2015.⁶ Section 66A criminalized several forms of online expression, including sending of information that was “grossly offensive” or persistently caused “annoyance, inconvenience, obstruction, insult, injury, enmity, hatred or ill-will”. It had been used on several occasions to prosecute people for legitimately exercising their right to free speech online.⁷

The Supreme Court ruled that Section 66A was “unconstitutionally vague” and overbroad, and that it “arbitrarily, excessively and disproportionately invades the right of free speech”. It stated: “Every expression used [in the law] is nebulous in meaning. What may be offensive to one may not be offensive to another. What may cause annoyance or inconvenience to one may not cause annoyance or inconvenience to another... Information that may be grossly offensive or which causes annoyance or inconvenience are undefined terms which take into the net a very large amount of protected and innocent speech.” The draft Rules are likely to have a similar effect.

⁵ Protecting the rights of others from advocacy of hatred that constitutes incitement to hostility, discrimination or violence does justify some restrictions on the right to freedom of expression. However, where a government seeks to justify restrictions on these grounds, it must demonstrate a direct and immediate connection between the expression and the threat to others’ rights. Advocacy of hatred is also more than just the expression of ideas or opinions that are hateful. It requires a clear showing of intent to urge others to discriminate, be hostile toward, or commit violence against the group in question. The draft Rules conflate many forms of protected expression with advocacy of hatred.

⁶ Supreme Court of India, *Shreya Singhal versus Union of India*, decided on 24 March 2015. Available at <https://indiankanoon.org/doc/110813550/>

⁷ See Amnesty International India, Submission to Law Commission of India on Media Laws, Available at <https://amnesty.org.in/wp-content/uploads/2014/06/Amnesty-International-India-submission-on-media-laws-with-summary.pdf>

Proactive content moderation obligations and censorship

Rule 3(9) of the draft Rules states: “The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.” This is a new provision, which was not present in the 2011 Rules. The draft Rules do not specify any penalty for non-compliance.

On 5 January, the Ministry tweeted during a question-and-answer session on the draft Rules on Twitter: “It is manually not possible to filter fake content in short span, hence automated tools are required.”⁸

Concerns:

Internet intermediary companies play a crucial role in facilitating the enjoyment of the right to freedom of expression online. While governments can require companies to remove content which is manifestly illegal, creating a regime where companies must proactively monitor and remove content can lead to ‘over-compliance’, causing legitimate expression to be restricted, and chilling free expression. This risk is heightened when the level of liability that companies face for non-compliance is unclear.

Such a system would not require the intermediary to hear the views of the content creator and would lack judicial oversight. In 2012, research by the Centre for Internet and Society showed that intermediaries were quick to err on the side of caution and suppress even legitimate expression in an effort to limit their liability, when asked by a third party to take down content.⁹ A proactive takedown regime, used in connection with the vague and overly broad terms mentioned above, would increase the likelihood of legitimate speech being restricted.

No government should require intermediaries to conduct censorship on its behalf.¹⁰ Requiring intermediaries to proactively remove content would risk violating India’s obligations to protect the right to freedom of expression. In 2018, the UN Special Rapporteur on freedom of expression in a report on regulation of user-generated online content described proactive content monitoring or filtering as “both inconsistent with the

⁸ Available at https://www.twitter.com/Gol_MeitY/status/1081504461569343489?s=20

⁹ Centre for Internet and Society, Intermediary Liability in India: Chilling Effects on Free Expression and the Internet, 2011. Available at <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf>

¹⁰ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27. Available at https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

right to privacy and likely to amount to pre-publication censorship” and recommended that governments refrain from establishing such arrangements.¹¹

The Special Rapporteur said, “Demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours...Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic.” Delegating responsibility to companies to adjudicate content, said the Special Rapporteur, “empowers corporate judgment over human rights values to the detriment of users.”

The 2014 Manila Principles on Intermediary Liability, developed by a coalition of civil society experts, expressly states that intermediaries should never be required “to monitor content proactively as part of an intermediary liability regime”.¹²

A proactive takedown regime could also run contrary to established Indian law. In 2015, India’s Supreme Court ruled that intermediaries would be required to remove content only when specifically directed to do so by a court or government order. The Court said, “This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.”¹³

Additionally, Rule 9 also appears to suggest that intermediaries would be expected to use automated tools to remove content. However automated systems that are used as the sole mechanism to take down content poses a serious risk to restricting legitimate expression online. For example, in June 2017, Google announced "four steps intended to fight terrorism online", among them more rigorous detection and faster removal of content related to 'violent extremism' and 'terrorism'. The automated flagging and removal of content resulted in the accidental removal of hundreds of thousands of YouTube videos uploaded by journalists, investigators, and human rights organizations.¹⁴

The UN Special Rapporteur on freedom of expression has pointed out that automation has significant limitations such as difficulties with addressing context, widespread variation of

¹¹ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35. Available at <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

¹² Principle 1 of the Manila Principles. Available at <https://www.manilaprinciples.org>

¹³ Supreme Court of India, *Shreya Singhal versus Union of India*, decided on 24 March 2015. Available at <https://indiankanoon.org/doc/110813550/>

¹⁴ Scott Edwards, Amnesty International, “Youtube removals threaten evidence and the people that provide it”, 1 November 2017. Available at <https://www.amnesty.org/en/latest/news/2017/11/youtube-removals-threaten-evidence-and-the-people-that-provide-it/>

language cues and meaning and linguistic and cultural particularities.¹⁵ There is also a risk that automated systems will entrench existing discrimination, including when the automation relies on understanding developed within certain countries.

Imposing a proactive takedown regime also raises the question of whether intermediaries will be required to break encryption to examine content. This concern is detailed below in the section on violation of privacy.

Compliance with government orders

Rule 3(8) requires intermediaries to remove, or block access to, certain kinds of content “upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency...as far as possible immediately, but in no case later than twenty-four hours.”

Concerns:

There are not sufficient procedural safeguards in the draft Rules over the authorities’ power to order the removal of, or blocking of access to, user-generated content.

The procedure for the operation of Section 69A of the Information Technology Act, which authorizes authorities to issue directions for blocking access to online content, is laid out in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.¹⁶ (It is likely, but not certain, that a similar procedure will apply to orders for the removal of online content under the draft Rules.) The 2009 Rules suffer from several deficiencies – they do not provide for appeals, they do not require the originators of content to always be notified or heard, and they require the details of orders to be kept secret.

Requiring intermediaries to take down content on the directions of government authorities greatly increases the risks of legitimate expression being restricted.¹⁷ As the UN Special Rapporteur on freedom of expression has recommended, governments should only seek to restrict content following an order by an independent and impartial judicial authority. The

¹⁵ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35. Available at <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

¹⁶ Available at <http://meity.gov.in/writereaddata/files/Information%20Technology%20%28%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public%29%20Rules%20202009.pdf>

¹⁷ The number of court orders for removal of content appear to be far fewer than requests from government agencies. For example, for the period from January 2017 to June 2018, Twitter says it received 13 removal requests through court orders, compared to 481 removal requests through government authorities. Twitter’s transparency report for India is available at <https://transparency.twitter.com/en/countries/in.html>.

Special Rapporteur has also said, “States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.”¹⁸ The Manila Principles also state: “Intermediaries must not be required to restrict content unless an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful.”¹⁹

II. Violation of privacy

Identifying creators of content

Rule 3(5) states: “When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency...The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”²⁰ On 5 January, the Ministry tweeted during a question-and-answer-session on the draft Rules on Twitter: “We are only asking to trace origin of messages which lead to unlawful activities without breaking encryption”.²¹

Concerns:

Access to and use of encryption is an enabler of the right to privacy and the rights to freedom of expression, information and opinion. Governments therefore have an obligation to ensure that any interference with encryption is necessary, proportionate and does not result in weakening the security of electronic communications and data for everyone.²²

Despite the Ministry’s ‘clarification’ on Twitter, Rule 3(5), by stating that intermediaries must enable the tracing of originators of information, appears to be requiring companies to weaken their encryption standards, build a backdoor to access communications protected by end-to-end encryption, or gather and store metadata about their users.²³

¹⁸ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35. Available at <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

¹⁹ Principle 2 of the Manila Principles. Available at <https://www.manilaprinciples.org>

²⁰ On 20 December 2018, the Ministry of Home Affairs issued a notification which enabled 10 central agencies to directly or indirectly intercept, monitor and decrypt any information from any computer. Amnesty India has similar concerns about this notification. See Indian Express, “10 central agencies not authorized to intercept information on computers”, 21 December 2018. Available at <https://indianexpress.com/article/india/10-central-agencies-now-authorized-to-intercept-information-on-computers-5503254/>

²¹ Available at https://www.twitter.com/Gol_MeitY/status/1081505492059467776?s=20

²² For more, see Amnesty International, Encryption: A Matter of Human Rights, March 2016. Available at https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf?x45368

²³ The measure could be particularly targeted at Facebook-owned Whatsapp, which has over 210 million users in India and has been reportedly used to spread disinformation and rumours that led to incidents of mass violence. The government has said in Parliament that law enforcement agencies have found it difficult to decrypt messages protected by the end-to-end encryption provided by Whatsapp. See NDTV, “Security agencies unable to decrypt Whatsapp communications: Prasad”, 2 May 2016. Available at

While governments can legitimately use electronic surveillance to protect people from crime, forcing companies to weaken encryption indiscriminately affect all users' online privacy by undermining the security of their electronic communications and private data. Such measures would be inherently disproportionate, and therefore impermissible under international human rights law.²⁴

The UN Special Rapporteur on freedom of expression, in a report on encryption and anonymity, has stated: "States should adopt laws and policies that provide comprehensive protection for and support the use of encryption tools, including encryption tools designed to protect anonymity...States should not require private actors to facilitate backdoor access in commercially available products and services."²⁵

Targeted decryption orders or requests for people's metadata from internet companies are on their face a more proportionate limitation of the rights to privacy and freedom of expression. However even these orders must be used only in exceptional circumstances and to achieve a legitimate aim. They must be clearly limited in scope, focused on a specific target, based on reasonable suspicion and authorized by a judicial authority. Companies should not be required to retain communications-related data outside the context of ongoing criminal investigations and on the basis of judicial orders containing proper individualisation and reasonable suspicion of wrongdoing.

The UN High Commissioner on Human Rights has stated that any interference with the right to privacy, including by communications surveillance, must be sanctioned by law, and necessary and proportionate towards a legitimate aim.²⁶ These principles were also recognized by India's Supreme Court in a landmark judgment in 2017.²⁷

The Manila Principles also state that intermediaries should not be required to ensure they have the capacity to identify users, or to disclose any personally identifiable user

<https://gadgets.ndtv.com/apps/news/security-agencies-unable-to-decrypt-whatsapp-communications-prasad-832494>

- ²⁴ In 2015, the Indian government released a draft policy on encryption that sought to require users of social media and messaging applications to save plain-text versions of their messages for 90 days so that they could be shared with the police. The proposal was withdrawn after a public outcry. The UN Special Rapporteur on the right to privacy, in a letter to Indian authorities, has raised concerns around mass surveillance in the context of a proposed data protection law. The letter is available at <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=24201>.
- ²⁵ Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Encryption and anonymity follow-up report, June 2018. Available at <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>
- ²⁶ Report of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age", 3 August 2018, A/HRC/39/29. Available at <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>
- ²⁷ Supreme Court of India, *Justice K.S. Puttuswamy (Retd). and others versus Union of India*, decided on 24 August 2017. Available at <https://indiankanoon.org/doc/91938676/>

information without an order by a judicial authority.²⁸ The International Principles on the Application of Human Rights to Communication Surveillance (or “Necessary and Proportionate Principles”), which were drafted by a consortium of NGOs, also state that determinations related to communications surveillance must only be made by a competent judicial authority that is impartial and independent, after it is satisfied that the surveillance is necessary and proportionate.²⁹

III. Lack of transparency

Transparency of companies

Rule 3(12) states that intermediaries shall publish the name and contact details of a grievance officer, and a mechanism for users to record complaints. There are no other requirements for transparency on the part of the companies.

Concerns:

The principle that companies have a responsibility to respect human rights is now well-established under international business and human rights standards. The UN Human Rights Council unanimously endorsed this principle when it approved the UN Guiding Principles on Business and Human Rights in 2011.³⁰

Unfortunately, many Internet companies adopt content standards and private rules of their own design that lack transparency and rigour and fall well short of international human rights standards.³¹ Companies frequently avoid public accountability and engagement with civil society, and reach secretive agreements with governments on implementation of content standards with regard to takedown requests and sharing of user data.

The UN Special Rapporteur on Freedom of Expression has pointed out that Internet companies need to incorporate principles of international human rights law into their policies and processes, and adopt a radically different approaches to transparency at all stages of their operations.³² Companies must carry out rigorous human rights impact assessments for product and policy development, and supplement them with ongoing assessment, reassessment and meaningful public and civil society consultation.

²⁸ Principles 2 and 5 of the Manila Principles. Available at <https://www.manilaprinciples.org>

²⁹ Principles 5 and 6 of the Necessary and Proportionate Principles. Available at <https://necessaryandproportionate.org/principles#the-principles>

³⁰ United Nations Human Rights Office of the High Commissioner, Guiding Principles on Business and Human Rights, 2011. Available at https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

³¹ See for example Amnesty International, Toxic Twitter – A Toxic Place for Women, March 2018. Available at <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>

³² Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35. Available at <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

They must also seek greater engagement with digital rights organizations and other relevant sectors of civil society, and make the development of industry-wide accountability mechanisms a top priority.

With regard to content moderation, companies should enable and empower users to understand and utilize individual security and privacy measures, and implement adequate and transparent reporting mechanisms. They should also record and publicly share disaggregated data about the levels and types of online violence and abuse reported, as well as their response on a regular basis. Any automated tools used to moderate content should be rigorously audited and developed with user and civil society input. The use of automated tools should only take place where there is a 'human in the loop' and should form part of a larger content moderation system characterized by human judgement, greater transparency, rights of appeal and other safeguards.

Inadequate Consultation

The draft Rules were initially reportedly discussed by authorities in a confidential meeting on 21 December with representatives from a few major technology companies.³³ They were uploaded on the Ministry's website only on 24 December, following media reports about the meeting. The draft Rules do not contain any explanatory materials.

Concerns:

The changes envisaged by the draft Rules could potentially affect millions of Internet users in India. It is essential that any proposal to change India's intermediary liability regime be as widely consultative as possible. The government must conduct a more thorough consultation with civil society actors, Internet companies, industry bodies and members of the public. It must also publish a background note explaining the rationale behind the proposed changes to the Rules, and providing evidence to support the proposed changes. Given the magnitude of the proposed changes, they must also be reviewed and discussed by Parliament.

Pending further consultation, Amnesty India calls on the government of India to withdraw the draft Rules, and take steps to review and amend existing laws and policies related to intermediary liability to ensure that they are compatible with India's human rights obligations.

³³ Indian Express, "Government moves to access and trace all 'unlawful' content online", 23 December 2018. Available at <https://indianexpress.com/article/india/it-act-amendments-data-privacy-freedom-of-speech-fb-twitter-5506572/>

चन्द्र भूषण कुमार, भा.प्र.से.
उप निर्वाचन आयुक्त
Chandra Bhushan Kumar
Deputy Election Commissioner



भारत निर्वाचन आयोग
Election Commission of India

MIT/79/034

PS/2019/01

Dated:- 19.01.2019

Dear Sir,


Kindly refer to the invite of comments/suggestions on the proposed Intermediaries Guidelines (Amendment) Rules, 2018, as available on the website of Ministry of Electronics and Information Technology.

Commission being concerned of the possibility of misuse of the platforms of the intermediaries, by some individuals/entities, which can influence the elections, has desired that a clause under the proposed Sub Rule (2) of Rule (3) to the following effect may be considered for incorporation in the said draft Rules:- "*violation of any of the provisions of election law or/and directions of the Election Commission, during the period of any election.*"

I request you to consider it and communicate the decision taken in this regard for the information of the Commission.

With kind regards,

Sincerely Yours,


(Chandra Bhushan Kumar)

MeitY/104 of 608

Office of Sr. Dir. (PK)
Date: 23/01/2019
Diary No. 60



Blank

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

forth ambitious plans for the country's growing digital economy. This is notable with India's improved ranking in the World Bank's *Ease of Doing Business* report for the second consecutive year.⁵

As currently written, the Draft Guidelines would hinder this progress and would significantly impact the open Internet in India. A key component of the Internet ecosystem is the understanding that intermediaries cannot police all content posted by third parties. A strong, innovative economy relies on certain protections that limit liability of intermediaries for the content posted by their users. India has recognized this through the exemptions granted for intermediaries under Section 79 of the Information Technology Act, 2000 ("IT Act"). The Supreme Court of India also provided welcome clarification regarding India's intermediary framework in *Shreya Singhal v. Union of India*, reducing regulatory uncertainty.⁶ As "intermediary" is defined broadly under the IT Act to cover a variety of Internet and communication services, an intermediary liability framework that does not strike the correct balance will have severe consequences for the digital economy and free speech in India.

However, as explained in further detail below, new rules as outlined in the Draft Guidelines would undermine this regime by introducing new obligations on intermediaries that lack necessary clarity and proper guidance on what is required. Further, the Draft Guidelines introduce assistance requirements that threaten to undermine secure communications and the privacy of Indian citizens and Internet users.

Comments on Amendments

1. Rule 3, sub-rule (4): Notice Requirements

(4) The intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.

The amendments introduce a new requirement that intermediaries must communicate rules and regulations, user agreements, and privacy policies to users every month.

⁵ WORLD BANK GROUP, *Doing Business 2019: Training For Reform* (2018), available at http://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2019-report_web-version.pdf.

⁶ Supreme Court (India), *Shreya Singhal v. Union of India*, (2015) S.C.C. 248, text available at https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/06/Shreya_Singhal_vs_U.O.I_on_24_March_2015.pdf (reading Section 79(3) of the IT Act to require an intermediary to achieve actual knowledge and act only upon receipt of a court order to remove content). While the clarification in the Draft Guidelines to align the intermediary rules with the ruling is welcome, other new requirements are inconsistent with *Singhal* as explained below.

While conspicuous notice of *changes* to terms and conditions is important, mandating recurring notices to consumers that contain no new information may drive users to ignore communications, including important messages. Often the information described is readily available to users to access at will. Already, observers have noted that mandatory compliance notifications in certain jurisdictions create “notice fatigue”, where users may ignore notices, pop-ups, and other communications from service providers.⁷ Not only does this suggest that recurring, non-essential communications represent a bad user experience, this also creates the risk that users misinterpret important communications as “routine” notifications and do not give those communications the attention they require. Accordingly, while intermediaries should be expected to notify users of important conditions of service, including termination, communications to users should only be required when those conditions are updated or changed.

2. Rule 3, sub-rule (5): Law Enforcement Assistance

(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. 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.

The amendments introduce provisions on law enforcement assistance that do not take account of the capabilities of different intermediaries, create new requirements that will undermine security in online communications, and do not include procedural safeguards to protect against abuse.

While it is reasonable for law enforcement authorities to request expeditious assistance, the capabilities of firms vary. Large firms with extensive legal departments may be able to meet demands proposed by these amendments, but small firms with fewer resources may elect to forego providing services that would come under these regulations. The result would be to decrease consumer choice. In particular, the 72-hour deadline is an arbitrary time frame that will disadvantage small online services. Even large services may not have the requisite time to process orders or seek necessary clarification from law enforcement officials.

⁷ A white paper by a Committee of Experts commissioned by the Government of India regarding data protection frameworks cited the problem of “notice fatigue.” The concerns are the same in the context of this current proceeding on the Draft Guidelines. See MEITY, White Paper of the Committee of Experts on a Data Protection Framework for India (2017), available at http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf.

Insofar as this rule contemplates compelling online intermediaries to provide information on encrypted communications, the tracing obligation will undermine user privacy and security. An intermediary cannot fulfill the tracing obligation as outlined in the Draft Guidelines without undermining end-to-end encryption, a feature upon which lawful users of Internet services around the world depend to secure personal information and other sensitive communications. Intermediaries would have to remove these protections in order to trace users' communications. In addition to undermining user security, this mandate is inconsistent with the three-pronged test of legality, necessity, and proportionality attached to state intrusions upon privacy by Indian Supreme Court jurisprudence. The amendments also do not specify which government agencies would be legally authorized to order an intermediary to trace users.

Internet platforms and services have devoted significant resources to deploy the most effective means of securing devices and user communications. This includes strong end-to-end encryption which protects users' sensitive information from bad actors who seek to exploit information. These protections should not be eroded by the Draft Guidelines.

3. Rule 3, sub-rule (7): New Local Presence Requirements

(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;*
- (ii) have a permanent registered office in India with physical address; and*
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.*

The local presence requirements outlined in the amendments including incorporation mandates, requirements to create permanent registered offices in-country, and a designated contact person for law enforcement assistance around the clock are all significant barriers to doing business in India. Localization requirements create artificial borders on the Internet, which is otherwise characterized by low barriers to entry.

Requiring online services to maintain a local presence denies smaller firms access to the Indian market. A local presence requirement functionally discriminates against small and medium-sized enterprises, who use the Internet to access new markets. This is important not only to service providers, but to the Indian customers who depend on small Internet services for personal or business needs. The fifty lakh user threshold is also arbitrary, and does not provide a meaningful exception for small businesses around the world to invest in the local digital economy.

Local presence requirements are also out of place in an intermediary guideline framework. Rather than introducing these sweeping provisions that would implicate serious trade concerns in amendments to the IT Act, Indian policymakers should engage in discussions with intermediaries on how best to address issues, to the extent they exist, regarding law enforcement assistance by Internet services.

4. Rule 3, sub-rule (8): Changes to Content Removal Requirements and Data Retention

*(8) 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 Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ **one hundred and eighty days** for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorized.*

The rules introduce a 24-hour deadline to remove content upon receipt of a court order or government notification. Just as a 72-hour deadline may be too burdensome for small firms, a 24-hour deadline would be unreasonable for an even larger number of firms. While law enforcement authorities may reasonably expect expeditious responses to problematic content, many firms could be expected to struggle to meet such timelines.

The deadline also does not provide necessary safeguards regarding due process. The short timeline would not allow for adequate processing and review of the content at issue. Like the United States, India provides constitutional safeguards for the concept of due process, and the proposed rules are inconsistent with Indian Supreme Court precedent interpreting these safeguards. Recently, for example, the Supreme Court struck down Section 33(2) of the 2016 Aadhaar Act on the basis that it permitted access to critical data of citizens, on national security grounds, without guardrails to ensure the proper exercise of that power.

The amendments would also extend the requirement for intermediaries to store data and records of users associated with the relevant content subject to the court order for at least 180 days. This requirement appears to be unnecessary, and is likely to result in confusion about what exactly online services are required to preserve. It is not uncommon for a court in appropriate circumstances to issue an order detailing that specific information be preserved. To impose this

burden as a matter of course would place a significant burden on intermediaries, when doing so is already with the power of a court with appropriate jurisdiction.

5. Rule 3, sub-rule (9): New Mandate to Deploy Technology to Filter Content

(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

The Draft Guidelines introduce a new obligation for an intermediary to “deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

A mandate to deploy filtering mechanisms or other automated tools should not be a prerequisite for protections under Section 79 of the IT Act.

The mandate runs contrary to international best practices. The Manila Principles, a globally accepted standard for intermediary liability regulation across governments, provide that intermediaries should be shielded from liability for third-party content, and not compelled to proactively monitor user communications. The Draft Guidelines disregard this principle by preconditioning the liability safe harbor upon proactive monitoring. This requirement will fall upon smaller services with particular prejudice, as proactively monitoring users is particularly costly at scale.

This also departs from existing Indian law. In *Shreya Singhal v. Union of India*, the Supreme Court interpreted provisions of the IT Act and associated rules to mean that an intermediary cannot be required to proactively monitor its platform for unlawful content.⁸ Given the technological challenges to affirmatively monitoring all user content at scale, policymakers should defer to online services’ own self-regulatory efforts in this regard.

While automated tools can in certain cases be a helpful component of addressing online content that is unlawful or that violates a platform’s terms of service, such tools are expensive, imprecise, and impractical for every type of “intermediary” covered by the Draft Guidelines to implement. Some companies have spent years and significant resources to voluntarily develop their own technology to help identify and remove specific content, but content moderation remains a difficult task. The most successful cases involve looking for content that is compared against an existing library.

To use one example, some platforms attempt at considerable expense to filter for copyrighted content, but only when copyright owners proactively furnish metadata about their content that

⁸ *Shreya Singhal v. Union of India*, *supra* note 6.

platforms can use to filter *against*. No worldwide database of copyrighted works exists, and even if it did, such a database would be unlikely to contain sufficient metadata to build a successful system of filtering. Thus, a small number of online services have forged relationships with large industrial copyright holders to filter incoming content against a reference library of certain works. Even in the scenario where metadata has been furnished, false positives abound, and require constant human oversight. Thus, despite best efforts, no automated tool is one hundred percent effective or accurate. These tools, when administered haphazardly, can lead to removal of lawful content, affecting free expression online.

Further, it places the intermediary in the position to determine what is “unlawful”, a determination that often requires complex legal and technological analysis, and may lead to over-enforcement due to uncertainty and fear of liability. This is inconsistent with the *Singhal* decision insofar as it places private actors in the position to determine what content is permitted online.⁹

Due to the inconsistency of this provision with the Indian Supreme Court’s ruling, global best practices, and technological feasibility for all Internet services affected, CCIA urges that it be removed.

Conclusion

Due to the concerns outlined in these comments, CCIA respectfully requests that MeitY reconsider these changes to its intermediary rules and further consult with industry, the public, and other stakeholders, so as to ensure that the interests of intermediaries and rights of users are protected under Indian law.

Respectfully submitted,

Matt Schruers
Rachael Stelly
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
(202) 783-0070
mschruers@ccianet.org

⁹ *Shreya Singhal v. Union of India*, *supra* note 6, at *48 (“Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.”).

CCAOI's comments on the Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018

MIT/79/037

Before making specific comments on the Amendment we wish to draw your attention to the **Intermediary Liability in India**

Under the Information Technology Act, 2000 (IT Act), an 'intermediary' with respect to any particular electronic message means "any person who on behalf of another person receives, stores, or transmits that message or provides any service with respect to that message". Intermediaries include telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places, and cyber cafes. While the IT Act provides safe harbour protection to intermediaries, that is, legal immunity from any liability arising from content hosted by third-parties on an intermediary's platform, the Information Technology (Intermediaries Guidelines) Rules, 2011 lays down the due diligence practices intermediaries should observe in order to avail safe harbour protection under the IT Act. These due diligence practices under the existing Intermediary Guidelines include merely acting as a facilitator with respect to the information being made available on the intermediary's platform, not initiating the transmission, selecting the receiver of transmission, and selecting or modifying the information contained in the transmission.

Since the safe harbour protection is an exemption that intermediaries can avail by fulfilling certain conditions specified under the IT Act, we are of the view that any additional obligations on intermediaries would have to comply with the ruling in *Shreya Singhal v. Union of India* (Shreya Singhal case).

In the *Shreya Singhal* case of 2015, the Supreme Court of India (SC) struck down Section 66A of the IT Act and declared it unconstitutionally vague as it consisted of ambiguous language such as "grossly offensive", "menacing", "false", and "causing annoyance, inconvenience, danger". The SC upheld that any request for restricting or taking down content from an intermediary's platform can only be carried out upon receiving actual knowledge through a valid court order or order by a government agency. Such requests must be in consonance with Article 19(2) of the Constitution of India, 1950 (Constitution), which provides for 'reasonable restrictions' on the freedom of speech and expression in specific cases only such as security of the State, defamation, contempt of court, etc. Requests must also comply with the due process laid down under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules).

Secondly, if we look at **International Standards**, such as the Manila Principles, that nations across the globe follow while framing guidelines for the regulation of intermediaries, mentions:

- Intermediaries should be shielded from liability for third-party content uploaded on its platform.
- Content must not be restricted unless by an order by a competent judicial order.
- Requests for take down of content must be clear and follow due process.

- Laws and content restriction orders must comply with the tests of legality, necessity, and proportionality.
- Transparency and accountability must be built into laws and content restriction policies.

In this regard, **CCAOI believes that the Amendment fails to adhere to the above mentioned global standards and judicial precedents in India** . The Amendment proposes changes which go way beyond the practices intermediaries ought to undertake while maintaining neutrality in relation to the content on their platforms. The Amendment significantly affects not only the status of intermediaries but also affects third-party users' constitutional rights in India.

Please find see our detailed comments to the **specific changes proposed by the Amendment** below.

1. **Disclaimers** – The existing Intermediary Guidelines impose an obligation on intermediaries to inform users using its platform not to post content of certain nature such as content that is defamatory, harmful to children, blasphemous, etc. The Amendment introduces two additional disclaimers, namely, information that threatens public health and safety, and critical information infrastructure.

The Amendment fails to prescribe any specific considerations on how content is likely to threaten public safety, health, or critical information infrastructure in India. Since the Constitution allows for restriction on the freedom of speech and expression under the particular grounds identified therein, this provision is likely to be arbitrarily interpreted, which may, in turn, impose unreasonable restrictions on the freedom of speech and expression. Since the Shreya Singhal case has clarified that any restriction on free speech must be within the contours of Article 19(2) of the Constitution, this provision is in contradiction to the SC's ruling.

2. **Monthly Information** – Under the provisions of the Amendment, intermediaries are now required to inform its users that “non-compliance with rules and regulations, user agreement and privacy policy” may lead to the termination of access or usage rights and removal of non-compliant information once every month.

This provision is not only burdensome for intermediaries in terms of increased expenditure on such compliance, it may lead to notification fatigue among users using the intermediary's platform. Given the lack of a causal link between the result to be achieved and measures adopted under the Amendment, we are of the view that such a change in the existing Intermediary Guidelines is not necessary. We would rather propose that whenever there is an updation of policies or services, the intermediaries can notify the same to their users.

3. **Tracing the originator of information** – The Amendment mandates intermediaries to trace the originator of information uploaded on the platform if and when required by government agencies and within 72 hours of such request. Additionally, intermediaries are required to provide any information and assistance “as asked by any government agency or assistance concerning security of State or cyber security;

or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto” upon receiving such lawful order. This provision falls short of providing for procedural safeguards or adequate justification with respect to requests made by government agencies. This provision seems to be in contravention of the SC’s ruling in the case of *K. Puttaswamy v. Union of India* (Puttaswamy case), which upheld the right to privacy of an individual as a fundamental right granted to Indian citizens under Part III of the Constitution. In the Puttaswamy case, the SC laid down a three-pronged test of legality, necessity, and proportionality with respect to any action that limits the right to privacy –

- i. Legality – which postulates the existence of law;
- ii. Necessity – defined in terms of a legitimate state aim; and
- iii. Proportionality – which ensures a rational nexus between the objects and the means adopted to achieve them.

Furthermore, at times, intermediaries may need more than 72 to address such requests and follow due process.

4. **Incorporation of Indian entity and designation of nodal officer** – The Amendment imposes an obligation on intermediaries with more than 50 lakh users, to establish a presence in India by incorporating an entity and registered office in India. Additionally, intermediaries are now required to designate a nodal officer who shall be available 24 x 7 to interact with the law enforcement agencies in India. While the intent may be to increase accountability of such intermediaries, we are of the opinion that intermediaries guidelines is not the appropriate document for incorporating such requirements to make companies more accountable.

5. **Blocking Orders** – The Amendment mandates intermediaries to remove any unlawful content within 24 hours of actual notice by a court or government agency. However, the Amendment does not provide for adequate safeguards when such take down request is made by a government agency without judicial authorization. Such a requirement can be abused due to the lack of adequate safeguards. Additionally, as noted by the Supreme Court in *Shreya Singhal*, Section 79 of the Information Technology Act is an exemption provision and cannot be used for issuing blocking orders.

Additionally, the proposed time frame of 24 hours to remove content does not allow an intermediary to review the request before taking down content. This is likely to result in third-party action against the intermediary for such take down. The Amendment also fails to provide for safeguards with respect to retaining records for 180 days or “such longer period as required by government agencies or courts”.

6. **Monitoring** – The Amendment requires intermediaries to proactively screen content that is hosted or uploaded on its platforms, which is in contradiction to the SC’s ruling in the *Shreya Singhal* case. The SC has clarified that intermediaries must not be required to screen content or assess the legality of such content. Not only does this

requirement impose a restriction on the right to free speech and expression, and right to privacy, it is also unreasonable for intermediaries to carry out such monitoring.

Further, by tying intermediary safe harbour to content monitoring, the government could require intermediaries to weaken the security of their services. For end-to-end encrypted services, only the sender and receiver of information have access to the content. No third party, even the intermediary providing the service, has access to that content. When intermediaries are required to proactively screen content on its platform, end-to-end encryption is no longer usable. The government should refrain from asking intermediaries to proactively screen content as that will not only erode trust of people, weaken the use of strong encryption and lead to censorship, but will also fail to achieve the objectives which the government is aiming at, while impacting all intermediaries.^[1] There are no easy answers to the discussion around proactive monitoring, encryption and lawful access. However, through identifying nuances, areas for improvement adhering to international principles or norms and through public and private cooperation the issues can be addressed to a considerable extent^[2].

Concluding Remarks:

To achieve the objectives of National Digital Communications Policy, 2018 of ensuring online trust, security, and privacy, , the Government must ensure that a symbiotic relationship is maintained between intermediaries, users, and the regulator. Since intermediaries facilitate day-to-day activities such as access, communication, business and trade, information and social media, any regulation of intermediaries should be aimed at allowing intermediaries to function in a smooth manner without adversely affecting the digital economy or imposing unreasonable restrictions on the rights of the users. The Government should ensure that intermediaries are not burdened with extensive, stringent obligations, which may hinder their ability to enter the Indian market or provide quality services to existing users.

1265/MeitY/ISPAl/19

MIT/79/039

January 21, 2019

To,
The Group Coordinator (Cyber Laws and E-Security Group)
Ministry of Electronics & Information Technology
Electronics Niketan 6,
CGO Complex, Lodhi Road
New Delhi – 110003

Subject: ISPAl comments on Draft "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

Dear Sir,

We thank you for inviting comments on the proposed draft on Information Technology (Intermediary Guidelines [amended]). We hereby submit the following comments with respect to the same:

1. At the outset, it is submitted that the definition of Intermediary in the IT Act is inclusive in nature. The Information Technology Act, 2000 (hereinafter, 'IT Act') defines an 'intermediary' as under:

"Section 2(w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

Intermediary is defined with respect to any particular electronic record means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record. The definition covers Telecom Service providers, Network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes. However, the definition does not specifically cover social media sites like Facebook, Twitter, Google-Youtube etc. which are content aggregators and other content provider sites.

The due diligence obligation is in respect of the content which is posted on the internet through any of the content aggregator sites by individual users of that website. It is our submission that the obligation of due diligence on the content should be of the intermediaries who are aggregating such content from the users and it would be unfair to obligate the ISPs to block such content by imposing obligations on ISPs in the name of due diligence. It is submitted that as far as attribution of duties to different intermediaries are concerned, they should also be distinct keeping in mind the nature of the said intermediaries. It is submitted that on the same principle different intermediaries should also have different standards of due diligence within the meaning of Section 79 (2) (c). It is further submitted that since different intermediaries are not situated similarly, the prescription of same standards of due diligence for all intermediaries would render the guidelines arbitrary as being violative of Article 14 of the Constitution of India.

2. It is submitted that it should be clarified as to which Rule/Sub-Rules applies to which kind of Intermediary so that there is no room for any confusion.
3. It is submitted that Rule 3 (4) should apply to content aggregators, web hosting service providers or content providers and should not apply to intermediaries who are providing merely access to internet which come under the purview of the 'safe harbor' regime satisfying the requirements of Rule 3 (3).
4. It is submitted that in Rule 3 (5) the term lawful order should be defined, moreover the term any government agency should also be defined considering that right to privacy has been recognized as a fundamental right hence the definition of the government agency on whose behest/communication such information or assistance is to be provided should not be vague and hence there should be a well-defined mechanism as per which the concerned intermediary is expected to act for example the guidelines laid down by the Supreme Court in the case of *PUCL v. UOI*, (1997) 1 SCC 301. It also needs to be clarified that Rule 3(5) is applicable only to those intermediaries who are providing platform base services and is not applicable to ISPs.
5. It is submitted that in Rule 3 (7) the number of users in India should be reduced to 10 lakhs.
6. It is submitted that the said Rule 3 (8) cannot be applied to Internet Service Providers providing access to the Internet as it make the said sub-rule ultra-vires section 79 of the IT Act. Section 79 (3)(b) of the IT Act. Section 79 (3)(b) of the IT Act is reproduced below:

“(3) The provisions of sub-section (1) shall not apply if-

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

It is submitted that since the Internet Service Providers providing the services of access to the Internet does not control any computer resource in which any information data or communication link resides or is connected to within the meaning of Section 79(3)(b) of the IT Act and hence the same does not apply to such ISPs.

7. Without prejudice, it is submitted that in Rule 3 (8) the blocking mechanism under Section 69 of the IT Act should be followed. It is further submitted that in *Shreya Singhal v. Union of India*, AIR (2015) SC 15523 the Apex Court advertent to Section 79 (3) (b) as amended by the Act concluded that in paragraph No.122 observed as follows:

Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

8. It is submitted that a bare reading of these observations clearly indicate that the kind of intermediaries that were being contemplated by the Hon'ble Supreme Court were content aggregators/content hosting intermediaries such as Facebook and You Tube. It is submitted that before blocking the access to website the mechanism laid down in Section 69 of the IT Act has to be

complied with by intermediaries who provide access to internet and in light of the same, it is requested: -

- a) The term "Appropriate government or agency" should have a clear and definite meaning.
- b) It is submitted if the service providers, providing access to the internet have to comply with any request under this subrule then a mechanism should be laid down which is consistent with the obligation of ISP's under Section 69 of the IT Act. Hence the government agency should be the government authority who is empowered to issue a blocking order under Section 69 of the IT Act.

It is submitted if the above twin requirements are satisfied then the objective of reading down of Section 79 (3) (b) would be fulfilled in the actual sense.

9. In response to Rule 3 (9) it is submitted that it should be clarified that the said clause is not applicable to internet service providers, providing access to the internet services in light of them satisfying the proviso to subrule 3. It is submitted that if the said ISP's are obligated with the duties laid down in the said clause, the performance of the same would be inconsistent with the conditions laid down in the twin provisos to subrule 3 which would lead them to lose their immunity under the said 'safe harbor' provision and the same can never be the objective of this subrule.

10. It is submitted that rule 3 (12) is not applicable to the ISP's who are providing access to the internet services as it applies to intermediaries which provide web hosting / content hosting / content aggregation services.

Thanking You,

Best Regards,
For Internet Service Providers Association of India



Rajesh Chharia
President
+91 - 9811 038 188
rc@cjnet4u.com

MIT/79/040



ESYA
centre

**Response to the Draft Information
Technology [Intermediary Guidelines
(Amendment) Rules], 2018**

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by Media)

30 January 2019



Response to the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018

We at the ESYA Centre, greatly appreciate the opportunity given to us by the Ministry of Electronics and Information Technology (MeitY) to respond to the draft 'Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 ("Draft Rules"), which seek to replace the rules notified in 2011. We appreciate that MeitY has undertaken to reform and clarify issues on Internet governance through these rules.

However, after a thorough analysis of these rules, we believe a more holistic understanding of evolving technologies, and global trends in Internet governance may be instructive for MeitY to take this discussion forward. As such, we have approached this analysis from a broad, techno-legal perspective, highlighting the major thematic areas under each proposed rule, rooting our arguments in broader discourses on internet governance and the attendant rights and obligations of stakeholders.

Therefore, **Part I** of this response will provide a brief snapshot of some of the proposed Rules, and how they can be revised to comply with prior legislative jurisprudence, and best practices. **Part II** will delve into a more detailed discussion on the broader principles of regulatory governance. We hope that these thematic discussions will prove instructive in a larger discourse about the growing Internet ecosystem in India.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Part I

Comments on the Draft Rules

Draft Rules	Text of the Draft Rule	Comments
1	<p>Short Title and Commencement – (1) These rules may be called the Information Technology Intermediaries Guidelines (Amendment) Rules, 2018. (2) They shall come into force on the date of their publication in the Official Gazette.</p>	<p>Although the Draft Rules intuitively fall under section 79 of the Information Technology Act, 2000 (IT Act), this is not currently specified. It may be useful to clearly state the principal provision under the IT Act to avoid future challenges on this basis.</p>
2(k)	<p>“Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;</p>	<p>An intermediary, as defined in the IT Act includes a vast array of service providers, ranging from internet service providers to cyber cafés. Given the various types of intermediaries involved and the evolving nature and functions of different classes of intermediaries, it is important that regulations applicable to them are graduated and differentiated.</p>
3(2) and 3(8)	<p>Rule 3(2): Rules and regulations, privacy policy and user agreement to be published by the intermediary to not allow for certain information.</p> <p>Rule 3(8): (8) 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</p>	<p>From a plain reading of the provisions, there appears to be an inconsistency between the list of objectionable and unlawful information mentioned under Rule 3(2), and unlawful acts mentioned under Rule 3(8). It may be helpful to either provide clarity on the distinction maintained for what is unlawful under the two provisions, or to harmonize the two. This will also help in better compliance of the provisions by intermediaries and users.</p>

	<p>section 79(3)(b) of Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.</p>	
3(4)	<p>The intermediary shall inform its users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.</p>	<p>The requirement to inform users “at least once every month” is a welcome step towards appraising users of the content take down and termination of access policies. This can be supplemented by providing useful context to users about the nuances of a company’s privacy policy, rules and regulations, and user agreements. One way of doing this is to provide details to users every time there is a change in the user agreements, or privacy policy, or the laws, in a clear and succinct manner, giving users greater autonomy over their choices on the internet.</p>

3(5)	<p>When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.</p>	<p>This Rule could have significant implications on the users' right to freedom of expression, and potentially requires intermediaries to intervene and break encryption on secure communication platforms. It also does not lay down qualifications for the use of these powers by the State, violating the users' right to privacy, which was held to be Constitutionally protected in the <i>Puttaswamy</i> judgment¹.</p> <p>There are problems with the construction of the provision as well. When unqualified access to all data is being requested by the State, the language of the provision should be restrictive, rather than illustrative. This is evidenced by the phrase “...and matters connected with or incidental thereto”. Therefore, a creative rather than restrictive reading would allow unfettered access of data to the State, without having to define narrowly the reach of this Rule.</p>
3(7)	<p>The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:</p> <ul style="list-style-type: none"> (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and 	<p>The rule applies to intermediaries with 50 lakh users, a number that represents 1.43% of India's Internet user base. There is no clear justification as to how this number was arrived at, and whether it signifies active users, subscribers, etc².</p> <p>Further, the aim of requiring certain intermediaries to be incorporated under the Companies Act, 2013, and to have a permanent physical office in India is unclear. If it is for law enforcement to have a point of contact for</p>

¹ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

² Nikhil Pahwa, Medianama, 22 January, 2019, “A serious and open threat to Internet in India”, available at <https://www.medianama.com/2019/01/223-a-serious-and-imminent-threat-to-the-open-internet-in-india/>.

	<p>alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.</p>	<p>communication or issuing directions, it could be accomplished by Rule 3(7)(iii). The proposed requirements in Rule 3(7)(i) and 3(7)(ii) would place entry barriers on smaller intermediaries, whether based in India or outside, who may not have the financial means to set up a physical company in India. There must also be clarity over the intent behind having a dedicated nodal person of contact, provided for in Rule 3(7)(iii). If the intent is to accrue liability to one person designated in India, that may still be difficult to implement. For example, there could be problems with extradition (as has been seen in previous instances of people fleeing the country to escape prosecution³), and it could also potentially sour relationships with intermediaries and foreign governments⁴, who could have better served as mutual aides.</p>
3(8) and 3(5)	<p><i>Provided above</i></p>	<p>While Rule 3(8) specifies that court or governmental orders can require intermediaries to remove or disable access to content only if the content relates to the restrictions provided for in Article 19(2) of the Constitution (per <i>Shreya Singhal</i>⁵), Rule 3(5), which is much wider in scope and has potentially greater implications for free speech, does not contain any such restrictions.</p> <p>Further, the “information or assistance” requested from intermediaries in Rule 3(5) is wide enough to also potentially cover blocking or disabling access to content, and does not contain Article 19(2) restrictions, nor does it</p>

³ The New Indian Express, 31 July, 2018, “Vijay Mallya Extradition case: India has weak extradition treaties”, available at <http://www.newindianexpress.com/nation/2018/jul/31/vijay-mallya-extradition-case-india-has-weak-extradition-treaties-1851272.html>.

⁴ The Telegraph, 18 December, 2004, “US slips in word for web loss”, available at <https://www.telegraphindia.com/india/us-slips-in-word-for-web-loss/cid/690202>.

⁵ *Shreya Singhal v Union of India*, AIR 2015 SC 1523.

		provide for judicial oversight. It can therefore potentially be used to circumvent the restrictions placed in Rule 3(8).
3(9)	The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.	<p>This Rule applies to all intermediaries, homogenously, without taking into account their size, function etc. This means that even intermediaries like cyber cafes, and regional news websites, amongst others, would also need to deploy these mechanisms; who may not have the resources to comply with this requirement, and hence may need to shut down.</p> <p>Further, this rule effectively delegates censorship and content moderation to intermediaries, who are motivated by profit and not user rights. It also does not define what “unlawful information or content” is, and intermediaries are likely to err on the side of over-enforcement to absolve themselves of liability. It does not provide for a judicial determination of unlawful content, or for any appeal or redressal mechanism. It also does not account for the limitations of automated tools and machine learning technology, and would significantly impair users’ right to freedom of expression.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Part II

Broad Principles of Internet Governance

Cyberspace is a complex ecosystem that has evolved to encompass the breadth of human activity within its fold, from commercial considerations, interpersonal matters, to issues of governance. However, along with a rise in prosperity the expansion of cyberspace has also birthed newer forms of malevolence. Resultantly, institutions are moving to regulate and monitor activity on cyberspace more closely, to insulate society from the broader harms presented by it, and to also ensure that the broader principles of democratic governance and constitutionality are observed when passing laws to regulate it. To this end, we analysed the Draft Rules, and gave specific comments in the previous Part (I), and in this Part (II), chart a principle-based underpinning to the governance processes will help evolve a more durable framework for Internet governance, and policy discussions. Thus, in the following section, we have delineated some of these principles, and highlighted how the Draft Rules may be harmonised with them.

However, before commencing a discussion on the Draft Rules, it must be noted that in this response, we largely understand intermediaries to mean ‘Internet intermediaries’, referring to a wide, diverse and rapidly evolving range of service providers that facilitate interactions on the Internet between natural and legal persons⁶.

Principle 1 - Blurring distinctions between the ‘State’ and ‘private parties’: The State must ensure that the unfettered power to seek information, and actively monitor content online is qualified both for the State and the intermediaries

There is an increasing blurring of distinction between the State/Government, and private parties in the form of intermediaries, in the regulation of online content, given the data analytic capabilities of big intermediaries. In this regard, Draft Rules 3(5) and 3(9) demonstrate a shift of responsibility of Internet governance and monitoring, seemingly from the State to the intermediaries. Further, these Draft Rules grant both the State, and the intermediaries the unfettered power to seek out any information they want, which may lead to instances of automated or conscious profiling, and discrimination. The Draft Rules particularly fail to lay down qualifications for the use of this power by the State, leading to a violation of a person’s right to privacy, a right now espoused and enshrined in judicial consciousness through the *Puttaswamy*⁷ judgement, which established that privacy forms the constitutional core of human dignity and autonomy⁸. A key part of this right has been conceptualised to include not only the control of personal information, but also the right to inaccessibility, and the right to subjectively desired inaccessibility⁹. Therefore, in light of the *Puttaswamy* judgement, the legality of provisions

⁶ For this understanding, we have referred to the Council of Europe’s “Roles and Responsibilities of Internet Intermediaries”, available at <https://rm.coe.int/leaflet-internet-intermediaries-en/168089e572>.

⁷ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

⁸ Bhandar and Sane, Socio Legal Review, Vol 14, “Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018”, pp. 147.

⁹ C Hunt, (2011) 37:1 Queen’s LJ, “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort”, pp. 173.

allowing for active policing by the State, and the imposed obligations on intermediaries to do the same, is suspect. Looking to international treatments, the Council of Europe also recommends that State authorities should not directly or indirectly impose a general obligation on intermediaries to monitor content which they merely give access to, or which they transmit or store, be it by automated means or not, and also impose proportionate sanctions for failure to comply, to avoid restriction of lawful content, and a resultant chilling effect on the right to freedom of expression¹⁰.

This issue of asymmetry of agency between citizens vis-a-vis the State and powerful intermediaries gains special importance in the absence of a comprehensive legislation on surveillance and privacy, the expansive mandate given to State authorities and law enforcement agencies operating through myriad laws and executive orders, and the express lack of judicial oversight in India.

Principle 2 - Upholding User rights: The State must ensure that any legislation or rules thereunder pertaining to cyberspace does not curtail user rights

a. *The Problems with Intermediary Oversight*¹¹

We understand why MEITY is considering placing greater responsibility on intermediaries to regulate behaviour on their own platforms. Cyberspace may be too vast for State agencies, in their current form and capacities, to manage alone. This is a trend that is being followed globally. Illustratively, the United States (US) enacted two statutes in 2018 – the Allow States and Victims to Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act (FOSTA-SESTA). FOSTA-SESTA was passed with the goal of mitigating sex trafficking online. These laws impose a limitation on the safe harbour provision in the US Telecommunications Act, 1996. Section 230 of the Communications Decency Act, which falls under the broader US Telecommunications Act holds that Internet intermediaries, like social media websites and internet service providers, cannot be held accountable for user-generated content posted on their platforms. FOSTA-SESTA carves out an exception to this protective rule, stating that Internet intermediaries would be held responsible if advertisements soliciting sex showed up on their websites.

The initial dearth of regulation on Internet intermediaries, coupled with the dotcom crash in the early 2000s, compelled these entities to develop business models that centred on the monetisation of user data. The data is collected largely through user engagement on the platform, and then sold to third parties who largely use it for advertisement purposes. Thus, the prime commercial motivation for intermediaries is to encourage the generation of as much user data as possible.

¹⁰ Council of Europe, “Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries”, pp. 1.3.5 -1.3.6

¹¹ As enunciated by one of the authors of this response in Meghna Bal, “Regulating Online Intermediaries: We Need to Start Focussing on User Rights,” *Firstpost*, December 17, 2018, <https://www.firstpost.com/tech/news-analysis/regulating-online-intermediaries-we-need-to-start-focusing-on-user-rights-5745201.html>.

As the vulnerability of these datasets has become increasingly apparent, regulators have started issuing data protection norms to govern how they are collected and processed. These regulations directly curtail the ability of intermediaries to gather user data. The extent of the effect these regulations have on the value of an intermediary may be evinced by the enactment of the General Data Protection Rules (GDPR) in Europe and the subsequent drop in the market capitalisation of one Internet intermediary by USD 123 billion,¹² even though there are reports stating that the GDPR did not hold back the digital marketing tide¹³. Therefore, in times of great legislative changes, the impact on the market, and on the ability of intermediaries to cope with these changes will have to be considered by any prudent State. This may also be the reason why intermediaries are also driven to resist any legislative action that would oblige them to regulate user behaviour on their websites or hinder their ability to collect user information.

In the context of increased intermediary liability obligations, intermediaries may overzealously enforce legislative and policy mandates to avoid further regulation, sometimes to the detriment of user rights. These may include the constitutionally protected and internationally recognised rights¹⁴ of users to freedom of expression, privacy, religious freedom, public participation, information, and assembly. Illustratively, FOSTA-SESTA's enactment prompted one prominent social media platform to amend its community guidelines to prohibit sexual solicitation of any kind. These guidelines go as far as forbidding implicit sexual solicitation through either suggestive comments or images. Justifiably, activists are concerned that these guidelines may lead to an inordinate level of censorship of speech online. It is therefore necessary for regulatory policies concerning intermediaries to be framed around principles of creating strong digital ecosystems of accountability, like encouraging more transparency in reporting on operations, to protect against potential harms.

b. Interplay with Shreya Singhal

The Draft Rules have significant implications for free speech, and run directly counter to the Supreme Court's directions in the *Shreya Singhal* case. The case dealt in part with the safe harbour provision available to intermediaries under the IT Act, which provides that intermediaries would lose their safe harbour protection under section 79 of the IT Act and be liable for content posted on their platforms, if they failed to act upon having actual knowledge of illegal content. In this respect, the Supreme Court read "actual knowledge" to mean a notice to Internet intermediaries in the form of a court order.¹⁵ This meant that the courts, and not the intermediary, would have to subjectively determine what would constitute illegal content. However, the Draft Rules, through Rule 3(9), now effectively outsource the determination of what constitutes lawful speech

¹² Romain Dillet, "Facebook Officially Loses \$123 Billion in Value," *Tech Crunch*, July 2018, <https://techcrunch.com/2018/07/26/facebook-officially-loses-123-billion-in-value/>.

¹³ MediaPost, "GDPR did not hold back the digital marketing tide", available at <https://www.mediapost.com/publications/article/331209/>.

¹⁴ United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, p.3; available at <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>

¹⁵ *Shreya Singhal v Union of India*, AIR 2015 SC 1523, para 117.

to private companies, which is something that neither they, nor the State should do, without judicial oversight.

In this context, it is also important to note that the State can only restrict speech on the grounds specified in Article 19(2), and in a manner that is necessary and proportional to meet those grounds. In *Shreya Singhal*, the Supreme Court specified that “unlawful acts” in Section 79(3)(b) of the IT Act would have to conform to Article 19(2) restrictions.¹⁶ Rule 3(9), which requires Internet intermediaries to proactively monitor their platforms for unlawful content, does not reflect this restriction.

c. The chilling effect on free speech

One of the primary issues with draft Rule 3(9), is the requirement to proactively identify and remove access to “unlawful information or content”. This is problematic for a number of reasons. First, the rules do not define what would constitute as “unlawful” information or content, leaving intermediaries with no guidelines to assess the standards they should use. This is compounded by the fact that it is often difficult to assess whether controversial content is constitutionally protected. For example, although various legislations broadly detail the types of expression that would attract criminal liability, accurately assessing whether a particular picture or statement, for example, intends to “outrage the religious feelings” or “insult the religious beliefs” of a class of persons¹⁷ is not something private parties are equipped to do.

Therefore, in order to absolve themselves of liability, intermediaries are likely to over-censor content and err on the side of over-enforcement, and take down even legal but controversial content. This is something that has occurred before in the context of Internet intermediaries,¹⁸ and would significantly chill free speech and reduce the quality of discourse around uncomfortable, but often necessary and important issues. Given the volume of data published online and the resources that Internet intermediaries would require to monitor all this data, this measure could vastly reduce the volume of information that is even available online, with a severe impact on the extent and diversity of online communication.

d. Ineffective redressal mechanisms

Globally, Internet intermediaries have been criticised for not being transparent about their processes, and for the lack of effective redressal mechanisms for appealing content takedowns¹⁹. Even if content is later reinstated, content removal and account suspensions during public protest or debate could significantly harm users’ political rights, and impair discourse.

e. Larger social context

¹⁶ *Shreya Singhal v Union of India*, AIR 2015 SC 1523, para 117.

¹⁷ Section 295A, Indian Penal Code, 1860.

¹⁸ Rishabh Dhara, Centre for Internet and Society, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, available at <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf>

¹⁹ United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, p.13; available at <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>

We appreciate that the Draft Rules are an attempt to reduce misinformation on online platforms. In this regard, it is also useful to remember that the provisions on safe harbour were meant to serve as an incentive for more responsible regulation of the Internet. However, we question whether there is any discernible benefit in the Draft Rules seeking to change this incentive based regulatory framework, by actively encouraging intermediaries to censure and surveil all content on the Internet. We argue that it may be essential to also assess whether increasing intermediary liability is the best, or even an effective way to address what are essentially human, social issues. Doing so would make sure that the regulations framed do not just serve to reactively address specific symptoms (which may change form and require further regulation), but serve to regulate the cause of such information online. The first step in this assessment would be to undertake in-depth and evidence-based research (based on previous instances of unrest) to ascertain the role that Internet intermediaries play in spreading misinformation, and the extent to which any censorship or content takedown methods were effective in achieving their aims.²⁰ Research suggests a correlation between online hate speech and anti-immigrant crime in Germany, but it is unclear whether the existing anti-immigrant sentiment drove online hate speech, rather than the converse.²¹ Some Internet intermediaries have commissioned related studies,²² and the State would be well placed to commission independent studies as well. In any case, an effective response to misinformation online would require the different stakeholders to proactively work together to develop and publicise ways to, for example, verify the truth of claims found on online platforms.

Principle 3 - Ensuring Transparency and Accountability: The State must ensure that legislation or rules thereunder pertaining to cyberspace upholds globally accepted principles of transparency and accountability for all relevant stakeholders

The value of transparency (both from intermediaries and the State) in safeguarding user rights and promoting accountability cannot be overstated. For the meaningful and effective exercise of free speech and information rights on digital media platforms, users must have a clear understanding of what kind of content they can and cannot post, and the reasons for and number of takedowns and account suspensions.

a. Intermediary Transparency

It is in the interest of all stakeholders for intermediary platforms to be transparent with policy-makers and users about the limits and abilities of technologies they deploy, with the help of specific case studies, to effectively demonstrate the extent of human intervention and judgment required in assessing controversial content online²³ (especially as it relates to issues of

²⁰ Anja Kovacs, *5 Ways in which the Indian Government can improve its responses to hate speech online*, available at <https://internetdemocracy.in/2012/09/5-ways-to-improve-responses-to-hate/>

²¹ Karsten Müller and Carlo Schwarz, *Fanning the Flames of Hate: Social Media and Hate Crime*, available at <https://dx.doi.org/10.2139/ssrn.3082972>.

²² Facebook Research, *Announcing the Whatsapp Social Science and Misinformation request for proposals*, available at <https://research.fb.com/announcing-the-whatsapp-social-science-and-misinformation-request-for-proposals/>.

²³ Anna Windemuth, Rachel Brown, Yuan Tian and Imogen Sealy, *Wikimedia panelists tackle the future of intermediary liability*, available at <https://wikimediafoundation.org/2018/08/02/intermediary-liability-future-panel/>.

misinformation and “fake news”, where much of the content is highly localised and context-based), and the difficult choices they can be required to make.

Secondly, encouraging transparency by Internet intermediaries with respect to the volume and details of content takedowns (both pursuant to State requests and company terms of use), and the decision-making process relating to handling relevant content, would go a long way in providing clarity to users and policy-makers on the metrics used for content regulation on platforms,²⁴ and in promoting consistency and accountability. It would also contribute to the creation of a “case law” of sorts, which would enable stakeholders to understand how intermediaries interpret and implement their standards.²⁵ Since companies currently can face legal risks relating to transparency on this front, it might be useful to consider granting intermediaries a transparency safe-harbour, which would encourage them to provide more information and being transparent, without fearing legal liability; and also provide a basis for informed engagement between Internet intermediaries, policy-makers, civil society and users.²⁶

b. State Transparency

Given the magnitude of user rights at stake and their importance in preserving our democratic institutions, it would be beneficial for the State to not think of regulation as a way of imposing liability on intermediaries, but to explore ways to enable the public to make meaningful choices about how to engage with online platforms.²⁷ Users can only make informed decisions on how best to engage on intermediary platforms if the relationship between the State and intermediaries is meaningfully transparent.²⁸

The Draft Rules, and the IT Act in general, currently do not provide for this kind of transparency. For example, State agencies are not required to provide details regarding the volume and types of content sought to be taken down, methods of inter-operability between various ministries and departments, actions sought (for example, blocking, partial or full takedown of content), etc. Further, Internet intermediaries may sometimes also be restricted from making such information public as part of their transparency reports or otherwise.

²⁴ United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, available at <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>.

²⁵ United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, p.19; available at <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>.

²⁶ Tiffany Li, Information Society Project, Yale Law School, *Beyond Intermediary Liability: The Future of Information Platforms*, available at https://law.yale.edu/system/files/area/center/isp/documents/beyond_intermediary_liability_-_workshop_report.pdf.

²⁷ United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, available at <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>.

²⁸ United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, pp.16, available at <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>.

Introducing a requirement to provide information regarding the interaction of the State with Internet intermediaries would go a long way in promoting accountability on both sides.

Principle 4 - Following Regulatory Best Practices: The State must ensure that globally accepted regulatory best practices are followed, to achieve optimal outcomes for internet governance

It is imperative for the State to frame stable and responsive regulations, taking into account evolving questions of the operation of technology, sharing and access, and the impact on the market. This is crucial in understanding the intersectionality of Internet governance, user rights, and interests of the State, and it will be meaningful to create a charter of regulatory principles, which can then find their place in any policy, or law that the State creates – both for public interest, and for creating a culture of accountability, as mentioned in the previous section. To do so effectively, the State must identify the specific issues it wants to regulate, provide cogent rationale for interventions, and the potential impact on people and businesses. Without a framework of predictable, responsive governance in India, there is a high probability of “global innovation arbitrage”, with innovators, businesses, and eventually the market shifting to regulatory regimes that are more hospitable to entrepreneurial activity²⁹.

a. Moving towards non-deterministic governance

Global best practices reveal several ways in which technological regulations can be made responsive and reflexive. One such example is the use of regulatory sandboxes, which can provide innovators the space to evolve new technologies without the burden of complying with regulations, and allowing the regulator to, in turn, be responsive, and use evidence and outcome-based research to inform further regulation. This approach necessitates more collaborative law making with other associated regulatory and State agencies to craft harmonised laws, optimise regulatory capacity, and make laws forward looking. This will aid in identifying big technological and appropriate governance trends for the future, and their impacts on markets and people on markers such as productivity, demography, and ethnography. This is substantiated by research, which states that for emerging science and technology issues, a non-deterministic approach to governance works much better in accommodating the various uncertainties about the future³⁰. It has also been noted that technologically neutral regulations can often be sub-optimal because of the problem of prediction, that is, laws may not be able to adequately regulate new technologies, unless such new technologies become known, or else, we risk referencing older technologies. Therefore, a combination of technology neutrality and specificity, may better serve policy goals by improving legal tailoring, reducing legal uncertainty, increasing statutory longevity, and promoting treating like technologies alike³¹.

b. Encouraging self-governance and principle-based regulations

²⁹ Adam Thierer, The Technology Liberation Front, August 22, 2016, “Global Innovation Arbitrage: Driverless Cars Edition”, available at <https://techliberation.com/2016/08/22/global-innovation-arbitrage-driverless-cars-edition/>.

³⁰ Kuhlmann, S., Research Policy, “The tentative governance of emerging science and technology—A conceptual introduction”, pp. 2, available at <https://doi.org/10.1016/j.respol.2019.01.006>.

³¹ Greenberg, Minnesota Law Review, 100:1495, “Rethinking Technology Neutrality”, pp. 1498-1500, available at http://www.minnesotalawreview.org/wp-content/uploads/2016/04/Greenberg_ONLINEPDF.pdf.

This means that the State must also encourage the development of self-governance standards, and voluntary codes of conduct to pursue newer and evolving perspectives on looking at newer challenges. This must be aided by regulations that are simple, certain, and accompanied by safeguards, and Constitutional values and principles. Further, older regulations that do not meet these regulatory standards should be periodically reviewed for their adequacy³². For instance, in the EU, regulations have been prescribed to have sunset provisions with periodic review of old and obsolete laws³³.

Principle 5 - There must be graduated and differentiated regulations for different classes of intermediaries

We urge that regulations on intermediaries be graduated, and differentiated for different classes of intermediaries, considering their heterogeneity, with differences in size, function, and convergence of services. Regulations that attempt to attach liability to this vast group as a homogenous class, run into the dangers of crafting a disproportionate liability framework, with no distinctions being made on the basis of the roles of intermediaries as publishers, mass-media, gate-keepers who control access to information etc.; making the law rigid, and unresponsive to future technological changes.

This has also been recommended in Europe, where Member States have been told to consider this heterogeneity to prevent possible discriminatory effects³⁴. They also recommend that apart from applying a graduated and differentiated approach, States must also determine appropriate levels of protection, as well as duties and responsibilities according to the particular role of the intermediary³⁵.

Principal 6 - Promoting good governance: There must be a shift from a culture of ‘liability’ to one of ‘responsibility’ for approaching questions of intermediary liability

There is significant global discourse on reviving the moral approaches to intermediary liability, with legal theory increasingly shifting from a framework of ‘liability’ to one of enhanced ‘responsibilities’ for Internet intermediaries³⁶. This is primarily under the assumption that the role of intermediaries is largely increasing in scope, and the potential for elevating the wider informational environment and users’ interactions is unprecedented. Therefore, increased public accountability and transparency may work far better in ushering good governance.

Further, several emerging economies such as Brazil are introducing civil liability exemptions for Internet access providers and other Internet providers. For hosting providers in particular, there are civil liabilities, except in cases of copyright infringement. In Europe, the European

³² American Legislative Exchange Council, “Six Principles for Communication and Technology”, available at <https://www.alec.org/model-policy/six-principles-for-communications-and-technology/>.

³³ European Parliament, EPRS, June 2018, “Review Clauses in EU Legislation“, pp. 10, available at [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621821/EPRS_STU\(2018\)621821_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621821/EPRS_STU(2018)621821_EN.pdf).

³⁴ Council of Europe, “Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries”, pp. 1.1.5.

³⁵ Council of Europe, “Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media”, pp. 7.

³⁶ G.F.Frosio, Ijlt Vol 13, ”Internet Intermediary Liability: WILMap, Theory and Trends”, pp. 25.

Commission, along with all major online hosting providers including Facebook, Twitter, YouTube and Microsoft, decided upon a code of conduct, including a series of commitments to combat the spread of illegal hate speech online in Europe³⁷. In Argentina, in the *Rodriguez M. Belen v. Google*³⁸ case, the Supreme Court held that intermediaries such as Google did not have any active monitoring obligation that could be linked to liability. We argue that while content moderation may help both intermediaries and law enforcement to filter unlawful and harmful content more efficaciously, it can be done in a more transparent and collaborative manner in the absence of any strict liability framework, and with joint development of mutually beneficial codes of conduct and standards.

Principle 7 - Upholding legal certainty of encryption: There must be legal certainty of preserving encryption for upholding the right of privacy for users

In the absence of certainty in the State's strategy and direction, evidenced from the lack of a coherent national encryption policy, having provisions such as the draft Rule 5, makes it uncertain and suspicious for users whether encryption would be broken to enable access for the State, or if encryption can be retained in the process at all, and how. We urge that the Draft Rules accord legal certainty to secure and preserve encryption, without any arbitrary qualifications.

Principle 8 - Mandating due process and judicial review: There must be due process and judicial review for orders to assist authorities in accessing information or content on the Internet

It is instructive to note that several countries across the world have ensured that robust and due processes are maintained with respect to provisions regarding obligations on providers to assist authorities. For instance, in the UK, section 253 of the Investigatory Powers Act 2016, states that the Secretary of State may give a telecommunications service provider a 'technical capability notice'. Such a notice may impose on the provider any applicable obligations specified, and require them to take all steps specified in order to comply with those obligations. This however requires the fulfilment of three requirements - (i) the Secretary of State must believe that the provider in question has the *capability to assist*; (ii) the Secretary of State must consider that the conduct required by the notice is *proportionate* to what is sought to be achieved by that conduct; and (iii) the notice must be *approved by a Judicial Commissioner*, who while deciding whether or not to approve the notice, must consider whether the notice is *necessary and proportionate*.

In Europe, Convention 108 on data protection specifically recommends that any demand or request by State authorities addressed to internet intermediaries to access, collect or intercept personal data of their users, including for criminal justice purposes, or any other measure which interferes with the right to privacy, should be *prescribed by law*, *pursue legitimate aims*, and be used

³⁷ European Commission, Press Release, May 31, 2016, "European Commission and IT Companies announce Code of Conduct on illegal online hate speech", available at http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

³⁸ WILMAP, M. Belen Rodriguez c/Google y Otro s/ daños y perjuicios, Corte Suprema [Supreme Court], Civil, R.522.XLIX, available at <https://wilmap.law.stanford.edu/entries/m-belen-rodriguez-cgoogle-y-otro-s-danos-y-perjuicios>.

only when it is *necessary and proportionate* in a democratic society³⁹. There are clear standards, which state that securing the restriction of illegal content by States with intermediaries must always be along the principles of *legality, necessity and proportionality*. States are urged to consider the fact that automated means, which may be used to identify illegal content, *currently have a limited ability to assess context*⁴⁰.

It is not abundantly clear from Draft Rule 5, if such tests of judicial approval (even when the order is lawfully made by a State agency), or necessity and proportionality are strictly to be applied, since powers of decision-making rest solely with the State agency. Further, it is unclear as to what a lawful order is; with the term neither being defined in the principal Act, or the attendant Rules. This is reminiscent of Rule 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011, wherein there was considerable confusion over the term “lawful order”, being interchangeably used with the term “request in writing”, which implied that a 'lawful order' could simply be a written letter or notice from authorized State agencies, which did not bear adequate force of law, or due process. As such, the process is inordinately simplified, and the lawful order in effect simply becomes a notification/executive order of the State.

In the interest of transparency and protection against abuse of power, it may also be beneficial for the State to make available to the public in a regular manner, comprehensive information on the number, nature and legal basis of content restrictions or disclosures of personal data that they have applied in a certain period, through requests addressed to intermediaries under this proposed rule. Therefore, we urge that due process requirements and effective remedies should be facilitated vis-à-vis both the State, and intermediaries for the entirety of the Draft Rules.

Principle 9 - Harmonising legislations: There must be clear intent for mandating onerous obligations on intermediaries, with attempts to harmonise legislations that specify different requirements for foreign companies carrying out business in India

With respect to foreign intermediaries that are operating in India, it is important to note that the Companies Act, 2013 does not impose the obligation of a foreign company to necessarily have a physical presence in India to conduct business. The Companies (Registration Offices and Fees) Rules, 2014 state explicitly that foreign companies carrying out business in India through an electronic mode may have their main servers located either in India, or abroad. A physical presence in India has till now, mostly been mandated for banks, but that has been with an express intent to counter money laundering concerns, and *benami* transactions⁴¹, along with offering significant protections like that of deposit insurance.

This is also evidenced world-wide, where regulators impose such obligations primarily on cross-border financial intermediaries like banks, pension funds and mutual funds, for considerations of

³⁹ Council of Europe, European Treaty Series No 108, “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, available at <https://rm.coe.int/1680078b37>.

⁴⁰ Council of Europe, “Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries”, pp. 1.3.8.

⁴¹ Reserve Bank of India, Extracts from FATF-IX Report, Annexure, Annexure II, available at <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=281>.

investor protection, and efficient capital markets. The OECD guidance on regulating commerce intermediaries also notes that while the requirement for residency or physical presence may be reasonable for conventional commerce, it is questionable in the context of B2C⁴² electronic commerce, because such a requirement could result in businesses either restricting their trade or inadvertently failing to comply⁴³. Therefore, in the case of draft Rule 3(7), it is not clear as to what the larger goals sought to be achieved are, by mandating a physical presence, and how this provision will be harmonised with other extant legislations like the Companies Act.

Principle 10 - Understanding the economic impact of provisions: There must be reliance on data about the economic impact of removal of safe harbour provisions in India, to draft more responsive legislations

It has been documented that having less onerous, or at least differentiated compliance requirements would assist in helping start-ups, and increase the expected profit for successful start-up intermediaries by 5% in India⁴⁴. Further, the economic impact of weakening safe harbour provisions for Internet intermediaries can be significant. For example, the impact of that on the US economy has been estimated to be elimination over 425,000 jobs, and a decrease of the US GDP by \$44 billion annually⁴⁵. No such study has been conducted in the context of India, and it would be instructive to have unambiguous data on the impact of these Draft Rules on the ecosystem, before notifying them.

Principle 11 - Resisting proactive monitoring of information and content through automated tools: There must be insistence on taking measured steps to regulate online information and content, to prevent against widespread censorship; and expensive requirements for smaller businesses.

Draft Rule (9) states that intermediaries, as a matter of obligation, have to “proactively” identify and remove, or disable access to unlawful information or content. The rule is similar in many ways to Article 13 of the proposed Directive for Copyright in the Digital Single Market Directive in the EU⁴⁶, which requires platforms to proactively work with rights holders to stop users uploading copyrighted content. This was criticised, for obligating these platforms to scan all data being uploaded to sites like YouTube and Facebook, with the possibility of this being used for widespread censorship, and also creating a huge burden for small platforms, both in terms of resources, and liability. As such, a number of the Internet’s original architects and pioneers and their successors, including Wikipedia’s founder, and the World Wide Web’s inventor, expressed

⁴² B2C means ‘business to consumer’, please see <https://www.investopedia.com/terms/b/btoc.asp>.

⁴³ OECD, “Facilitating Collection of Consumption Taxes on Business to Consumer Cross-Border E-Commerce Transactions”, pp. 9, available at <http://www.oecd.org/tax/consumption/34422641.pdf>.

⁴⁴ 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.pdf>.

⁴⁵ Nera Economic Consulting, June 5, 2017, “Economic Value of Internet Intermediaries and the Role of Liability Protections”, pp. 2, available at <https://cdn1.internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf>.

⁴⁶ European Commission, COM(2016) 593 final, 2016/0280(COD), “Directive of the European Parliament and of the Council on Copyright in the Digital Single Market”, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593>.

their dissent by stating that the proposed rule was an “*unprecedented step towards the transformation of the Internet from an open platform for sharing and innovation, into a tool for the automated surveillance and control of its users*”⁴⁷. They further said that the cost of adopting necessary automatic filtering technologies would be expensive and burdensome, and yet those technologies have still not developed to a point where their reliability could be guaranteed.

Thus, we urge a re-think on the draft rule, because by obligating platforms to proactively scan information and content, the Rule not only impacts the business models of several small platforms, that would now have to invest in technologies to enable them to comply with this Rule, but also embed an automated infrastructure for monitoring and censorship deep into the networks of an intermediary will run contrary to the essential values on which the internet today functions for the users – freedom, and safety.

a. *Understanding Algorithmic oversight and its discontents*

Intermediaries are relying increasingly on algorithms to oversee the quotidian administration of their platforms. These algorithmic oversight mechanisms rely on the continual gathering and dissecting of vast amounts of current data to trigger automatic responses.⁴⁸ Algorithmic oversight systems present palpable advantages for regulating behaviour and ensuring desirable behavioural outcomes. However, there are some key issues with algorithmic oversight that make it an imperfect mechanism for the large-scale regulation and monitoring of human activity online.

- i. *Algorithms are not immune to making errors* - Algorithms generally find it hard to interpret the contextual meanings of words.⁴⁹ The meaning of content is relative to the specific context it is placed in. A particular word may have several meanings, depending on the setting or even the language it has been spoken or written in. Therefore, algorithms may erroneously dub a statement as nefarious, because they might not be able to interpret its context correctly. For instance, an algorithm used by Twitter to weed out ‘hate speech’ has been known to wrongfully remove harmless statements because it could not identify the context in which these statements were made.⁵⁰
- ii. *Lack of Transparency and Accountability* - Due to the opacity of these systems, it is difficult to ascertain the extent of the damage or harm they cause.⁵¹ Further, algorithmic opacity also

⁴⁷ The letter is available at <https://www.eff.org/files/2018/06/13/article13letter.pdf>.

⁴⁸ Karen Yeung, “Algorithmic Regulation: A Critical Interrogation,” *Regulation & Governance* 12 (2018): 505–23, <https://doi.org/10.1111/rego.12158>.

⁴⁹ Nicholas Thompson, “Instagram Unleashes an AI System to Blast Away Nasty Comments,” *Wired*, June 29, 2017, <https://www.wired.com/story/instagram-launches-ai-system-to-blast-nasty-comments/>.

⁵⁰ Ibid

⁵¹ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015) as cited by Karen Yeung in “Algorithmic Regulation: A Critical Interrogation,” *Regulation & Governance* 12 (2018): 505–23, <https://doi.org/10.1111/rego.12158>.

makes it difficult to trace the point of system error such as which faulty dataset led the algorithm to make its final determination.⁵²

- iii. *There are inherent biases in the datasets used to train algorithms* - For instance, researchers have found a high rate of racial and gender bias in publicly available text embedding - a common source of data used to train machine-learning algorithms.⁵³
- iv. *No due process for individuals to challenge algorithmic decisions* - Algorithms geared towards taking down offensive or unlawful content generally do so automatically, by granting the user little or no opportunity to contest the take-down. Even when there is an opportunity to do so, the system may be loaded in favour of one party against the other. For instance, Google launched a Content ID program to allow rights-holders to make claims of copyright infringement on YouTube videos. Under the Content ID program copyright owners upload their videos to Google's repository. Algorithms proceed to scan the content and create a unique fingerprint of its elements. Thereafter, the algorithms search YouTube for any content that may match that fingerprint. Copyright owners may also make manual searches. Once a claim is filed, copyright owners may either have the allegedly offending video taken down, or monetise it through YouTube. As is evident, unfortunately, the system places the entire burden of proof solely on the alleged infringer, even in cases when it is blatant that no infringement has been made.⁵⁴ Further, disputes are a lengthy process and if the claimant insists that the work is infringed, the system weights their claim over the alleged infringer.⁵⁵

Therefore, having a “person in the middle” is often presented as a solution for the issues with the automated decision-making proffered by algorithms. The premise here is that the algorithm will present its findings to a human being who will then make the final determination. Scholars note two reasons that such a strategy is ineffective for tackling the problems of algorithmic decision-making and oversight⁵⁶ --

- Making an individual a part of the procedure of determination fails to meet the “requirements of due process”, namely “a fair hearing” and an impartial trial.
- People are susceptible to “automation bias” and have a tendency to yield to the data generated by computational calculations and analysis.

⁵² Karen Yeung, “Algorithmic Regulation: A Critical Interrogation,” *Regulation & Governance* 12 (2018): 505–23, <https://doi.org/10.1111/rego.12158>.

⁵³ Nathaniel Swinger et al., “What Are the Biases in My Word Embedding?” (Arxiv, December 27, 2019), <https://arxiv.org/pdf/1812.08769.pdf>.

⁵⁴ Paul Tassi, “The Injustice Of The YouTube Content ID Crackdown Reveals Google’s Dark Side,” *Forbes*, December 19, 2013, <https://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/>.

⁵⁵ Ibid

⁵⁶ Karen Yeung, *Regulation & Governance* 12 (2018): 505–23, “Algorithmic Regulation: A Critical Interrogation”, available at <https://doi.org/10.1111/rego.12158>.

In this context, it is our recommendation that if any legislation places the onus on intermediaries to regulate activity on their platforms, such legislation must ensure that the methods used by the intermediaries at the very least, adhere to the Santa Clara Principles, which set out a minimum threshold for accountability and transparency in online content removal.⁵⁷

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

⁵⁷ The Santa Clara Principles are summarized as follows:

- i. Companies must publicly share the number of posts and accounts that were “removed or temporarily suspended” for violating their community standards or “content guidelines.
- ii. Appropriate notice must be provided to users whose accounts are temporarily or permanently suspended or posts are taken down.
- iii. Users must get a realistic chance to appeal the take down of their account or post. Further, if a human is put in charge of making the final determination on an appeal, such an individual should be an independent authority that is not part of the company whose platform the content was removed from. For more detail please see, “The Santa Clara Principles on Transparency and Accountability in Content Moderation” (New America, 2018), available at https://newamericadotorg.s3.amazonaws.com/documents/Santa_Clara_Principles.pdf.

Asia Cloud Computing Association's (ACCA) Response to the Ministry of Electronics and Information Technology (MeitY) Draft of the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018

MIT/79/041

Comment #1: Rule 3 (2)

(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;

- 1.1 The ACCA notes that “public health or safety” is not defined under the IT Act or any statute per se. Furthermore, the phrase “threatens public health or safety” is subjective and can be broadly interpreted.
- 1.2 The ACCA recommends that this sub rule be focused on “advertising” and not “promotion”, while being aligned with existing laws which govern tobacco, alcohol and nicotine products in other areas. A distinction between advertisements and other kinds of content must be drawn because intermediaries simply provide a neutral platform for parties to interact, deeming it inappropriate to cast compliance obligations that should specifically apply to advertisers. For instance, Section 5 of The Cigarettes and other Tobacco Products (Prohibition of Advertisement and Regulation of Trade and Commerce, Production, Supply and Distribution) Act, 2003 only prohibits “advertisements” of tobacco related products and not “promotion” of any and all content. Similarly, the Cable Television Networks (Regulation) Act 1995 only restricts alcohol, cigarette and tobacco advertising and not all forms of content which relates to them. This sub-rule thus exceeds the scope of the Cigarettes and Other Tobacco Products Act.
- 1.3 The ACCA recognised that this sub-rule relies on the Drugs and Cosmetics Act which does not apply to the subject matters sought to be covered here, except the use of “nicotine”. Additionally, the Drugs and Cosmetics Act only prohibits advertisements and cannot be the overarching legislation which determines the scope of these subject matters.
- 1.4 Alternatively, the ACCA recommends that this sub rule cover any content that is already governed by legislations covering cinematography or broadcasters, that may be re-posted / re-uploaded online in the exact same form.

Comment #2: Rule 3 (2)

(k) threatens critical information infrastructure.

2. The ACCA recommends that this sub-rule be removed as the IT Act already recognises a “protected system” that the government mandates various organisations including intermediaries to comply with, and the intended purpose of the proposed sub-clause is achieved through a combined reading of sub-rules (h) and (i). There already exist laws which govern critical information infrastructure, and cover what is intended to be covered under the proposed sub-rule (k):
 - a. Section 70 of the IT Act addresses the issue of threatening critical information infrastructure, which is accompanied by enabling rules for their implementation [Sec 70A(3), the Information Technology (National Critical Information Infrastructure Protection Center and Manner of Performing Functions and Duties) Rules, 2013].

- b. The scope of CERT's powers as laid down in Section 70B of the IT Act and in the Information Technology (The India Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.
- c. Further, Sec 70B(7) of the Act provides for penal provisions that provide for substantive steps to be taken and lay down the penalties to which intermediaries will be subject for non-compliance with such provisions. Thus, the proposed sub-rule could create double jeopardy for intermediaries as it implies that they would be liable for penal provisions under sec 70B(7) and additionally, will risk the loss of their safe harbour protection if the sub-rule is not met.

Comment #3: Rule 3 (4)

*The intermediary shall inform its users **at least once every month**, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.*

- 3.1 The ACCA recommends that MeitY allow intermediaries the flexibility to determine the most appropriate way in which a user can be informed of their obligations to comply with the Terms of Service (TOS) as the proposed sub-rule is over-prescriptive. It would lead users to receive a hoard of messages from all their service providers, which could create a situation of "notification fatigue", which may have the unintended consequence of users no longer paying any attention to such notices, defeating the intended purpose of the sub-rule. Additionally, intermediaries have existing provisions in place to periodically require users to confirm at the time of upload that their content abides with the TOS which includes local laws.
- 3.2 The ACCA further suggests that the government collaborate with industry stakeholders to run awareness and digital literacy campaigns for users to not upload unlawful content.

Comment #4: Rule 3 (5)

*When required by lawful order, the intermediary shall, **within 72 hours of communication**, provide such information or assistance **as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto**. Any such request can be made in writing **or through electronic means** stating clearly the purpose of seeking such information or any such assistance. **The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.***

- 4.1 The ACCA recommends that the proposed sub-rule be modified from "within 72 hours of communication" to "expeditiously", with the inclusion of a 72 hour action provision for urgent cases where there is an imminent threat to life, national security concerns and other grounds in the nature of those under Section 69A of the IT Act. This could also involve a graded classification of subject matters. The proposed 72 hour response period for all types of information requests is infeasible given the enormous quantity of incoming requests, broad range of services offered by intermediaries, content existing in different Indian languages/dialects and its contextual background. This aggressive response timeline will create a situation wherein urgent requests are pushed down the queue and do not receive the priority they deserve. It would also be technically infeasible, especially for start-ups and MSMEs, and

procedurally impossible to comply with for requests for data governed by foreign data protection and data sharing laws.

- 4.2 Alternatively, the ACCA recommends that MeitY add a parallel provision to sub-rule 5 which reads "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".
- 4.3 While the first part of the proposed sub-rule requires intermediaries to respond to requests made by "any government agency", the second part restricts agencies to those which are legally authorised to do so. This is inconsistent and thus the ACCA recommends that the scope of agencies which can seek information be narrowed down to only the agencies lawfully authorised to do so. The government should appoint state nodal agencies or designate cyber cells to streamline the process.
- 4.4 The ACCA requests clarity on the definition of terms such as "protective or cyber security" and "competent authority".
- 4.5 The ACCA recommends that there is uniformity and consistency of approach insofar as online and offline offences are concerned, to the extent application of basic principles of criminal law, both substantive and procedural, are concerned.
- 4.6 The ACCA recommends that sub-rule 5 on traceability be removed as it lacks clarity, is technically infeasible, has the potential for breach of privacy via surveillance, introduces subjectivity in enforcement and may conflict with foreign laws in cases where the originator is based outside India.
- 4.7 Alternatively, the ACCA requests that MeitY clarify whether the phrase "enable tracing" implies enabling traceability by the government or by the intermediary in response to a government request. MeitY should also 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.
- 4.8 The ACCA recommends that the provision is revised to read as: "The intermediary shall provide basic subscriber information pertaining to users of its services as are responsible for the unlawful act on receipt of a lawful order received from an authorised government agency."

Comment #5: Rule 3 (7)

The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;*
- (ii) have a permanent registered office in India with physical address; and*
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.*

- 5.1 The ACCA recommends that a locally based representative of an intermediary (nodal point of contact) is sufficient to ensure that the process of review is timely and effective, and compliance to their orders/requisitions are made in accordance with provisions of law or rules.

- 5.2 The ACCA further recommends that MeitY remove the requirement for local incorporation, registration and a physical presence as would place onerous burdens on a vast majority of intermediaries. Requiring intermediaries to be registered or established in India would mean that certain established intermediaries that are conducting their business in compliance with applicable local laws may now fall short of restrictions under the FDI policy and may be required to wind up their service offerings, significantly disrupting business activities of sectors in India dependent upon intermediary services and affecting the ease of doing business in India.
- a. While 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). The proposed provision of local incorporation and physical presence thus extends beyond the current scope of the IT Act. Further, there are no parameters set out for the government to list an intermediary to follow the above requirements, leaving open the possibility of arbitrary classification.
 - b. The economies of scale achieved through globally located infrastructure have contributed to the affordability of services on the internet, because companies do not have to incur additional costs of setting up and running local offices in each country where they offer services. This proposed sub-rule will harm consumer experience on the open internet, increase costs to an extent that offering services to consumers in India becomes financially unviable.
- 5.3 The ACCA seeks clarity on the criteria for notifying intermediaries, the methodology to determine metrics such as number of users and enforcement mechanisms (e.g., for international websites) to ensure effective enforcement and clarity in day to day operations for all relevant actors.
- 5.4 The eligibility criteria of fifty lakh users is quite low and can especially burden start-ups/smaller intermediaries who would not have the ability or infrastructure to comply with the requirements under this amendment, further hurting innovation in India. The ACCA thus recommends that the threshold be backed by statistical analysis of usage patterns.

Comment #6: Rule 3 (8)

*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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ **one hundred and eighty days** for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.*

- 6.1 The ACCA recommends that 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 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 of 24 hours for intermediaries to act.

- a. Given that only courts can conclusively determine the illegality of content, platforms will end up removing content without reviewing it sufficiently to take a “better safe than sorry” approach. This may pose a threat to constitutionally-protected right to freedom of speech and expression.
 - b. Additionally, the 24 hour period is inconsistent with the one month time period that is prescribed for the Grievance officer to act within (Rule 3 [12]). Further, the current wording of Rule 3 (8) refers to compliance with Rule 3 (6), which pertains to security practices regarding data, and is not relevant to takedowns. It also omits to mention take-down of content which may fall under Rule 3 (2), which was present in the 2011 Rules.
- 6.2 The ACCA also suggests that in all instances, the provision should list 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.
- 6.3 The ACCA recommends that MeitY retain the 90 day period 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. The increased retention period for a minimum of 180 days is not consistent with the principle of data minimisation that runs as a common thread across the proposed Personal Data Protection Bill. Also data retention rules must comply with the principles of legality, necessity and proportionality.
- 6.4 Further, the ACCA requests MeitY to clarify how the retention period would operate for users outside of India who also exercise their right to delete personal data pursuant to other foreign laws.
- 6.5 The ACCA recommends that the power to seek preservation of data for investigation purposes should be limited to “authorised law enforcement agencies”, instead of “appropriate government” or “its agency”.

Comment #6: Rule 3 (9)

The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

- 7.1 The ACCA recommends that this proposed sub-rule be removed, or disengaged with due diligence guidelines that would form the basis for an intermediary to avail of its statutorily granted defence of safe harbour. The ACCA’s recommendation is based on the following reasons:
- a. Developing and implementing automated technology tools to pre-screen content is an extremely high burden for start-ups and smaller intermediaries, and may even hinder innovation and investment in the sector, especially if its linked to their ability to avail of the statutory immunity to which they are entitled.
 - b. “Unlawful content” is a subjective expression, making it impossible to determine in a full proof manner which information or content is objectionable or offensive. Further, the rule envisages AI technologies to have “appropriate controls” which only renders the scope of the rule even more open-ended and practically impossible to comply with.

- c. The requirement for intermediaries to implement proactive measures to identify and remove unlawful content, and if failure to do so could endanger its service and legal defences, it would pressurise them to adopt a “better safe than sorry” approach which in this case would mean excessive takedown of content. This would incentivise the removal of even legitimate content.
- d. While automated detection tools can help identify content that violates policies as applicable to a particular intermediary / product, its efficacy varies greatly based on the type of content, and human review/context remains important. For instance, content that might be considered in one context to instigate violence may be appropriate when featured as part of news reporting. Similarly, with defamation, no one single party is the arbiter of truth.
- e. It is important to distinguish between online content sharing platforms that host the content from other services that do not have direct access to content because here the business entity providing the end service to its users is in a more appropriate position to handle removal and user information requests along with conducting proactive monitoring.
- f. The proposed sub-rule shifts the onus and duty of the State to identify or determine whether content is unlawful or illegal to the intermediary (private party).
- g. This proposed sub-rule violates IT Act Provisions and Supreme Court Judgements:
 - i. In light of *Shreya Singal vs. Union of India*, any obligation for proactive monitoring of platform content could exclude such intermediary from claiming the safe harbour exemptions.
 - ii. Sub-rule 9 goes against the statutory intent 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
 - iii. Sub-rule 9 also goes against the established legal position in India against pre-censorship of content and would fail to meet the test of reasonable restrictions that can be imposed on the constitutional right of freedom of speech.
 - iv. Courts have ruled that blanket bans of certain categories of content from being carried by platforms that enable expression would not be legal given the constitution's protection of freedom of expression, indicating that case-by-case determination of whether applicable laws were violated would be required.
- h. This proposed amendment goes against established international laws and India's commitments under various international covenants including 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)¹, and the Joint Declaration on Freedom of Expression and the Internet (2011) issued inter alia by the UN Special Rapporteur on Freedom of Opinion and Expression.²
- i. Furthermore, the legal and regulatory framework in other jurisdictions do not support proactive monitoring of content whether by automated or by human means as a pre-condition for intermediaries to avail of safe harbour protection.

¹ Paragraph 39 and 43 (pg 18 and 19) - <http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf> | Article 19 of ICCPR (pg 27 at 32) (Text of <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>)

² Clause 2: Intermediary Liability and Clause 3: Filtering and Blocking (pg 24).
<http://www.cidh.oas.org/relatoria/showarticle.asp?artID=849&IID=1>

- j. In the absence of any industry standard on what amounts to “technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content”, it would lead to subjective interpretations by courts on whether an intermediary has satisfactorily fulfilled its role of "proactive monitoring".

7.2 The ACCA recommends that online platform should not be penalized for taking voluntary steps to address harmful content. Legal provisions that make this clear (called “Good Samaritan” protections) facilitate platforms’ ability to innovate and evolve new ways to address illegal content over time.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)



BROADBAND INDIA FORUM

SUBMISSION TO THE DRAFT INFORMATION TECHNOLOGY [INTERMEDIARIES GUIDELINES (AMENDMENT)] RULES, 2018

Broadband India Forum (*BIF*) is a leading think-tank in India which seeks to achieve the ambitious vision of creating Digital India. BIF works with multiple stakeholders including technology providers, telecom service providers, internet service providers, satellite operators, value-added service provider, broadcasters, and start-ups to promote the development of different technologies, regulations, and policies that promote access to affordable and high speed broadband throughout India.

With the same objective, BIF would like to take this opportunity to provide its comments and suggestions to the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules, 2018 (*Draft Amendment*)] released by the Ministry of Electronics and Information Technology (*MeitY*) that seeks to amend the extant Information Technology (Intermediaries Guidelines) Rules, 2011 (*Intermediary Guidelines*).

High speed internet has played an important role in enabling economic integration and boosting user experience in India. This technological development has paved the path for online intermediaries to provide platforms for communities from different cultural, ethnic, and political backgrounds to express and create. This in turn, has enhanced the efficiency of the digital democracy.

With the presence of smartphones and inexpensive Internet at each user's disposal, the online space has become an important medium of speech and expression. Intermediaries have played a key role in facilitating communication, trade, entertainment, and other services that have become an integral part of users' lives. Therefore, regulating such intermediaries requires stakeholder consultation to ensure that any laws regulating intermediaries and how they interact with users are in sync with the needs of the market, protection of users, and existing legal framework.

However, BIF observes that the Draft Amendment poses severe challenges to privacy, innovation, and competition by not only restricting the nature of content being uploaded online but also deterring companies that are transforming how users use the Internet in their everyday lives. In this context, we submit the following comments to the proposed provisions of the Draft Amendment.

A. *Intermediary Liability in India*

An intermediary is anyone who, on behalf of another person, receives, stores or transmits an electronic message or provides any service with respect to that message. Intermediaries in India include social media platforms, e-commerce websites, search engines, etc. Under the Information Technology Act, 2000 (*IT Act*), intermediaries enjoy 'safe harbour protection' under certain circumstances. These conditions include: acting merely as a facilitator; not initiating the

transmission; not selecting the receiver of information or selecting or modifying the information contained in the transmission; and several due diligence criteria specified in the Intermediary Guidelines.

The Intermediary Guidelines deal with specific due diligence criteria that have to be fulfilled in order for an intermediary to avail the safe harbour exemption. Since such safe harbour protection is an exemption provision derived from Section 79 of the IT Act, any rules formulated on the same must lie within the limits set by the parent legislation.

The Supreme Court of India (SC) in its judgment in *Shreya Singhal v. Union of India* has amended the application of Section 79 of the IT Act and the Intermediary Guidelines to be in consonance with the requirements of due process, and has also read down any obligation on intermediaries of judging the lawfulness of content uploaded on their platforms. Accordingly, intermediaries are required to remove or disable access to content upon receiving actual knowledge of a court order or on being notified by the appropriate government/agency. Any request for taking down of content must pertain to the grounds under Article 19(2) of the Constitution, which provides the grounds for reasonable restrictions on freedom of speech and expression.

BIF believes that the Draft Amendment fails to comply with the existing framework applicable to intermediary liability as it oversteps the rule-making powers under the IT Act and requires intermediaries to adhere to overbroad requirements to claim safe harbor, including proactive monitoring of content.

Right to Privacy

In its landmark decision, the SC upheld the right to privacy as a fundamental right under Part III of the Constitution of India in the case of *K. Puttaswamy v. Union of India*. The SC observed that any legislation that limits the right to privacy must fulfil the three-pronged tests of:

- i. ***legality***, which postulates the existence of law;
- ii. ***necessity***, defined in terms of a legitimate state aim; and
- iii. ***proportionality***, which ensures a rational nexus between the objects and the means adopted to achieve them.

BIF believes that the Draft Amendment is likely to impose unreasonable restrictions on the fundamental right to privacy, as certain proposed amendments do not meet the test mentioned above.

Specific Comments

Accordingly, please find below our comments to the specific provisions of the Draft Amendment:

1. **Rule 3(2) – Disclaimers** – Under the Intermediary Guidelines, intermediaries are required to observe due diligence while discharging their duties. This includes informing users not to host content of certain nature such as content that may harm minors, infringe any intellectual property, etc. The Draft Amendment introduces two additional categories of content, which intermediaries are required to relay to its users through its privacy policies and other user agreements. These include information that –

- i. threatens public health or safety; promotion of cigarettes and other tobacco products, or consumption of intoxicants including alcohol and Electronic Nicotine Delivery System; and
- ii. threatens critical information infrastructure.

However, the Draft Amendment does not provide guidance on what content can be said to be threatening to public safety, health or critical information infrastructure in India. The use of such vague language may result in arbitrary and inconsistent interpretations of this provision. As discussed above, free speech in India can only be restricted by the State based on the grounds identified in the Constitution of India. These include: (i) sovereignty and integrity of India; (ii) the security of the State; (iii) friendly relations with foreign State etc. As such, the grounds identified under Rule 3(2) do not fall under the abovementioned reasonable restrictions and seem to be vague as there is no explanation for what may constitute a threat to public health or critical information infrastructure. As a result, these grounds may be open to challenge for being unreasonable restrictions on the freedom of speech or expression enjoyed under Article 19(1) of the Constitution of India. Please note that in the *Shreya Singhal* case, Section 66A of the IT Act was struck down and declared unconstitutionally vague as it consisted of ambiguous language such as “grossly offensive”, “menacing”, “false”, and “causing annoyance, inconvenience, danger”. The SC clarified that any restriction requests must fall within the contours outlined in Article 19(2) of the Constitution of India and include principles of natural justice and elements of due process of law.

2. **Rule 3(4) – Monthly Information** – The Intermediary Guidelines requires intermediaries to inform their users that “non-compliance with rules and regulations, user agreement and privacy policy” may lead to the termination of access or usage rights and removal of non-compliant information. However, as per the Draft Amendment, such information is required to be provided to users on a *monthly* basis.

Since intermediaries typically include such information in their terms of use/service, privacy policies and user agreements, mandating additional ongoing compliance would be burdensome for intermediaries and result in greater business costs for them. On the other hand, users may suffer from notification fatigue with multiple changes in such privacy policies and user agreements.

3. **Rule 3(5) – Tracing the originator of information** – Firstly, the Draft Amendment directs intermediaries to trace the originator of information uploaded on the intermediary platform if and when required by government agencies. Secondly, the Draft Amendment also requires intermediaries to provide, within 72 hours of a lawful order, *information and assistance* “as asked by any government agency or assistance concerning security of State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto”. Since the term “assistance” has not been defined, intermediaries may have to provide information and assistance for non-specified purposes, which goes against due process of law. This requirement is also in contravention of the right to privacy as upheld by the SC as it does not fulfil the three-pronged test of legality, necessity, and proportionality.

Lastly, the requirement of providing the requested information or assistance within 72 hours is unreasonable as such time frame may not be sufficient to address such requests in all instances

or analyse and respond to such requests.

4. **Rule 3(7) – Incorporation of Indian entity and designation of nodal officer** – The Draft Amendment mandates that if any intermediary has a user base of 50 lakh or above, or is specifically notified by the government, it would be required to comply with the following conditions:
- i. incorporate an entity in India under the Companies Act, 1956 or 2013;
 - ii. maintain a permanent registered office in India; and
 - iii. appoint points of contact in India for liaising with the law enforcement on a 24x7 basis.

This requirement is burdensome and onerous for several companies, which currently provide services to Indian users but do not have any domestic presence in India. Furthermore, this may have a negative impact on potential companies looking to target the Indian market, which in turn, will have an adverse effect on competition in the digital economy. Stringent norms such as these may deter companies from entering the Indian market as it may affect their functioning and trade prospects. In times where India intends to achieve maximum access to services provided by intermediaries, such provisions will deter companies from providing adequate and quality services in India.

5. **Rule 3(8) – Blocking Orders** – The Draft Amendment imposes an obligation on intermediaries to remove any content within 24 hours of actual notice by a court order or authorised government agency. However, there are no procedural checks provided for in the Draft Amendment when the request is made by a government agency without prior judicial authorisation, which gives rise to potential for misuse.

Additionally, the time frame within which content has to be taken down, that is, 24 hours, is unreasonable and not backed up by any clear legal reasoning. The Draft Amendment also does not provide any sufficient grounds or procedural safeguards where it increases the period of retention of records from 90 days to 180 days *or such longer period as required by government agencies or courts*. Such provisions may be misused, give rise to surveillance related concerns, issued without adequate justification and furthermore the law does not prescribing any privacy safeguards around this requirement.

6. **Rule 3(9) – Monitoring** – The Draft Amendment mandates intermediaries to proactively monitor content being uploaded on its platforms, which is not only unfeasible, but also in contradiction to the role of an intermediary. The *Shreya Singhal* case has clarified that intermediaries should not be required to screen content uploaded by users to assess their legality. Any law that is likely to have the effect of making intermediaries ‘monitors’ and ‘judges’ of content would change the nature of an intermediary as a neutral medium of transmission of information. It would also be an unreasonable interference with the rights of such intermediary to carry on its business. Furthermore, this provision would also violate the fundamental right to freedom of speech and expression and right to privacy of individuals as it requires intermediaries to constantly monitor user content and creates an incentive for them to censor content in order to avail of legal exemption from liability.

B. Global Positions on Intermediary Liability

The Draft Amendment disregards the international norms that countries across the globe have developed with respect to intermediary liability.

1. **The United Nations Rapporteur's Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression** (A/HRC/38/35 2018) – This states that states should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy. It also provides that states should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.

Clearly, the Draft Amendment fails in this regard, as it provides for legally authorised government agencies to become the arbiters of lawful expression without due process – having the dual powers to issue content takedown orders and compel tracing of originators of content.

2. **Manila Principles** – The Manila Principles¹ are a global set of standards that constitute best practices for nations follow for while structuring regulations for intermediary liability. These include:

- i. Intermediaries should be shielded from liability for third-party content uploaded on their platform.
- ii. Content must not be restricted unless by an order by a competent judicial order/authority.
- iii. Requests for take down of content must be clear, unambiguous and follow due process.
- iv. Laws and content restriction orders must comply with the tests of legality, necessity, and proportionality.
- v. Transparency and accountability must be built into laws and content restriction policies.

The Draft Amendment fails to adhere to the standards applicable to intermediaries, their liability, and safeguards available to them under the Manila Principles.

C. Conclusion

With jurisdictions across the globe following international standards with respect to treatment of intermediaries, free speech online, and protection of users, the Draft Amendment fails to incorporate some core principles governing intermediaries worldwide. Not only does it exceed the scope of the IT Act, 2000, it is also violative of the right to freedom of speech and expression and privacy of users. In order to ensure that the population of India has access to a wide variety of services over the internet, Indian laws should act as an impetus for service providers to compete in the Indian market. However, by imposing onerous obligations on intermediaries, the Draft Amendment disincentivizes innovation and betterment of Internet services. To ensure

¹ See <https://www.manilaprinciples.org/>

that the law keeps pace with global developments, widespread consultations should be undertaken before any changes are made to existing law in this regard.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Introduction and Background

Section 79 of the Information Technology Act, 2000, (“**IT Act**”) provides for a conditional exemption from liability for certain classes of intermediaries (as defined under the IT Act) from third-party content which is made available by them. This immunity is available to certain intermediaries, provided that they comply with the rules and guidelines made by the Central Government under Section 79(2)(c). The Information Technology (Intermediary Guidelines) Rules, 2011, (“**Intermediary Guidelines**”) were made by the Central Government under Section 79(2)(c) and provide for various conditions which must be complied with by the intermediaries, subject to which they would be able to avail the exemption from liability for hosting third-party content. The proposed draft Information Technology Intermediary Guidelines (Amendment) Rules, 2018, (“**Draft Rules**”) attempt to amend the Intermediary Guidelines in an effort to “*strengthen the legal framework and make the social media platforms accountable under the law.*”

The conditional immunity Section 79 of the IT Act has been crucial for the development and innovation in internet technologies in India, particularly in the growth of online ‘platforms’, which host and enable the sharing of user-generated content. Providing conditional immunity for third party content which has not been selected or modified by them, (also known as ‘safe harbour’) to such platforms, has developed (in various forms) as an important principle of internet governance in legal regimes around the world, including, notably, in the European Union,¹ the United States of America,² Brazil,³ Chile,⁴ and several other jurisdictions.⁵ This has enabled and inculcated the spirit of permission-less innovation, freedom of information and freedom of expression that is the hallmark of the internet in the 21st century.

¹ ‘Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market’, (Directive on E-Commerce).

² 47 U.S.C. § 230, Communications Decency Act, 1996.

³ Law 12.965, Marco Civil da Internet, 2014.

⁴ Law No. 20.435, 2010.

⁵ See World Intermediary Liability Map, Stanford Centre for Internet and Society, *available at* <https://wilmap.law.stanford.edu/>.

At the same time, the rise of platform-mediated online communication has given rise to a host of concerning issues, particularly on the prevalence of unlawful content and information on such platforms. The issues of illegal online speech, which includes content ranging from child pornography to infringement of copyright, is of concern not just to law enforcement, but to the online community as a whole. The present legal and regulatory framework appears to be inadequate to appropriately address issues of unlawful content online.

While the effort to make social media and the internet a safer space for Indians is commendable and appreciated, the Draft Rules in their present form will fail to achieve their intended effect, and may also raise legal and constitutional challenges. My submissions is intended to assist the Ministry with its effort to improve the legal framework regarding unlawful content and information on social media platforms to make the internet a safer and more democratic space.

At the outset, while anecdotal evidence suggests the increasing prevalence of unlawful information online, the Government of India has not provided any empirical basis for recommending changes to the Intermediary Guidelines. Reference to such evidence is necessary to inform policy making in the sphere of intermediary regulation in India, so that any reform to the legal regime is responsive to facts and not merely rhetoric. There is an urgent need for empirical studies on content moderation practices of various intermediaries in India and its effects on unlawful information online, which can provide a basis for a revised legal framework.

It is recommended that the Ministry of Information Technology must refer the agenda of reforming the intermediary liability regime under Section 79 to a parliamentary select committee or an independent committee of experts who can recommend substantive, evidence-based reforms. Any such committee must be both consultative and representative of the diverse stakeholders in the Indian online community.

Part – I: Specific Comments and Recommendations on the Draft Rules

I. The draft Rule 3(5) states that:

“(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”

This draft amendment states that an intermediary must provide such information with a government agency, as required by a lawful order, for the purpose of “security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto.” Moreover, the draft rule prescribes a separate procedure for such requests for information, and also mandates that intermediaries trace the ‘originator of the information’ as required by government agencies, which are legally authorized.

While the draft rule makes a reference to ‘lawful orders’ and ‘legally authorized agencies’, it is unclear what specific legal procedure is being referred to and which must be followed by intermediaries. Similarly, it is unclear what the ‘assistance’ referred to in the draft rule pertains to.

Section 69 and 69B of the Information Technology Act, (“IT Act”) read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, (“Monitoring Rules”) prescribe a specific procedure for law enforcement access to information held by

intermediaries. This procedure is a self-contained code, which includes the grounds on which information may be accessed, the procedure for authorisation of information requests as well as the procedure for ensuring 'traceability' of the information. Inasmuch as the procedure prescribed under draft Rule 3(5) is in contradiction of the procedure laid down under the IT Act in Section 69 and the Monitoring Rules, it may be *ultra vires* the IT Act and therefore struck down by the courts.⁶

Notwithstanding the above, the provision for ensuring law enforcement access to information is unconnected with the rationale for the enactment of Section 79, which is to ensure legal immunity for third-party content made available by intermediaries. Requiring intermediaries to comply with such procedures to avail legal immunity for third party content goes beyond the scope of Section 79 and is also contradictory to the international best practices on intermediary regulation set forth in the Manila Principles on Intermediary Liability.⁷

It is recommended that draft Rule 3(5) should be omitted from the Draft Rules.

II. Draft Rule 3(7) states that:

“(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;

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

⁶ Indian Express Newspapers v/s. Union of India, AIR 1986 SC 515.

⁷ Manila Principles on Intermediary Liability Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation, (March 24, 2015), available at https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.

(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.”

Draft rule 3(7) imposes certain obligations on all intermediaries above a *de minimis* threshold of fifty lakh users. While it is appreciated that the regulation of intermediaries operating at scale may pose special concerns for the purpose of regulation,⁸ certain aspects of the draft rule require further scrutiny:

First, the basis of establishing whether an intermediary has '50 lakh users' is unclear and the criterion for assessment should be clarified. Further, the provision for notification of the 'list of intermediaries' which may also be subject to such regulation is unclear.

Second, it is unclear what purpose is sought to be achieved by requiring intermediaries to incorporate companies with a physical address in India. If the concern is over the exercise of legal jurisdiction over online platforms and intermediaries, this concern may be better solved by the inclusion of a long-arm provision within the IT Act to clarify the exercise of jurisdiction over specific intermediaries operating in India and purposefully directing their services at Indian users.⁹ While Sub-Section (2) of Section 1 of the IT Act already provides that it shall also extend “to any offence or contravention hereunder committed outside India by any person” it is unclear whether this is sufficient basis for establishing jurisdiction over intermediaries.

Third, while the requirement for intermediaries to establish a permanent liaison officer or company representative for its operations in India may be helpful in ensuring greater regulatory compliance and accountability to online communities, there should be additional clarification on the specific designation of such a liaison and what role they are expected to perform within a company. For example, it should be clarified if the liaison is expected to play a role similar

⁸ Tarleton Gillespie, 'Platforms Are Not Intermediaries', 2 Geo. L. Tech. Rev. 198 (2018).

⁹ A similar test has been developed by the Delhi High Court in case of *Banyan Tree Holding (P) Limited vs A. Murali Krishna Reddy*, 2010 (42) PTC 361 (Del).

to that of the designated officer under Rule 13 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information for Public) Rules, 2009. Further, the objective of the rule may be better served by clarifying that the liaison should be an Indian 'resident' as defined under the Income Tax Act.

It is recommended that draft rule 3(7) be amended to include the following:

- 1. It must only include a requirement that certain notified intermediaries shall nominate a permanent representative and law enforcement liaison officer, who shall be a resident of India.***
- 2. The criteria on the basis of which intermediaries which must may be notified should be clearly and specifically defined under the rules, and should provide a rational basis for classification, for example, the deliberate targeting of the business of such intermediary to users based in India.***
- 3. The applicability of the IT Act to cover activities of intermediaries located outside of India should be clarified by appropriate amendments to the IT Act itself.***
- 4. The rule should also provide the appropriate designations of who may be appointed as a permanent representative for an intermediary as well as the obligations and responsibilities of such a representative.***

III. Draft Rule 3(8) lays down the procedure for the removal of information to be followed by an intermediary in the aftermath of the judgement of the Supreme Court of India in *Shreya Singhal v Union of India*. While the incorporation of the Supreme Court's decision is appreciated, the draft rule includes vague language such as the requirement to remove notified content 'as far as possible immediately'. Moreover, as the provision relates more specifically to the standard of 'actual knowledge' to be applied in the interpretation of Section 79(3)(b), ***it is recommended that this change be incorporated as an explanation, by amending Section 79 of the IT Act, which should state as follows:***

“Explanation: For the purpose of this Section, ‘actual knowledge’ shall mean the receipt, by an intermediary, of an order by a court of competent jurisdiction, notifying the intermediary of the specific unlawful content.”

IV. Draft Rule 3(9) states that:

“The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

Draft Rule 3(9) uses ambiguous and vague language to require intermediaries to identify and remove access to ‘unlawful information or content’ using ‘automated tools or appropriate mechanisms’. This rule requires reconsideration for the following reasons:

- 1. The requirement to proactively identify and remove access to all ‘unlawful content’ is vague and overbroad, and may violate Articles 14 and 19(1)(a) of the Constitution of India**

In *Shreya Singhal v Union of India*,¹⁰ the Supreme Court of India, in reading down Section 79 of the IT Act, observed that an intermediary should not be placed in a position to decide the legitimacy or legality of information, particularly given the scale at which certain intermediaries operate.

The draft rule imposes a vague and unreasonable obligation upon intermediaries to proactively monitor and disable information which may be ‘unlawful’, without providing sufficient clarity on what constitutes ‘unlawful’ content or on what standard an intermediary is to be held liable to in cases of failure to proactively filter unlawful speech. The use of the term ‘unlawful’ does not provide sufficient standards for intermediaries to determine which content should or should not be permitted, and thereby to determine what actions would amount to an

¹⁰ (2013) 12 SCC 73.

infringement of such a rule. As such, leaving the interpretation of the term 'unlawful' open to the determination of intermediaries can lead to an arbitrary, inconsistent and discriminatory application of the power to remove content. The Supreme Court in *Shreya Singhal v Union of India*, struck down a provision of law as void for vagueness, on the grounds that '*there is no manageable standard by which a person can be said to have committed an offence or not to have committed an offence.*' The draft rule suffers from similar infirmity, and may be struck down as void on grounds of vagueness.

Similarly, the over-breadth of the term 'unlawful content' is likely to lead to self-censorship of legitimate and legal content by intermediaries to avoid liability – creating a 'chilling effect' on constitutionally protected speech. There is substantial empirical evidence, including from India¹¹ that over-broad requirements to monitor and filter speech results in over-removal of constitutionally protected speech.¹² Vague and over-broad laws which create a 'chilling effect' on constitutionally protected speech and expression have been held to be unconstitutional by the Supreme Court of India, and may similarly pose a challenge to the impugned draft Rule 3(9).¹³

2. The use of 'automated' tools for filtering and removal is not appropriate for all forms of unlawful information.

Despite the advancement of machine learning and automated tools for content removal, they are unfortunately not a panacea for harmful or illegal online content.¹⁴ While the use of automated information filtering and blocking mechanisms has been in use by online intermediaries, their efficacy is highly

¹¹ Rishabh Dara, 'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet', Centre for Internet and Society, (2011), available at <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf>.

¹² D. Keller, 'Empirical Evidence of "Over-Removal" by Internet Companies under Intermediary Liability Laws', Stanford Centre for Internet and Society, (October 12, 2015), available at <http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws>.

¹³ (2013) 12 SCC 73.

¹⁴ United Nations Human Rights Council, 'Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression', A/HRC/38/35, (April 6, 2018); Daphne Keller, 'Internet Platforms Observations On Speech, Danger And Money', Hoover Institution, (June 13, 2018).

dependent on the context of the information at issue as well as the precise nature of the technology used. For example, many platforms already utilise filtering technologies like PhotoDNA to disable access to child pornography, which are based on the hashes or digital fingerprints of images which have already been human-reviewed and identified as clearly illegal.¹⁵ This use of automated filtering may be appropriate as the unlawfulness of child pornography is rarely context-dependent. However, in other instances, such as defamation or copyright, the determination of legality of information is heavily context-dependent, and even the most sophisticated of automated technologies, such as YouTube's ContentID, are prone to both censorship and over-removal of constitutional and legitimate speech, as well as under-removal of unlawful content.¹⁶ There are several examples of over-censorship caused by the use of automated filtering mechanisms.¹⁷

Finally, several automated tools pose a distinct problem in that their functioning is particularly non-transparent, even to the human operators which may employ such tools. Such non-transparency of the mechanisms of such tools results in opaque, discriminatory and arbitrary decision making without the ability to audit the functioning of such tools.¹⁸

Therefore, the use of automated tools without human review may not be appropriate for all forms of unlawful speech which this rule seeks to prohibit, and should not be made a precondition for ensuring conditional immunity from liability for intermediaries.

3. The requirement to monitor and proactively identify and disable all 'unlawful' information and content and will disproportionately affect smaller intermediaries and discourage innovation.

¹⁵ Briefing on Online Child Sexual Abuse Imagery, Internet Watch Foundation, *available at* https://www.iwf.org.uk/sites/default/files/inline-files/Technology%20Briefing%201%20-%20Online%20CSAI%20v5.4%20%28002%29_0.pdf.

¹⁶ Electronic Frontier Foundation, 'Content ID and the Rise of the Machines', (February 26, 2016), *available at* <https://www.eff.org/deeplinks/2016/02/content-id-and-rise-machines>.

¹⁷ Sydney Li and Jamie Williams, 'Despite What Zuckerberg's Testimony May Imply, AI Cannot Save Us', Electronic Frontier Foundation, (April 11, 2018), *available at* <https://www.eff.org/deeplinks/2018/04/despite-what-zuckerbergs-testimony-may-imply-ai-cannot-save-us>.

¹⁸ Zachary C. Lipton, 'The Mythos of Model Interpretability', *available at* <https://arxiv.org/pdf/1606.03490.pdf>.

The use of automated mechanisms for the monitoring and filtering of context-dependent information can prove to be massively expensive to implement. For example, YouTube has spent over 100 Million USD in implementing such a system for monitoring copyright infringement,¹⁹ which nonetheless remains imperfect. The possibility of legal liability, including criminal liability for the failure to implement such systems may discourage new and innovative online services while entrenching the dominance of large online intermediaries who are in a position to implement them.

It must be noted that several content hosting intermediaries, including most popular social media networks, already disable content which they deem to be inappropriate for their networks, as per their own internal policies and practices.

It is recommended that draft Rule 3(9) should be omitted from the Draft Rules.

Part – II: Legal Reforms for A Safer Internet

While the draft rules in their present form are inappropriate, for the reasons mentioned above, to deal with the problem of unlawful content online, there is substantial scope for improvement of current practices and mechanisms to counter unlawful content online and bring about a safer and democratic internet for India.

This section recommends principles upon which to base the regulation of intermediaries in order to promote safer online spaces in India.

1. Defining the Scope of Regulation for Online Content

The present approach towards intermediary regulation adopts a one-size-fits-all approach. As such, the regulations, including the Intermediary Guidelines and

¹⁹ Paul Sawers, 'YouTube: We've invested \$100 million in Content ID and paid over \$3 billion to rightsholders', VentureBeat, (November 7, 2018), available at <https://venturebeat.com/2018/11/07/youtube-weve-invested-100-million-in-content-id-and-paid-over-3-billion-to-rightsholders/>.

the Draft Rules, do not take into account the immense differences between various intermediaries (as defined under the IT Act), such as ISPs, online marketplaces, or social network providers.

For the purpose of public oversight of online content, regulation should focus on the sub-set of intermediaries which operate at scale, provide a network for third-parties to share content and exercise proximate control over such content. These intermediaries are an appropriate point of regulatory control over unlawful content for two reasons:

1. The reach and spread of unlawful content is magnified considering the scale at which such intermediaries operate. Further, the network effects established by such intermediaries often leaves users and online communities with few alternative channels for online communication.
2. As opposed to other intermediaries like ISPs or 'mere conduits', such intermediaries already govern or moderate the content which is hosted by them in a number of ways, even though they may not be 'selecting or modifying' such content directly. These practices include amplifying, recommending, promoting, filtering, curating, suspending or blocking of content, and is intrinsic to the service that such intermediaries perform.²⁰

2. **Ensuring Transparency and Accountability in Content Moderation**

The IT Act and associated rules do not adequately address the issues of transparency and accountability of the private practices by which hosting intermediaries govern online content. These practices are often arbitrary, exclusionary and discriminatory undermine the constitutional rights to free expression and freedom of information.²¹ At present, the legal regime grants online intermediaries the right to govern online content according to their own internal private practices, but does not ensure responsibility for ensuring that such governance is accountable or transparent to the online communities. For example, Rule 3(5) of the Intermediary Guidelines, allows intermediaries to

²⁰ Gillespie, *supra* note 9.

²¹ Frank Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power', 17 *Theoretical Inquiries in Law* 487, (2016).

‘immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information’, without any responsibility towards such users to ensure that such decisions are not arbitrary or discriminatory.

Apart from preserving freedom of expression online, making the content moderation practices of online platforms more clear, transparent and accountable to online users also results in safer online spaces. Transparency and accountability can empower online communities to enforce community standards for content in a decentralised manner. Several platforms already employ some form of ‘trusted flaggers’ to inform the platform of potentially unlawful content for the purpose of removal,²² recognising that empowering online users and communities to maintain community standards of speech can provide decentralised control over harmful or unlawful content.²³

Given the scale at which most content hosting platforms operate, some degree of miscalculation in the application of content moderation policies will be inevitable. Regulatory efforts should instead be focussed on ensuring independent public oversight of content moderation practices and procedures, rather than on liability for specific instances of incorrect moderation.

Firstly, regulatory efforts can focus on ensuring that the substantive individual content moderation *policies* are tailored to Indian law take into account legal standards applicable in India. Such a determination should involve some form of judicial oversight of the publicly available content moderation policies (such as community guidelines and user terms of services on platforms).²⁴

Secondly, such policies should ensure some form of procedural transparency and accountability in their enforcement. Platforms must ensure that content moderation practices are made transparent and available in all languages for which there exists a significant user base. Further, procedures for content

²² YouTube, ‘Growing our Trusted Flagger program into YouTube Heroes’, (September 22, 2016), available at <https://youtube.googleblog.com/2016/09/growing-our-trusted-flagger-program.html>.

²³ Ivar Hartmann, ‘Let the Users be the Filter? Crowdsourced Filtering to Avoid Online Intermediary Liability’, 2 Journal of the Oxford Centre for Socio-Legal Studies, (2018).

²⁴ Kyle Langvardt, ‘Regulating Online Content Moderation’, 106 The Georgetown Law Journal 1353, (2018).

restriction must include at a minimum the requirement of a notice to the affected parties whose content has been restricted, allow for an appellate mechanism and ensure some level of explainability for the users whose content has been restricted. In particular, specific efforts should be made for simplifying the mechanisms whereby law enforcement agencies can issue content restriction requests. The Santa Clara Principles on Transparency and Accountability in Content Moderation Practices provide a good starting point for the development of standards for content moderation procedures.²⁵

Regulation should also allow for leeway in determining what *form* of moderation is most appropriate for different kinds of content. For example, oversight of content moderation policies could require automatic removal of child sexual imagery and extremist content flagged by law enforcement agencies, subject to the issuance of a subsequent judicial order within an appropriate time frame. On the other hand, the moderation of content deemed defamatory, or content which infringes copyright, (which offences are largely civil, rather than criminal, in nature) may be better dealt with through a notice-and-notice mechanism wherein the platform's obligations would be limited to identifying the uploader of flagged content and forwarding a legal notice prepared by the affected party. Such a mechanism has been adopted, for example, under Canadian law.²⁶

Leaving the enforcement of such practices to the self-regulation of platforms may not be a feasible or appropriate method of ensuring compliance with the above norms. As an alternative, the Government may consider establishing an office of an independent social media ombudsman which can have the powers of public oversight of content moderation practices, along with powers to issue appropriate and proportionate sanctions for failure to apply such standards in good faith. The ombudsman can also be responsible for working with specific platforms under its purview to develop codes of practice. One example of such 'regulated self-regulation' is provided under the German Network Enforcement Act, which provides incentives for social networks under its purview to self-

²⁵ 'The Santa Clara Principles on Transparency and Accountability of Content Moderation Practices', available at http://globalnetpolicy.org/wp-content/uploads/2018/05/Santa-Clara-Principles_t.pdf.

²⁶ Canadian Office of Consumer Affairs, 'Notice and Notice Regime', available at <http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html>.

regulate through an independent body.²⁷

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

²⁷ William Echikson and Olivia Knodt, 'Germany's NetzDG: A key test for combatting online hate', (November 2018), *available at* https://www.counterextremism.com/sites/default/files/CEP-CEPS%20NetzDG%20Report_112218.pdf.

We understand that the amendments proposed in the Draft Intermediary Rules have been introduced as a measure to curtail amongst others, “misuse of social media platforms and spreading of fake news”. We, as the intermediary, have some observations/comments/suggestions which are discussed in detail below:

I. Deployment of automated tools

Rule 3(9) of the Draft Intermediary Rules introduces a new obligation on an intermediary to “deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

It seems that this draft rule has been added in a haste and its overall repercussions have not been deeply thought through. By use of the words ‘automated tools’ it appears that the government is referring to artificial intelligence-oriented technologies, which will exhibit intelligent human like learning, thought, discretion and will have the ability to identify, disable or remove any ‘unlawful information or content’ from the intermediary’s platform and block public access of such ‘unlawful information or content’.

However, it must be mentioned at the very outset that the technology of artificial intelligence is at a very nascent stage. In the present day, it is very difficult for anyone to build an automated tool that will be able to review content and make the complex decision of ‘unlawfulness’ of any and all types of content with the required accuracy. To our mind, there are major technical challenges to developing such an ‘automated tool’ which have been discussed in detail below and therefore, in our view implementing such a rule will become a challenge if not an impossibility.

1. *Lack of sentiment and ability of complex analysis by the automated tools*

As mentioned before, ‘self-aware artificial intelligence’ or ‘general artificial intelligence’ which mimics human behaviour, emotions, thought and decision-making pattern has a long path to cover and still under development.

Decisions around what is to be considered “lawful or unlawful content or information” will be based on a very complex set of factors, besides being subjective. In fact it has been noted that even the courts in India take time to deliberate and assess as to what content/information is unlawful as per (i) the existing rule 3(2); and (ii) grounds for reasonable restrictions to Article 19 (2) of the Constitution of India (*Fundamental right to freedom of speech and expression*), and even so different benches may consider one type of content ‘unlawful’ while the other bench may disagree to such an interpretation. Therefore, frankly it is unthinkable to develop a technology with such complex decision making that will meet the ends of this Draft Rule 3(9).

Practically, in order to develop such an automated tool, it will be a good starting point if the government clearly lists out 'restricted keywords' that a software can be programmed to block from an intermediary's platform. However, it is suggested that more deliberations on development of this automated tool be held with the intermediaries and software developer community to find a more practical solution for implementing this draft rule.

For an enterprise communications solutions provider like Exotel, there are additional challenges. We work under a telecom license and provide our customers conference calling and IVR (interactive voice response) services. In this regard, it will be difficult for us to develop an automated tool ensure that no unlawful content/information is communicated on the conference call. Also, to develop an automated tool to keep unlawful content or information from being communicated through IVR, the automated tool/software will have to be input with 'keywords' or 'key phrases' or 'key messages' that the government should specifically set out. Without such clarity of instructions from the government, this automated tool could become a means for unauthorised censorship by intermediaries and may be misused in ways that we cannot yet imagine.

2. *No definition of unlawful content or information*

The Draft Intermediary Rules fail to provide a clear and specific definition of what constitutes 'unlawful information or content'. If such automated tools have to be employed by the intermediaries with the immediate effect then it is important to provide such tool with ready 'keywords' or 'details' of what is 'unlawful information' and for which sentiment analysis is not involved. In this regard, it is important to define 'unlawful content or information' in terms of specific keywords or specific cases (eg. bloodshed, rapes, child pornography) which will have to be fed into the automated tool/software so developed.

Without very clear and specific parameters given by the government (such as restricted keywords), it will be extremely challenging for an intermediary to comply with the Draft Rule 3(9).

3. *Time and cost constraint in developing such new technology*

Development of such a 'automated tool' which will be a software (including software based on machine learning or artificial intelligence), is a time consuming and expensive affair. It will take time to develop a software that will simply block content containing restricted keywords. If the vision of the government is that of creating a machine learning oriented software, this will take a much longer period. The software based on machine learning will have to be fed requisite information, different use cases, restrictive keywords over a much longer period of time. In addition to the time expense, development of such technology is likely to come at a large monetary expense. It is our opinion that if government wants to retain the

obligation under Draft Rule 3(9), the government should provide intermediaries atleast one year for developing and implementing an 'automated tool' before bringing this obligation in effect and set down clear and measurable minimum performance standards that the 'automated tool' is required to qualify.

II. Assistance to the government in investigation

Rule 3 (5) of the Draft Intermediary Rules provides that *“when required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”*

The draft rule provides that when an intermediary receives a request from the government (or its agency) for assistance concerning cyber security or in an investigation, the intermediary shall provide such assistance within 72 hours (3 days) from receiving such a request. Further, it is provided that such assistance may include tracing of the originator of the information under investigation.

As discussed earlier, Exotel is an enterprise cloud communication service provider wherein the customers of Exotel are enterprises/businesses. In our user agreements with our customers/immediate users, we have an obligation to keep their information confidential and only disclose information to a government authority when supported by a legal notice or order. Some of our customers are also intermediaries and they in turn have an obligation to their end users to not disclose their end users' information to a third party such as us. In some cases, the end users of our customer (an intermediary) may also be using communication services provided by us through the Exotel account of our customer (intermediary); and under new draft rule 3(5), the government may require information from Exotel (an intermediary) about an end-user of our customer (another intermediary). In such a case, it would be best for intermediaries like Exotel serving other intermediaries to direct the government to their customer (concerned intermediary) for obtaining any information related to the latter's end-user.

A clarification should be made in this rule to that extent stating that: *“In case of an intermediary serving other intermediaries, the intermediary may direct the government agencies to its immediate user intermediary.”*

Therefore, as stated above in a business-to-business availing of services, the assistance that Exotel can provide is directing the authorities to the relevant enterprise whose users are the originators of the information and may not necessarily direct them to the originator of information themselves. Therefore, this exception may be carved out for the enterprise communication platforms who necessarily do not deal with end users

directly in the manner specified above or in any other language that may be considered fit for the purpose.

We understand the motive behind introducing such rule. However, owing to the diversity in the nature of different intermediary platforms, it is suggested that a blanket requirement should not be put on all intermediaries. This draft rule should be revised keeping in view the different types of services intermediaries may be providing.

III. Notifying users once a month

Rule 3(4) provides that *“the intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.”*

As stated earlier, owing to the nature of services we provide, our customers or users of our software product are businesses. Through the accounts of our customers (businesses) on our platform, the software may be used by the customer’s employees or other end-users. We generally do not deal directly with end-users of our immediate customers. Therefore, at most, we can inform our immediate customers/ users (the businesses) of the effects of non-compliance with rules and regulations, user agreement and privacy policy are required by the draft rule 3(4).

We, therefore, suggest that an **amendment** be made to the draft rule with following effect:

“(4) The intermediary shall inform its immediate users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the immediate users to the computer resource of Intermediary and remove noncompliant information.”

**RESPONSE TO MEITY: THE DRAFT INFORMATION TECHNOLOGY INTERMEDIARIES
GUIDELINES (AMENDMENT) RULES, 2018**

The Ministry of Electronics and Information Technology (**MEITY**) has 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 is 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 the intermediaries more accountable, we believe that there are certain lacunae and concerns which need to be addressed.

MEITY has invited public comments on the Draft Rules. The key observations and comments to the Draft Rules are as listed below.

1. Rule 3(2) of the Draft Rules

The Draft Rules require intermediaries to inform their users against hosting any material that may threaten the critical information infrastructure (the “**CII**”) or public health or safety¹.

IndusLaw Comments

Rule 3 (2) (k) of the Draft Rules require the intermediary to display rules informing the users not to host, publish any information that *inter alia* threatens CII.² However, there are practical challenges associated with this. Users and intermediary, 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, in order to obtain a court order to request the intermediary to take-down such content from its platform, will be a challenge. The intermediaries will also not be in a position to deploy technology based automated tools or other control mechanisms for pro-actively identifying content that are likely to threaten CII and removing / disabling such content under Rule 3(9) of the Draft Rules. We hence are of the opinion that the Draft Rules should (i) either objectively elaborate on the nature of information/content that is perceived as a threat to CII; or (ii) prescribe standards to determine whether any content is likely to threaten CII.

Rule 3 (2) (j) which has been added in the Draft Rules require the intermediary to display rules informing the users not to host, 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*³, the Hon’ble Supreme Court citing *Grayned v. City of Rockford*, has noted that the law on the subject of vagueness is clearly stated thus:

¹ CII has been defined to mean any computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

² 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.

³ AIR 2015 SC 1523.

“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 'abuts 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)” .

It may be advisable to clarify in Rule 3 (2) (j) the exact nature of information that cannot be posted, e.g., the restrictions on the advertisement and media sector under the applicable laws, etc.

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 ⁴, it is necessary that Rule 3 (2) (i) of the Draft Rules is streamlined in accordance with the reasonable restrictions on the freedom of speech under Article 19(2) of the Indian Constitution.

2. Rule 3 (4) of the Draft Rules

The Draft Rules mandates the 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.⁵

IndusLaw Comments

There are 2 (two) points to note here:

- i) 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 the 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 the 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.

⁴ AIR 2015 SC 1523

⁵ Rule 3(4), Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018.

- ii) A requirement of this nature poses a challenge for small scale start up intermediaries or intermediaries having a smaller user-base. This requirement may add up to their financial burden. Therefore, 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. Uniform imposition of such requirement will create an uneven playing field which is against the principle of fair market economy.

3. Rule 3 (5) of the Draft Rules

Rule 3 (5) in the Draft Rules incorporates several procedural changes.

IndusLaw Comments

The requirement for providing assistance and information to government agencies in a time bound manner is a welcome measure as it serves the interest of the nation.

Please find our specific comments in relation to proposed Rule 3 (5) of the Draft Rules below:

S. No.	Changes to the Current Rules	IndusLaw Comments
a)	An intermediary is required to provide the information requested under a lawful order, within 72 (seventy two) hours from the communication.	
b)	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 offence(s); protective or cyber security and matters connected with or incidental thereto.	i) The provision '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 the specified grounds such as 'assistance for security of the State, cyber security,' etc. 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:

		<p>a. fish for information thereby exposing the private information of citizens to scrutiny.</p> <p>b. 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.</p> <p>The Draft Rules should limit the nature of information that can be requested by a Government agency to the grounds specified in Rule 3(5) and the lawful order should specify the nature and extent of assistance that is expected from the intermediary.</p> <p><i>Drafting Point:</i> 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 the government agencies authorized with investigative, protective and cyber security activity. It is requested that Rule 3 (5) be revised to clarify that the right vests with appropriate Government and its agencies who are armed with a lawful order.</p>
c)	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.
d)	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 sad affair of the mob lynching caused due to the recent social media messages and other social media news is indeed a menace to the society. To that end this measure is commendable. However, in the present form the requirement is not qualified by any requirement and appears to provide an omnibus

	<p>right to demand the tracing of any information. This means that:</p> <ol style="list-style-type: none"> i) 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, ii) there is potential for the breach of the fundamental right of speech of Indian citizens, and iii) there is an enhanced onus on the intermediaries to have accurate and updated identification records of each user of the platform, in a manner that can be shared with the government agencies. <p>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.</p>
--	---

4. Rule 3(7) of the Draft Rules

Under the Draft Rules, it has been stated that an intermediary who has more than 50 (fifty) lakh users in India or an intermediary who has been specifically listed as per 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 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.⁶

IndusLaw Comments

The mandate for being registered as a company under the company laws of India and having a permanent registered office in India would prove to be financially as well as logistically burdensome for certain intermediaries, especially small scale start up intermediaries having more than 50 (fifty) lakh users. In addition, it will also deter foreign intermediaries from doing business in India as there will be additional statutory compliances and costs for the same. Further, such requirement may also create permanent establishment risks for certain foreign intermediaries.

⁶ Rule 3(7), Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018

Although the revisions in the Draft Rules make it easier for the Indian courts to exercise jurisdiction over intermediaries situated outside India - 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 Computer⁷ or a Computer System⁸ or a Computer Network⁹ located within India. Further, the concern in relation to protecting the personal data collected by intermediaries with over 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. The requirement of a permanent registered office in India with a physical address may place a higher burden on the intermediaries than even 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. 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 kind, for example, orders relating to unlawful acts relating to Article 19 (2) of the Indian Constitution.

5. Rule 3(8) and Rule 3(9) of the Draft Rules

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 unlawful acts relating to Article 19(2) of the Indian Constitution such as 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.

IndusLaw Comments

We have tabled the requirement under the Current Rules and compared it with the requirement under the Draft Rules below:

⁷ 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.

⁸ 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.

⁹ 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

Sl. No.	Current Rules	Draft Rules	IndusLaw Comments
1.	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 Act...	<p>The Draft Rules proposes to codify the evolving jurisprudence on this subject.</p> <p>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 the intermediaries to take action only upon receiving a court order or a notification from a regulatory authority. This safeguards the intermediaries from excessive responsibility or liability.</p> <p>The requirement for taking down content by an intermediary only on receiving a court order is commendable, protecting the interest of the both the intermediary and its users - as it is not practicable for an intermediary to examine all uploaded content to evaluate whether it is liable to remove or disable access.</p>
2.	As per 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 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 takedown 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. 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 only to those in relation to Article 19(2) of the Indian Constitution.
3.	Rule 3(4) of the Current Rules also covered a request for take down of content that infringed intellectual property.	The Draft Rules does 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/ executive order for actual knowledge to be constituted under Section 79(3)(b). Therefore, in light of the above, it is important that the intermediaries should have the power to address take down requests for intellectual property infringement, in the absence of a court/executive order, unless the intermediary reasonably and bonafidely believes that they are not in a position to assess actual intellectual property infringement from the take down notice, and would require a court or executive order to take down the content.
4.	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.
5.	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 will mean that the intermediaries will have to incur additional costs in preserving and safeguarding user data/records for a longer period, to ensure that there is no misuse or unauthorized access to data during this period.

As per 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.¹⁰

The requirement to install automated tools have been previously discussed under the Supreme Court's judgment- *Sabu Mathew George vs. Union of India*¹¹. However, under the Draft Rules, there is no clarity on the manner in which the 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, the use of such automated tools may arbitrarily, excessively and disproportionately pre-censor information and content, having a chilling effect on an individual's right to free speech, defeating the intention behind the Supreme Court's judgment- *Shreya Singhal vs. Union of India*¹²

There is a need to set out certain standards and specifications with respect to use of automated tools to ensure uniformity in the digital space, however the risk of over-censorship would still prevail.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

¹⁰ Rule 3(9), Draft Information Technology (Intermediary Guidelines (Amendments) Rules, 2018.

¹¹ 2017(1) RC R (Civil) 175.

¹² 2015X AD (S.C.) 586.

Internet Society India, Delhi Chapter's (ISOC Delhi) comments on the Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018

Internet Society India, Delhi Chapter (ISOC Delhi) is pleased to submit these comments to the Ministry of Electronics and Information Technology (MeitY) on the draft Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018.

ISOC Delhi is a chapter of the Internet Society, and one of six Internet Society Chapters in India. The Internet Society is a global not-for profit organization that supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society."

Intermediary Liability in India

Before making specific comments on the Amendment we wish to draw your attention to the existing legislation and legal rulings that shape intermediary liability in India.

Under the Information Technology Act, 2000 (IT Act), an 'intermediary' with respect to any particular electronic message means "any person who on behalf of another person receives, stores, or transmits that message or provides any service with respect to that message." Under the IT Act, intermediaries include telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places, and cyber cafes. The IT Act provides safe harbour protection to intermediaries, that is, legal immunity from any liability arising from content hosted by third-parties on an intermediary's platform. However, the Information Technology (Intermediaries Guidelines) Rules, 2011 introduces the due diligence practices intermediaries must observe in order to avail safe harbour protection under the IT Act. These due diligence practices under the existing Intermediary Guidelines include merely acting as a facilitator with respect to the information being made available on the intermediary's platform, **not** initiating the transmission, selecting the receiver of transmission, and selecting or modifying the information contained in the transmission.

Since the safe harbour protection is an exemption that intermediaries can avail by fulfilling certain conditions specified under the IT Act, we are of the view that any additional obligations on intermediaries would have to comply with the ruling in *Shreya Singhal v. Union of India* (*Shreya Singhal case*).

In the *Shreya Singhal case* of 2015, the Supreme Court of India (*SC*) struck down Section 66A of the IT Act and declared it unconstitutionally vague as it consisted of ambiguous language such as "grossly offensive", "menacing", "false", and "causing annoyance, inconvenience, danger". The SC upheld that any request for restricting or taking down content from an intermediary's platform can only be carried out upon receiving actual knowledge through a valid court order or order by a government agency. Such requests must be in consonance with Article 19(2) of the Constitution of India, 1950 (Constitution), which provides for 'reasonable restrictions' on the freedom of speech and expression in specific cases only such as security of the State, defamation, contempt of court, etc. Requests must also comply with the due process laid down

under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules).

International Standards

International standards, such as the Manila Principles, also guide nations across the globe on the regulation of intermediaries. The Manila Principles state that:

- Intermediaries should be shielded from liability for third-party content uploaded on its platform.
- Content must not be restricted unless by an order by a competent judicial order
- Requests for take down of content must be clear and follow due process.
- Laws and content restriction orders must comply with the tests of legality, necessity, and proportionality.
- Transparency and accountability must be built into laws and content restriction policies.

Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018

ISOC Delhi believes that **the Amendment fails to adhere to the above mentioned global standards and judicial precedents in India**. The Amendment proposes changes which go way beyond the practices intermediaries ought to undertake while maintaining neutrality in relation to the content on their platforms. The Amendment significantly affects not only the status of intermediaries but also affects third-party users' constitutional rights in India. The Amendment could cause intermediaries to weaken their end-to-end encryption, putting Indian users at greater risk.

Please find our detailed comments to the specific changes proposed by the Amendment below:

1. **Disclaimers** – The existing Intermediary Guidelines impose an obligation on intermediaries to inform users using its platform not to post content of certain nature such as content that is defamatory, harmful to children, blasphemous, etc. The Amendment introduces two additional disclaimers, namely, information that threatens public health and safety, and critical information infrastructure.

The Amendment fails to prescribe any specific considerations on how content is likely to threaten public safety, health, or critical information infrastructure in India. Since the Constitution allows for restriction on the freedom of speech and expression under the particular grounds identified therein, this provision is likely to be arbitrarily interpreted, which may, in turn, impose unreasonable restrictions on the freedom of speech and expression. Since the Shreya Singhal case has clarified that any restriction on free speech

must be within the contours of Article 19(2) of the Constitution, this provision is in contradiction to the SC's ruling.

Further, there is a greater need for careful, responsible, peer-reviewed and research on the content and its implications towards blocking and surveillance.

2. **Monthly Information** – Under the provisions of the Amendment, intermediaries are now required to inform its users that “non-compliance with rules and regulations, user agreement and privacy policy” may lead to the termination of access or usage rights and removal of non-compliant information once every month.

This provision is not only burdensome for intermediaries in terms of increased expenditure on such compliance, it may lead to notification fatigue among users using the intermediary's platform. Given the lack of a causal link between the result to be achieved and measures adopted under the Amendment, we are of the view that such a change in the existing Intermediary Guidelines is not necessary. We would rather propose that whenever there is an update of policies or services, the intermediaries notify their users of these changes.

Further, a generic polite warning be notified instead of targeting individual users indicating that repeated posting of abusive content be restricted.

3. **Tracing the originator of information** – The Amendment mandates intermediaries to trace the originator of information uploaded on the platform if and when required by government agencies and within 72 hours of such request. Additionally, intermediaries are required to provide any information and assistance “as asked by any government agency or assistance concerning security of State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto” upon receiving a lawful order. This provision falls short of providing for procedural safeguards or adequate justification with respect to requests made by government agencies. This provision seems to be in contravention of the SC's ruling in the case of *K. Puttaswamy v. Union of India* (Puttaswamy case), which upheld the right to privacy of an individual as a fundamental right granted to Indian citizens under Part III of the Constitution. In the Puttaswamy case, the SC laid down a three-pronged test of legality, necessity, and proportionality with respect to any action that limits the right to privacy –
 - i. Legality – which postulates the existence of law;
 - ii. Necessity – defined in terms of a legitimate state aim; and
 - iii. Proportionality – which ensures a rational nexus between the objects and the means adopted to achieve them.
4. **Incorporation of Indian entity and designation of nodal officer** – The Amendment imposes an obligation on intermediaries with more than 50 lakh users, to establish a

presence in India by incorporating an entity and registered office in India. Additionally, intermediaries are now required to designate a nodal officer who shall be available 24 x 7 to interact with the law enforcement agencies in India.

While the intent may be to increase accountability of such intermediaries, we are of the opinion that the intermediaries guidelines is not the appropriate document for incorporating such requirements to make companies more accountable.

- 5. Blocking Orders** – The Amendment mandates intermediaries to remove any unlawful content within 24 hours of actual notice by a court or government agency. However, the Amendment does not provide for adequate safeguards when such take down request is made by a government agency without judicial authorization. Such a requirement can be abused due to the lack of adequate safeguards. Additionally, as noted by the Supreme Court in Shreya Singhal, Section 79 of the Information Technology Act is an exemption provision and cannot be used for issuing blocking orders.

Additionally, the proposed time frame of 24 hours to remove content does not allow an intermediary to review the request before taking down content. This is likely to result in third-party action against the intermediary for such take down. The Amendment also fails to provide for safeguards with respect to retaining records for 180 days or “such longer period as required by government agencies or courts”.

Further for small and medium scale enterprises and for start-ups these content management will be a tall order and obligations disproportionate to their resources.

- 6. Monitoring** – The Amendment requires intermediaries to proactively screen content that is hosted or uploaded on its platforms, which is also in contradiction to the SC’s ruling in the Shreya Singhal case. The SC has clarified that intermediaries must not be required to screen content or assess the legality of such content. Not only does this requirement impose a restriction on the right to free speech and expression, and right to privacy, it is also unreasonable for intermediaries to carry out such monitoring.

Further, by tying intermediary safe harbour to content monitoring, the government could require intermediaries to weaken the security of their services. For end-to-end encrypted services, only the sender and receiver of information have access to the content. No third party, even the intermediary providing the service, has access to that content. When intermediaries are required to proactively screen content on its platform, end-to-end encryption is no longer usable. The government should refrain from asking intermediaries to proactively screen content as that will not only erode trust of people, weaken the use of strong encryption and lead to censorship, but will also fail to achieve the objectives which the government is aiming at, while impacting all intermediaries.^[1] There are no easy answers to the discussion around proactive monitoring, encryption and lawful access. However, through identifying nuances, areas for improvement adhering to

international principles or norms and through public and private cooperation the issues can be addressed to a considerable extent^[2].

Concluding Remarks:

To achieve the objectives of National Digital Communications Policy, 2018 of ensuring online trust, security, and privacy, the Government must ensure that a symbiotic relationship is maintained between intermediaries, users, and the regulator. Since intermediaries facilitate day-to-day activities such as access, communication, business and trade, information and social media, any regulation of intermediaries should be aimed at allowing intermediaries to function in a smooth manner without adversely affecting the digital economy or imposing unreasonable restrictions on the rights of the users.

The Government should not attempt to remedy discrete challenges through rules which will impact all intermediaries. Instead it should ensure that intermediaries are not burdened with extensive, stringent obligations, which may hinder their ability to enter the Indian market or provide quality services to existing users.

There is a need to have a balance among the various stake holders. How this intermediary changes are going to affect conflicting requirements of users, service providers, technical / network community, policy makers from the point of view of compliance, cost, risks, technical expertise, is the critical question.

Further a way forward may be to have a dialogue, collaboration and cooperation within the multi-stakeholder environment.

ISOC Delhi thanks the Ministry of Electronics and Information Technology (MeitY) for the opportunity to comment on the Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018 and looks forward to continued engagement on these issues.

IAMAI Response to The Information Technology Intermediary (Amendment) Rules 2018

Background to the Submission

Intermediaries are recognized by Section 2(w) of the Information Technology Act 2000 (“IT Act”) as *“Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.”*

Section 79 of the Act exempts the liability of Intermediary in certain cases. This exemption is based on compliance with the conditions specified therein, including the understanding that intermediaries are not liable if their action is *“limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or the intermediary does not (i) initiate the transmission, (ii) select the receiver of the transmission and (iii) select or modify the information contained in the transmission”*.

The Supreme Court of India in its landmark judgment on the Information Technology Act, 2000 i.e. *Shreya Singhal v. Union of India*, (Writ petition (Criminal) No 167 of 2012) upheld the online right to freedom of speech and expression by striking down section 66[a] of the IT Act and reading down Section 79.

The Apex Court found that a combined reading of Section 79(3)(b) and Rule 3(4) of the Intermediary Rules means that the intermediary must receive a court order/ notification from a government agency in order to remove content. Further, such a notification or a Court order must necessarily fall within the ambit of the restrictions under Article 19(2) of the Constitution of India. The Court ordered a read down *“...This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.”*

The highlights of this judgment regarding Intermediaries, intermediary liabilities and safe harbor provisions are:

- Certain *digital services qualify as intermediaries with exemption provisions of safe-harbor*, provided those services abide by certain limitations of scope and due diligence as provided by the IT Act.
- In light of the volume of information and thereby requests received by an intermediary, section 79(3)(b) and the Intermediary Guidelines must necessarily be

read down, failing which the intermediary would be placed in the role of an adjudicator.

- The critical *aspect of 'knowledge' of misdoing and availing this knowledge via court order or appropriate government agencies*, is reactive (rather than proactive) as the liabilities of intermediaries is being limited to removal of content and sharing details of such information with law authorities on official request.
- There is no requirement of active monitoring of content on intermediary platforms to determine their legality.

The intent of the Legislature in limiting the duty of due diligence and in omitting of a proactive duty of monitoring on the intermediary under section 79 of the IT Act is also observed by a Single Judge of the Delhi High Court deciding a case of design infringement in the case of Kent RO Systems & Anr v. Amit Kotak & Ors. (C.S.(Comm.) 1655/2016) in which it was observed that imposing an obligation of proactive monitoring on an intermediary would result in an unreasonable burden on the intermediary.

Any amendment to the Intermediary rules needs to be read with the main body of the IT Act and its interpretations by the Courts. This is the context in which we have analysed the draft rules below.

Our detailed submission to the draft amendments, based on this basic understanding is as follows.

Proposed Amendment (4) The intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of intermediary and remove noncompliant information.

Issues: Intermediaries offer varied services across sectors and scope of services or technical capability and it is not possible to adopt a hard and fast rule to be applied in all the situations to come and in all the circumstances. Monthly notices will lead to spamming and user fatigue, leading to poor user experience.

IAMA Submission: The Intermediaries' services cut across sectors and services making it impossible to have a single mode of communication with the consumer. The frequency of the 'communication' will vary according to the business models Therefore, we suggest intermediaries be allowed to determine how to communicate with their users, while agreeing in principle that constant communication with consumers is important.

Proposed Amendment: 3(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or

investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.

Issues: The proposed amendment is beyond the scope of Section 79 which is an exemption provision and hence it cannot be used to introduce new obligations on request for information and assistance, and traceability.

The obligation on intermediaries to trace such communications would be violation of the right to privacy recognized by the Supreme Court in the case *KS Puttaswamy v. Union of India*, which is an important fundamental right exercised by the users of any platform. It must be noted that any assistance that can be provided by an intermediary platform can already be sought under the Code of Criminal Procedure.

The 72 hours deadline is arbitrary and does not consider factors such as communication time within an organization, cases where extensive human intervention may be required due to programming / system requirements, time required for authentication of request.

IAMA Submission: Asking intermediaries to assist in investigations and enable tracing cannot be a condition for intermediary rights. Provisions of Section 79 are meant to be safe harbor exceptions from certain liabilities as detailed in other sections of the IT Act. Any amendment in provisions for assistance from intermediaries must be done via amendments in other relevant sections of the IT Act that deal with such provisions.

Proposed Amendment (7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;**
- (ii) have a permanent registered office in India with physical address; and**
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.**

Issues: The threshold for selection of intermediaries that are covered within this rule is arbitrary. There is neither any reasoning for the fifty-lakh user requirement nor for the intermediaries that shall be covered by means of the government notification.

Many digital platforms providing global services do so from limited jurisdictions and centrally located data centre/operation headquarters. It is likely that incorporating in several countries of operation as required by this provision, would not be financially sound.

IAMAI Submission: We request that a safe harbor provision in this legislation be not used to mandate local incorporation, which constitutes a trade barrier on global companies. The Companies Act, 2013 provides detailed provisions for the regulatory environment which the Companies need to follow on the basis of their classification as per the Act to do business in India. Any additional requirements have to come through Amendments in that Act.

We submit that the proposed amendment is ultra vires the provisions of IT Act. The inclusion of this requirement on any intermediaries must be by way of an Act of the Legislature with appropriate Parliamentary sanction.

Proposed Amendment: (8) 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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.

Issues: The revision of the takedown notice mechanism is a departure from the Supreme Court judgment as it explicitly expands the mechanisms of knowledge beyond court order. Suggesting 'appropriate Government or its agency' without qualifying the agencies allows for wide reaching influences that would be impossible to abide by.

'Remove or disable access' makes it a take-down provision that comes under the purview of section 69. It is to be noted that Section 79(3)(b) is applicable in all the circumstances where the intermediary has to act upon at its own discretion. The proposed amendment extends the period of storage of information and associated records to 180 days and indefinitely, as required by government agencies. Such a requirement is not just created without any checks and balances, but also leads to concerns regarding the privacy of the users involved with such information and records.

IAMAI Submission: It is agreed that take down requests must be complied within a reasonable time period. However, such stipulation should be brought under Section 69A Rules, which empowers the Government to send takedown requests. As per *Shreya Singhal v. Union of India*, section 79 of the IT Act is an exemption provision and does not empower the Government to send take down requests.

IAMAI recommends that the discussion on time limits for complying with take down requests should be taken up under Section 69A and rules thereof and not under Section 79 which deals with exemptions only.

Proposed Amendment: (9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

Issues: This provision is a gross violation of Section 79 (2) of the IT Act as it proposes the intermediaries to 'select and modify the information contained in the transmission' and thereby select/restrict the receiver of the communication. herein an intermediary is forced to violate section 79(2)(b), i.e. give up its statutory immunity in order to comply with section 79(2)(c), i.e. protect its statutory immunity.

The Supreme Court categorically read down Section 79(3)(b) to suggest intermediaries only had a reactive role in removing content to play upon receiving knowledge. Holding these service providers to proactively monitor content is in violation of the Supreme Court judgment. Notably, the Supreme Court also recognized that in light of the volume of data processed by intermediaries, the latter cannot be placed in an adjudicatory role.

IAMAI Submission: We believe that safe harbour protections, which are guaranteed by the Statute and endorsed by the Apex Court, must not be changed. The provision 'unlawful information' is prone to subjective interpretations, especially where multiple authorities can make such requests without any judicial vetoing of such requests. Moreover, each intermediary may treat the same information differently, given the vagueness of the definition of 'unlawful information', potentially creating a situation where unlawful content may still be available.

The entire provision may lead to multiple governmental authorities sending requests based on their limited and subjective interpretations, which can not only make business operations of intermediaries onerous but can also have grave consequences for freedom of speech and expression in the country. Therefore, it is better if a centralized authority issued directives under Section 69 to all intermediaries to maintain uniformity in interpretation and action.

Conclusion

The IT Act, and the Supreme Court judgment categorically recognizes certain digital services as intermediaries and upholds certain exemptions for such services. However, the suggested amendments undermine Section 79 as:

- These amendments extend the scope of the Intermediary Guidelines beyond the letter and spirit of the IT Act. As the Intermediary Guidelines are formed in exercise of the powers conferred under the IT Act, specifically section 79(2) and are

delegated legislation, the Intermediary Guidelines cannot traverse beyond the scope of the section or the other provisions of the IT Act.

- The amendments have a direct impact on the statutory exemption provided by section 79 and, in effect, overhaul the immunity guaranteed to intermediaries. Any amendment to the immunity or scope thereof, can only be made by the Legislature by means of an amendment of the Act.

In our collective understanding some of the proposed amendments are in direct contravention to the Shreya Singhal judgment and will amount to compromise of user privacy, make intermediaries party to state driven censorship and overall rob intermediaries of the exemptions provided by the IT Act and upheld by the Supreme Court in its landmark judgment.

The objectives of the proposed amendments are unclear, and we would urge MeitY to initiate a Stakeholder's Consultation outlining the key objectives which Government seeks to achieve through these proposed amendments.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

CII inputs on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

Introduction

The Confederation of Indian Industries (“**CII**”) is an industry-led and industry-managed organization which has several thousand members from the private as well as public sectors, including SMEs and MNCs. We have a history of assisting the government on important issues of law and policy and have been a critical force of change in India’s past policy reforms. In this context, we would like to offer our inputs on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 (“**Draft Amendment**”) which seek to amend the Information Technology (Intermediary Guidelines) Rules, 2011 (“**Intermediary Guidelines**”) under the Information Technology Act, 2000 (“**IT Act**”). We believe that the advent of various types of intermediaries providing a variety of services over the internet, has revolutionised the way in which Indian internet users communicate, consume content and products, and engage in trade and business. Thus, any legal framework impacting intermediaries are of critical importance for both internet users as well as service providers in India.

The Draft Amendment Has a Detrimental Impact on the Right to Privacy

The Supreme Court of India (“**Supreme Court**”) has recently upheld a fundamental right to privacy of individuals, as a critical and essential component of the right to life and liberty under Article 21 of the Constitution of India, 1950 (“**the Constitution**”). While upholding this right, the Supreme Court stated that any limitation on the right to privacy should satisfy the following three requirements:

- legality, which postulates the existence of law;
- need, defined in terms of a legitimate state aim; and
- proportionality, which ensures a rational nexus between the objects and the means adopted to achieve them.

In this context, we would like to submit that the Draft Amendment poses several critical impediments to the right to privacy of individuals, but fails to satisfy the three-pronged test that is laid down for this purpose. Given that several provisions of the Draft Amendment could have a crucial bearing on the fundamental right to privacy, it is important to ensure that any potential violation of this right enshrined in law is backed up by a broadly recognized need, and fulfils the requirement of proportionality.

The lack of legitimate state aim and proportionality can be evinced through the following provisions of the Draft Amendment as examples:

- (a) *Requiring tracing of originator:*

Rule 3(5) specifies that in order to claim exemption from intermediary liability, an intermediary would have to enable tracing out the originator of information on its platform as may be required by authorized government agencies. While this may constitute a restraint on the right to privacy of the originator, there are no safeguards to ensure that the provision is not misused and does not create undue constraints on any fundamental rights. Thus, the requirements of need and proportionality are not demonstrably fulfilled by this legal provision.

(b) Active monitoring of content / expansive list of grounds:

The Draft Amendment mandates active monitoring and filtering of content through automated tools, as a pre-requisite for an intermediary to be able to claim exemption from liability. This creates a legal incentive for intermediaries to engage in overbroad censoring of content in order to retain legal immunity, thereby potentially censoring lawful content and violating the privacy of users.

In light of these concerns, it is critical that the exercise of amending the Intermediary Guidelines should be based on a much broader consultation specifically with the aim of safeguarding the privacy of users and without introducing provisions that are more intrusive than required.

The Draft Amendment Creates Unclear / Onerous Obligations

Given that all sub-rules under Rule 3 of the Intermediary Guidelines deal with the obligations that an intermediary must fulfil in order to claim safe harbor from prosecution, it is important for the language to be adequately clear and not unnecessarily onerous. The lack of clarity in relation to the obligations under the Intermediary Guidelines could lead to arbitrary prosecution, and onerous obligations that are likely to potentially drive several intermediaries out of business in India. Some of the unclear and/or onerous obligations sought to be introduced are highlighted below:

- (a) The draft rules use various terms such as ‘any government agency’ lawfully authorized government agency, appropriate government agency, government agencies who are legally authorized, in various provisions, creating confusion and ambiguity and likely to lead to implementation challenges. It is suggested that the terminology be uniform, clear and unambiguous.
- (b) Rule 3(2) which add two further provisions in the due diligence requirements, viz. threaten public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol, etc and threatens critical information infrastructure are vague and ambiguous provision as the terms ‘threaten’ promote etc and not clearly defined and may be open to subjectivity. .

- (c) The proposed amendment in several provisions have added or modified the timelines making them more stringent and therefore onerous to comply with. This has been done without any basis or justification and may thus be considered arbitrary.
- (d) Rule 3(5) of the Draft Amendment mandates providing “information and assistance” as asked for by any government agency when required by lawful order, without specifying the scope of what constitutes the same. Further, the language of the sub-rule states that what could be demanded of an intermediary may fall into any of the following categories:
- information or assistance as asked for by any government agency;
 - OR assistance concerning security of the State or cyber security;
 - OR investigation or detection or prosecution or prevention of offence(s).

The placement of the term “or” in the present iteration of the above sub-rule in the Draft Amendment makes it unclear whether the terms such as “security of state”, “cyber security”, “prosecution or prevention of offences” are meant to serve as purpose limitations on the scope of assistance sought, or whether *any* assistance could be sought by any government agency relating to issues in addition to these issues identified under the proposed rule. This makes the actual obligation on the intermediary quite unclear and overbroad.

- (e) The provision that the request can be made by ‘any’ government agency is without any procedural safeguards and may be subject to misuse.
- (f) Rule 3(5) also states that the intermediary will “enable” tracing out of originator of content – this may not be practically possible to implement as each intermediary may only be able to assist to the extent of the origin of the information at their end. Further, this provision is not phrased as an endeavor clause or a best efforts clause, which means that it is unclear whether the intermediary has to conclusively trace content originators in pursuance of this obligation. Apart from the practical limitations, in this case, there could be major technological changes necessary in order to introduce traceability of content. In this context, it is worth noting that several intermediary platforms are already working closely with the government in order to come up with the best ways to combine the interests of law enforcement with the business and technology operations of said intermediaries. To impose a conclusive legal mandate may have undesirably restrictive impacts on such platforms without giving rise to a corresponding benefit. Further, to the extent proposed Rule 3(5) contemplates the storage of any data or information, no time period has been prescribed for any such storage, and no safeguards to protect user privacy been provided.

- (g) Rule 3(7) states that an intermediary who has more than fifty lakh users in India, or any other intermediary as notified, would have to incorporate in India, have a permanent registered office in India with physical address; and appoint in India, a nodal person of contact. While our telecom members have no comments to offer on this provision our other members believe that this may result in several intermediaries being unable to provide services in India if it is not feasible for them to incorporate in India. They also believe that the provision that any service provider that the government seeks to have visibility on for any reason could be asked to incorporate in India, without any criteria specified, would be an impossibly onerous task for small companies in particular.
- (h) Rule 3(9) mandates deployment of automated tools to monitor content. In addition to the fact that such an obligation is illegal (as it goes against express stated law in *Shreya Singhal vs. UOI* judgment of the Supreme Court), it is also extremely onerous as a precondition to getting safe harbour as it involves creating new technology with very little clarity on what threshold of content monitoring would meet the relevant criteria. Further, Rule 3(2) has introduced a requirement to notify users that any content they post that “threatens” public health or safety or critical information infrastructure, could be taken down. Assuming that this is regarded as being part of the “unlawful” content that should be proactively monitored and disabled by intermediaries, the lack of clarity on what “threatens” health or infrastructure would make the obligation of monitoring content especially ambiguous and onerous. This is without prejudice to a separate argument that no kind of monitoring obligations should be imposed on intermediaries at all.
- (i) Rule 3(4) mandates providing notifications every month specifying the disclaimers to be provided to users. These disclaimers are already provided in the terms and conditions of use of all websites, and requiring changes to the interface of all intermediaries across several jurisdictions for this purpose may be unduly onerous without serving any corresponding public benefit. Further, this could lead to notice fatigue on the part of the users thus failing to have its intended impact.

The Draft Amendment Lacks Procedural Safeguards

The Draft Amendment fails to satisfy the requirements of due process that are imperative for any restriction on the freedom of trade and commerce, freedom of speech and right to privacy as prescribed under the Constitution. There are several legal requirements sought to be introduced by the Draft Amendment which restrict the above rights in some capacity, but without adequate procedural safeguards. Some examples of this are as follows:

- (a) *Any lawfully authorized government agency can request tracing of originator / no limitation of purpose*

As pointed out earlier in this submission, the requirement of tracing an originator of information comes with inadequate procedural safeguards. From the perspective of the user, this constitutes a violation of their right to freedom of speech and expression, as well as their right to privacy, while from the perspective of the intermediary, this may impinge on their freedom of business and commerce as it may require the introduction of procedures to comply with these requirements that would potentially change several underlying technologies and business practices. In this context, it is also problematic that any lawfully authorized government agency can request tracing of originator, with no restrictions based on obtaining prior judicial authorization, seniority of law enforcement officers who can issue such requests, or any limitation on purpose for which such requests can be made. This amounts to a restriction on several fundamental freedoms without satisfying the requirement of consequent due process.

As the rule is structured presently, any member of a government agency could potentially request tracing an originator – regardless of the content created by the originator, and the intermediary would necessarily need to “enable” the same.

- (b) *Any government agency could request information or assistance*

Rule 3(5) states that when required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by *any* government agency. While the obligation on the intermediary comes with a strict time limit that has no specific justification, there is no corresponding obligation on the government agency to keep their requests limited to specific purposes, or even limit the scope of what is meant by “assistance.”

There is also an inconsistency in this provision as the former part of the provision requires information or assistance to be given to any government agency, whilst the latter part of the provision pertains to agencies who are legally authorized.

- (c) *Blocking orders can be issued without any safeguards*

Section 69A of the IT Act and the rules notified thereunder already provides for a procedure of issuing blocking orders with specific processes and safeguards. The Draft Amendment seeks to introduce a parallel process for the same under Section 79 of the IT Act without providing for any safeguards.

- (d) *Any company can be asked to incorporate in India*

Without specifying any grounds or any criteria for the same, the Draft Amendment specifies in Rule 3(7) that any intermediary may be required to incorporate in India if notified. This is an unclear and onerous provision that may deter several intermediaries from providing services in India. The proposed amendment does

not provide for any safeguards to prevent arbitrarily notifying companies for incorporation.

Draft Amendment May Violate International Standards / Norms / Obligations

There are several obligations that have been identified as being extremely broad in scope in the submission thus far. Some of these obligations, such as the requirement to establish local entities, appear to have no limitations by way of service sector, which may conflict with international obligations India has made in respect of sectors where cross border provisions of services are permitted without limitation.

Further, India has signed and ratified the International Covenant on Civil and Political Rights which provides for several specific rights such as: no one shall be subjected to arbitrary or unlawful interference with privacy or correspondence, and everyone has the right to the protection of the law against such interference or attacks. This is in addition to the obligation to safeguard the freedom of opinion, speech and expression. Any intrusion into such rights without procedural safeguards may fall short of India's international obligations in this regard.

Lastly, the global best practices in intermediary guidelines are usually structured along the lines of the Manila Principles, which provide for several core principles that the Draft Amendment violates. The principles are as follows:

- (a) Intermediaries should be shielded from liability for third-party content
- (b) Content must not be required to be restricted without an order by a judicial authority
- (c) Requests for restrictions of content must be clear, be unambiguous, and follow due process
- (d) Laws and content restriction orders and practices must comply with the tests of necessity and proportionality
- (e) Laws and content restriction policies and practices must respect due process
- (f) Transparency and accountability must be built into laws and content restriction policies and practices.

It is clear that several of the obligations under the Draft Amendment fall short of these principles, such as arbitrary restriction of content, no requirement of clarity or due process in content restriction orders, no compliance with necessity and proportionality standards in any of the amended sub-rules, and inadequate focus on transparency and accountability. Thus, if the Draft Amendment were to come into effect, it would put India's legal regime significantly out of step with global best practices.

The Draft Amendment Goes Against Statutory Provisions

The cardinal principle governing rule-making powers in India is that the delegated legislation cannot exceed the scope of the enabling parent legislation. Section 79 of the IT Act, which is the parent provision in this regard, is very clearly designed as an *exemption* clause – and it is expected that the rules notified thereunder would contain obligations falling within the scope of an exemption clause. However, requirements such as proactive monitoring of content, blocking orders and India incorporation requirements entirely defeat the objective of providing exemptions, as they specifically impose onerous obligations on intermediaries. Blocking orders are in fact specifically provided for under Section 69A of the IT Act. Incorporation clauses are not related to exemptions in any way. Proactive monitoring of content has been struck down by the Supreme Court in *Shreya Singhal versus Union of India*. Thus, all of these obligations are *prima facie* outside the scope of what is legally contemplated and permitted as part of the rule-making powers under Section 79 of the IT Act.

Conclusion

In the context of the reasons provided above, we believe that any law which is likely to critically hamper the Indian internet experience should be preceded by a wide stakeholder consultation including a reasoned basis for each proposed amendment. In this regard, we would be happy to assist the government in its endeavor to modernize the legal regime applicable to the digital economy.

1. **Draft Rule 3(5)** of the Guidelines contemplates that intermediaries shall enable tracing of originators of information on platforms as may be required by government agencies who are legally authorised.

By requiring intermediaries to trace originators of information, there is an implicit expectation for users of platforms to be known, and for data on these users to be collected. It is submitted that this draft rule is **technically infeasible** in case of some intermediaries like Signal, Telegram, banking applications and other end-to-end encrypted platforms that do not collect or retain metadata required for the purposes of traceability. Further, even in the case of platforms that do collect metadata, the draft rule implies that encryption will need to be weakened through ‘back-doors’ in order to understand the payload of user communication. The draft rule further implies a general monitoring obligation, which can lead to **unwarranted censorship**. All of these implicit requirements translate to a **significant dilution of privacy, freedom of expression and security of users online**. The language of the draft rule only exacerbates these concerns - it does not shed light on what constitutes a “legally authorised government agency”, nor does it lay out the circumstances, checks, or balances under which the requirement of traceability may arise.

ARTICLE 19 submits that this draft rule is violative of the fundamental right to privacy (including informational privacy) recognised by the nine-judge Constitutional bench in *Justice K.S. Puttaswamy v. Union of India* (2017)¹ and the right to privacy under international law. The bench in *Puttaswamy* laid down the test for “**proportionality and legitimacy**”² that any interference with the right to privacy must meet, which the draft rule does not satisfy. We further submit that Draft Rule 3(5) does not meet the requirements under the International Principles on the Applications of Human Rights to Communications Surveillance³ (“**Necessary and Proportionate Principles**”) which was cited by Justice R.F. Nariman in *Puttaswamy*. We also note that this draft rule is in direct tension with the principle of **data minimisation** which has been recognised and implemented by the Srikrishna Committee on data protection.⁴

Anonymity and encryption are fundamental concepts in the protection of freedom of expression and the right to privacy.⁵ In May 2015, the UN Special Rapporteur on the promotion

¹ Justice K. S. Puttaswamy (Retd) & Another v. Union of India & Ors (2017), Writ Petition (Civil) 494 of 2012.

² Concurring opinion of Justice Sanjay Kishan Kaul, Paragraph 71, Page 37, *ibid*.

³ International Principles on the Application of Human Rights to Communications Surveillance, <https://necessaryandproportionate.org/principles>.

⁴ A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Page 52 - 27, available from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf. Also see the Personal Data Protection Bill, Sections 5 & 6, available from http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

⁵ ARTICLE 19, Right to Online Anonymity, June 2015. Available from https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_f inal-web.pdf.

and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) released a report⁶ on online anonymity and encryption, which made clear that **attempts by governments to gain backdoor access to people's communications or intentionally weaken encryption standards are a violation of international law**. In light of these observations, we urge reconsideration of this rule.

2. **Draft rule 3(7)** of the Guidelines requires an intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India to be incorporated as a company in India with a permanent registered office, and appoint a nodal person of contact for coordination with law enforcement agencies.

ARTICLE 19 submits that this draft rule imposes obligations on intermediaries in a manner that may **disproportionately and significantly affect small and medium enterprises**. The threshold of fifty lakh users is not significant given the nature of the information flows on internet, and the requirement of setting up physical offices in India, hiring a full time employee for coordination with law enforcement is **thoroughly impractical** for most intermediaries. These onerous compliance costs would mean that information from small and medium enterprises would not be accessible in India. Further, the draft rule does not lay down the grounds on which the government can notify intermediaries, or on what parameters, making the obligation on intermediaries **uncertain and vague**.

This is legally significant for two reasons. First, it violates the **right to receive information under Article 19(1)(a) of the Indian Constitution** by precluding internet users in India from accessing information from around the world. It also violates freedom of expression and information as contemplated under **international human rights law**, which recognises that the freedom of expression includes the freedom to “*seek, receive and impart information and ideas of all kinds*”.⁷ Second, it has implications for **competition in the market**, as it risks encouraging larger players to become gatekeepers of information on the internet. The high compliance costs of the draft rule perpetuates dominant players' position in Indian markets by making it impractical for smaller players and newer entrants to compete.

3. **Draft Rule 3(8)** requires intermediaries to take down content upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency within 24 hours. Further, the draft rule requires intermediaries to retain such data for a minimum of 180 days, or for any such longer period as may be required by a court or by government agencies.

The grounds on which content can be considered unlawful are found, for the purposes of this draft rule only, in Article 19(2) of the Indian Constitution. Some of the grounds listed are

⁶ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, 29 May 2015, Available from <https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx>.

⁷ Article 19 of the International Covenant on Civil and Political Rights. Available from <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

extremely vague and could be interpreted to include even legitimate speech. Some of these grounds include, “*in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality..*”. The term “**appropriate government**” **also does not find definition in the draft rules**, further broadening the scope of this draft rule.

Further, draft rule 3(8) contemplates a **data retention requirement** of a minimum of 180 days, or “*for such longer period as may be required by the court or by government agencies who are lawfully authorised.*” Specificity in periods for data retention, is a fundamental aspect of progressive data protection practices, as it imbibes the **principles of collection limitation, data minimisation, and purpose limitation.** All three principles have been recognised and adopted by the Srikrishna Committee of Experts on data protection in India and to this extent, this draft rule is in **direct conflict with the Personal Data Protection Bill, 2018.**

4. **Draft Rule 3(9)** requires intermediaries to deploy technology based automated tools for proactively identifying and removing or disabling public access to unlawful content.

ARTICLE 19 notes that this draft rule embeds the assumption that automated content moderation is part of the answer to problems like disinformation, hate speech, election manipulation and terrorist propaganda. We believe the draft rule’s approach to proactively identify, remove or disable access to content using automated tools can have **dangerous unintended consequences taking into account technical limitations of automated systems, and additionally has the proclivity to violate fundamental rights under the Indian Constitution and international human rights law.**

The draft rule does not define what is meant by “unlawful information and content”, making the scope of this rule **vague and open to arbitrary interpretation.** The standard to which these automated tools are expected to adhere to are nebulous at best, which **incentivises intermediaries to err on the side of caution** to avoid liability, thus resulting in over-censorship and restriction on legitimate speech. This is particularly worrying as the **draft rule does not stipulate an appeal mechanism** for users whose content has been taken down, nor does it contemplate the importance of **accountability, transparency, or scrutability** of these systems. Instead, it imposes a blanket obligation on intermediaries to deploy these tools.

In *Shreya Singhal v. Union of India* (2015),⁸ the Supreme Court reaffirmed India’s tradition of free speech in the technological age, and emphasized the limits of **reasonable restrictions** that can be used to limit free speech under the Indian Constitution. This is in line with international human rights law⁹ with contemplates freedom of expression as a human right with **narrowly tailored restrictions** that must (i) be provided by law, (ii) in pursuit of a legitimate aim, and (iii) be necessary and proportionate to the aim pursued. **The intended use of automated tools under this draft rule does not satisfy these tests.**

⁸ *Shreya Singhal v. Union of India*, Writ Petition (Criminal) No. 167 of 2012.

⁹ Article 19, Paragraph 3 of the International Covenant on Civil and Political Rights. For a detailed explanation and interpretation, see General Comment No 34, CCPR/C/GC/3, para. 21, 22.

Specifically on the question of intermediaries, in *Shreya Singhal*, the Supreme Court held that private companies could not be tasked with ascertaining the legality of content themselves, and should rely on a court order or notification by the appropriate government to have ‘actual knowledge’ of unlawful content, “for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.” **This draft rule, by requiring private intermediaries to proactively identify, remove or disable public access to unlawful content, is thus, in direct conflict with the precedent laid down by the Supreme Court in *Shreya Singhal*.**

Further, the definitions of hate speech, disinformation, terrorist propaganda are extremely subjective and complicated even for the human eye. The assumption that automated tools have the ability to moderate content efficiently and accurately is deeply flawed. **Even the most sophisticated machine learning systems today are not equipped to understand context and nuance in speech**, social intricacies, let alone complicated constructs like hate speech and fake news. While machine learning systems can carry out rudimentary sentiment analysis, the ability of these systems to understand key aspects of speech – tone, context, sarcasm and irony – is extremely limited at present.¹⁰

Finally, and most importantly, the draft rule assumes that automated tools are the appropriate mechanism to proactively monitor content and tackle problems like hate speech and election manipulation. **This trust in automated systems should be demonstrated and earned, but the growing global tendency has been instead to assume their appropriateness, which this draft rule does.** Even once these systems reach greater levels of sophistication in re: context and nuance, ongoing research in the field indicates that automated tools embed and potentially exacerbate existing biases, that these systems rely on models which perform in opaque and unfair ways, with the tendency to disadvantage vulnerable communities.¹¹ These tools are far from being neutral, and in fact encode societal discrimination and unfairness into inscrutable systems.¹² As we have shown through previous research,¹³ this has **significant implications in jurisdictions like India**, and thus, we would urge MEITY to tread with extreme caution in this regard, and to reconsider this rule entirely.

¹⁰ ARTICLE 19, Facebook Congressional testimony: Why “AI tools” are not the panacea, April 2018. Available from

<https://www.article19.org/resources/facebook-congressional-testimony-ai-tools-not-panacea/>.

¹¹ Safiyah Umoja Noble, *Algorithms of Oppression: How search engines reinforce racism*, 2018. New York University Press, New York.

¹² Virginia Eubanks, *Automating Inequality: How high tech tools profile, police, and punish the poor*, Page 190, January 2018. St. Martin’s Press, New York.

¹³ Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making*, October 2018. 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240384.



MIT/79/051

BSA Submission
on
Draft Information Technology
[Intermediary Guidelines (Amendment) Rules] 2018

January 31, 2019

Dear Sir,

Subject: BSA Submission on Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

BSA | The Software Alliance (“BSA”)¹ welcomes the opportunity to provide its views on the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 (**Draft Guidelines**) released by the Ministry of Electronics and Information Technology (**MeitY**).² BSA recognizes that online content platforms have important responsibilities to aid in the fight against unlawful content online by removing such content in a timely manner. However, we are concerned that the Draft Guidelines adopts a “one-size-fits-all” approach which disregards key technical distinctions between the range of service providers that fall within the IT Act’s definition of “intermediary”. As a result, the Draft Guidelines may unintentionally impose obligations that are technically infeasible for many enterprise cloud services.

In this context, we respectfully submit that not all online service providers are alike, and that it would undermine the objectives of the Draft Guidelines to ignore the technical characteristics

¹ BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world’s most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA’s members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday..

² *The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 – Draft* available at:http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

that distinguish online content platforms that are the rightful focus of this inquiry. An Intermediary Guidelines framework with overbroad applicability and no distinction between online content platforms and enterprise cloud services represents a horizontal approach that risks negatively impacting the growing Indian enterprise cloud economy. Consequently, we encourage MeitY to consider a risk-based approach that is focused on the specific subset of online intermediaries that both make available content to the general public and have the technical capabilities necessary to block the dissemination of unlawful content.

More specifically, and in relation to the provisions of the Draft Guidelines, we would like to bring to your attention the following issue-specific points:

1. Overbroad Definition of Intermediaries

Pursuant to the definition of “intermediary” in the IT Act, the Draft Guidelines will apply to any entity “who on behalf of another person receives, stores or transmits” or “provides any service” with respect to an online communication. This broad definition would seemingly extend to virtually every online entity, from the infrastructure level (e.g., Internet Service Providers, Domain Name System providers, and Infrastructure-as-a-Service providers) to the application level (e.g., social media platforms, video sharing sites, and search engines). The Draft Guidelines makes no distinction between these different types of service providers or their role in the Internet ecosystem. In its current form, the regulation would apply uniformly to all intermediaries irrespective of their technical capabilities. To ensure that the proposed Draft Guidelines create an effective set of rules that are necessary, proportionate, and fully respect civil rights, we suggest that the scope of the Draft Guidelines should generally exclude providers of enterprise cloud services.

Many of the Draft Guidelines’ obligations are predicated on the assumption that all intermediaries make content directly available to the public and that they can unilaterally intervene to identify and remove unlawful content. For instance, the proposed amendments are aimed at addressing the spread of unlawful content by requiring intermediaries to: (1) assist law enforcement personnel in the identification of the particular users who posted such content [Rule 3(5)], (2) remove such content in response to a court order or Government request [Rule 3(8)], and (3) prevent the posting of such content through the use of automated filtering tools [Rule 3(9)]. As a practical matter, however, enterprise cloud service providers will be unable to comply with these requirements. For instance, cloud Infrastructure-as-a-Service providers offer computing power and database storage upon which their enterprise customers can build and run their own public-facing Internet services. Because such enterprise cloud service providers do not have unfettered access to the data stored by their enterprise customers, a cloud infrastructure provider would be unable to comply with a request to remove specific unlawful content. Consequently, if an enterprise cloud service provider received an order requiring it to remove unlawful content from one of its enterprise customers, the service provider would have no other option than to shut down the entire service of the customer. An enterprise cloud service provider would likewise lack access to the log information that would be needed to identify an individual who posted content on an enterprise customers’ public-facing Internet service.

2. Filtering Obligations Undermine Constitutional Protections

In *Shreya Singhal v Union of India*, the Supreme Court concluded that legislation that restricts the constitutional right to free expression must both be necessary to achieve a legitimate state interest and narrowly tailored to avoid unnecessarily chilling legitimate speech.³ The requirement for all intermediaries to implement automated filtering tools “for proactively identifying and removing or disabling public access to unlawful information or content” is inconsistent with these core constitutional principles. By conditioning the availability of the IT Act’s safe harbor for online intermediaries on their implementation of automated filters to preemptively block any potentially “unlawful information or content”, the Draft Guidelines would create perverse incentives that would result in the systematic over-blocking of lawful content.

In addition to undermining Indian users’ free speech interests, the automated filtering requirement will create significant privacy and data protection concerns as laid down by the Supreme Court in *K. Puttaswamy v. Union of India*.⁴ Filtering the content stored and/or processed by intermediaries would potentially require them to go against contractual privacy commitments and oblige them to filter, for example, the personal, corporate, medical, or financial data of millions of persons, businesses, or governments. Accordingly, in order to ensure privacy and data protection for their customers, we urge MeitY to eliminate the proposed filtering requirement from the Draft Guidelines.

Recommendations

For the reasons set out above, we urge MeitY to specifically exclude enterprise cloud service providers from the scope of the Draft Guidelines’ new obligations. Furthermore, we request you to eliminate the filtering obligations imposed on businesses in Rules 3(9).

Yours sincerely



Venkatesh Krishnamoorthy

Country Manager

BSA | The Software Alliance

³ W.P. (Criminal) No. 167 of 2012

⁴ W.P. (Civil) No. 494 of 2012

MIT/79/052

From : Harsheet Yogesh Shaah

(Cyber Expert and Researcher Contributor For Smart Cities at NIUA)

Email : harsheet@inbox.lv Mobile Number : +91-9220785999

NEW DELHI BRANCH :

RZF-906/23-F-08, SUBHASH MARG, RAJ NAGAR -2,

DWARKA, SOUTH WEST DELHI. NEW DELHI. INDIA

PIN CODE NO. 110077

To,

Shri P Kumar

CYBER LAW & E - SECURITY DEPARTMENT,

The Ministry of Electronics and Information Technology,

GOVERNMENT OF INDIA.

SANCHAR BHAWAN

NEW DELHI . INDIA

SUBJECT : SUGGESTION FOR DRAFT ON THE INFORMATION TECHNOLOGY [INTERMEDIARIES GUIDELINES (AMENDMENT) RULES] 2018

Intermediaries, the companies providing the Internet's infrastructure and platforms, often care about cybersecurity, but in selective ways driven by their incentives. Research can uncover these incentives and public policy can correct the biases that emanate from them.

Online privacy will be much harder to solve than cybersecurity. There is no clear antagonist and the term means many things. Furthermore, in the context of online tracking, users, intermediaries, and different government agencies have conflicting incentives.

In recent years, the role of Internet intermediaries in cybersecurity has received special attention from researchers. Intermediaries are organizations that provide the Internet's basic infrastructure and platforms, and enable communications and transactions between third parties and services.

Examples include broadband providers, payment systems, search engines, and other services provided by firms such as Apple, Amazon, Facebook, Google, or Microsoft. In the absence of a central authority, these companies decide on technical standards and enforce procedures, making them de-facto rule makers (Van Eeten and Mueller 2012; Hall and Biersteker 2002). Their influence is felt in many Internet operations.

Intermediaries can play a positive role to improve cybersecurity, at least in theory. Their centrality means they see much of what goes on in the network, and they have direct access to users. They are often resourceful and technically apt, and their scale makes them easier to engage by policymakers. In practice, however, their incentives concerning cybersecurity are mixed. They often see cybersecurity as a necessity to maintain user trust. They also see it as costly. Many times, they voluntarily take steps to protect their customers from attacks. But there are also times that they avoid action, or do things that impose costs on other actors or on society at large.

One of the most promising areas of security economics research has concentrated on Internet intermediaries. These entities provide the Internet's basic infrastructure and platforms, and enable communications and transactions between third parties and services. Players include Internet Service Providers (ISPs), hosting providers, payment systems, e-commerce platforms, search engines and participative platforms. The role of intermediaries has increased over the years gradually modifying the original vision of an 'end-to-end' design of the Internet. Most intermediaries are private businesses and IT forms the core of their business. We will first make some general observations applying to all intermediaries, and then look at different types separately.

Intermediary markets are highly concentrated because of network effects and economics of scale. Network effects, as previously explained, reflect the increasing value of a service as more users adopt it. Economies of scale are cost advantages that firms gain due to their size. In many markets—for instance search engines, participative platforms or certificate authorities, a handful of companies control large market shares, sometimes up to eighty or ninety percent of the revenues or user base (Noam 2009). Some of the largest Internet intermediaries are among the world's top firms and well-known brands—e.g. Google, Facebook, eBay, Amazon, Apple and Microsoft.

Intermediaries raise interesting governance issues. They are in some sense gatekeepers of the Internet economy with direct access to end users. They become de-facto standardization bodies and their mundane technical choices frequently have more profound effects on outcomes than formal Internet governance structures (Van Eeten and Mueller 2012). Their scale makes them focal points for regulation, whereas a network of thousands of organizations and millions of end users can hardly be regulated by traditional governance arrangements.

However, like in the case of other players, the security incentives of Internet intermediaries are mixed. In some cases, security is a cost to avoid, in particular if it conflicts with business interests. In many cases however, intermediaries take security seriously and are among the largest defenders of users against attacks, as they have incentives in maintaining trust in the Internet economy. Often, their role as multi-sided platforms which are enabling other market players will generate strong incentives to internalize some of the externalities in the system. Moreover, many intermediaries have the resources, knowledge, and capabilities to provide security.

Internet service providers (ISPs) are companies that connect subscribers to the global Internet. ISPs come in different sizes—from small regional ISPs to multinational tier-1 networks. There are several thousand ISPs worldwide but the 200 largest ones serve about 80 percent of broadband and mobile Internet markets (Van Eeten et al. 2010). Since ISPs have access to their subscribers' Internet traffic they are affected by and involved in policy debates on privacy protection, network neutrality, copyright enforcement, infrastructure resilience, the blocking of malware, and the disruption of botnets.⁴ In many countries, ISPs have historically been regulated in a less intrusive fashion than traditional telecommunications companies.

In the U.S. they were historically classified as ‘information service providers’ and in other countries as value-added service providers. As part of these legal arrangements, they were shielded from liability for traffic carried on their networks as long as they followed certain required business practices.

Hosting providers are organizations that operate servers used by customers to make content and services available to the Internet. Many hosting providers are also registrars: entities that sell and register domain names. As with virtually all services on the Internet, these businesses are abused by criminals. Phishing sites, command-and-control servers for botnets, and the distribution of child pornography, malware and spam all require such services. Like ISPs, hosting providers can thus play a key role in fighting cybercrime.

Much of the criminal activity runs on compromised servers of legitimate customers but some run on servers rented by the criminals themselves. In either case, the hosting provider typically becomes aware of the problem only after being notified of the abuse. Responses to abuse reports vary widely, ranging from vigilant to slow to negligent (Canali, Balzarotti, and Francillon 2013; Stone-Gross, Kruegel, et al. 2009; Bradbury 2014). In a small number of cases, the hosting provider passively or actively facilitates the criminal enterprise and shields it from takedown attempts—a practice referred to as ‘bulletproof hosting’.

Payment and other financial service providers (FSPs) are no strangers to attacks. Annual global losses from financial fraud amount to billions of dollars (R. Anderson et al. 2013). At the same time, these intermediaries have benefited tremendously from the growth of online payments, and in relative terms, fraud has been stable or diminishing (Financial Fraud Action UK 2015). This is because they have become good at detecting fraud while maintaining convenience, for instance by profiling credit card transactions in real time in their back-end systems, rather than imposing additional security measures on the users directly. One advantage they have is that calculating the monetary gains and losses of certain trade-offs is easier for them than for other sectors. For example, after a data breach credit card issuers can calculate the relative cost of replacing cards or refunding victims of fraudulent cases (Graves, Acquisti, and Christin 2014). The FSPs have also been helped – perhaps paradoxically - by legal regimes in the U.S. and some European countries that limited the liability of consumers in cases of fraud. The burden of proof for fraud was put on the FSPs who actually had the capability to do something about it (Van Eeten and Bauer 2008). In short, financial service providers are in a position to internalize some of the externalities in the sector and thus absorb and mitigate the sector-wide costs of fraud.

Related to payment providers and ecommerce platforms are certificate authorities (CAs) organizations that issue digital certificates. Such credentials are intended to enable secure online communications, assuring confidentiality and integrity of information and transactions. A series of high profile breaches at CAs in recent years, most notably the breach and bankruptcy of DigiNotar in 2011 brought to light serious weaknesses in the current system (Arnbak and Van Eijk 2012). Vratonjic et al. (2013) looked at how TLS/SSL certificates are deployed on the top one million websites and found many misconfigurations. Durumeric et al. (2013) gathered all digital certificates in use in the public web and found hundreds of CAs with the authority to issue certificates that are recognized by browsers. If any of these CAs were to be breached, certificates can be maliciously issued for any other website, a serious negative externality. Arnbak et al. (2014) used the same data to calculate the market shares of CAs and connect them with their prices. Surprisingly, they found the market share of the most expensive CAs was much larger than cheaper CAs for identical certificates.

Search engines, portals, and participative platforms are used to find content and connect to others. While these intermediaries have explored many different business models in the last decades, the market has converged on a business model in which users receive services for free while revenues are generated from targeted advertising. This development is driven by a combination of network effects and the 'economics of attention': in a world abundant with information, the scarcest resource is the attention of users (Shapiro and Varian 1998). These platforms fight for user attention (Davenport and Beck 2001). Since the marginal cost of information is close to zero, offering services at a low price or free is an economically rational strategy as it maximizes the size of the potential audience. Key players combine 'free' with a variety of nudging techniques to keep users on the platform (an interesting glimpse into this is the controversial study by Kramer et al. (2014) on changing the emotional content of Facebook news feeds to see how it effects users).

Creating a revenue stream via advertisement is, of course, not new: broadcasting and newspapers have used the model for decades. The key difference is that targeted advertising can extract higher value (Goldfarb and Tucker 2011).

In terms of cybersecurity, these platforms overall seem to internalize costs to keep their users satisfied. Just to illustrate, Google has a team dedicated to protect users against state-sponsored attacks (Grosse 2012). This is not done out of nicety but as a competitive necessity: Myspace lost to Facebook partially as a result of increased spam and abuse on its network (Dredge 2015).

Another example is handling 'click fraud'. When a bot imitates a legitimate user clicking an ad to generate revenue, the advertisers and the platforms are harmed financially and by the erosion of confidence. Chen et al. (2012) suggest that platforms will likely pay the costs of click fraud investigations thus internalizing some of the costs to the system at large. Schneier (2012) draws an analogy with 'feudal security' in the past: platforms provide users with security in exchange for allegiance. This approach has some benefits but it also comes with serious risks particularly with regard to privacy. Evidence of this tension is visible in how the platforms balance the interests of users and advertisers: Facebook Connect is preferred by many websites as a federated identity and password system over alternatives because of the user details it shares.

In the end, focusing on incentives rather than the technology helps understand trade-offs and develop sound cybersecurity policy. Given the dynamic nature of cybersecurity, all the issues discussed in this chapter are the subjects of ongoing research. Among emerging topics are security on mobile communications platforms, in the cloud, in the Internet of Things (IoT) and the industrial Internet, user behaviour and education across life stages, the establishment of better national and international governance frameworks for security, and the development of better and more reliable metrics.

Thanking You !

Regards,

HARSHEET YOGESH SHAAH

Dated : 31st January 2019, Thursday

SHAK SAMVANT 1940



MIT/79/053

To,
Shri Ajay Prakash Sawhney
Secretary
Ministry of Electronics and Information Technology
secretary@meity.gov.in

CC: Cyber Laws & E-Security Division
Ministry of Electronics and Information Technology
gccyberlaw@meity.gov.in; pkumar@meity.gov.in; dhawal@gov.in

Jan. 30, 2019

Dear sir,

Re: "Comments / suggestions invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018"

About IFF

We are a civil liberties advocacy organisation focusing on technology and fundamental rights. Working across the spectrum -- with expertise in free speech, digital surveillance and privacy, net neutrality and innovation -- we champion human freedom in the digital space. Our aim is to ensure that people in the world's largest democracy are able to use technology with liberty and justice guaranteed under the Constitution of India.

We work across a wide spectrum, with expertise in free speech, digital surveillance and privacy, net neutrality and innovation to champion freedom in the digital age. With grassroots membership, we build campaigns on public policy issues such as, "SaveTheInternet" (for Net Neutrality); "SpeechBill" (to reform Defamation Law); "KeepUsOnline" (against Internet Shutdowns); "SaveOurPrivacy" (for a Data Protection Law); "RightToMeme" (against online censorship). We are also litigants in the Supreme Court and the High Court of Delhi on issues of privacy and free expression.

Private meetings preceded public consultation

We value institutional outcomes and frequently participate in public consultative exercises. To us they greatly help further transparency and accountability in rule making. While we congratulate the ministry for the present consultation, we also note with concern a curious sequence of events which has impacted public confidence in its outcome. On December 24, 2018 the Indian Express reported on its front page a private meeting was conducted between Ministry Officials and a few social media companies and industry associations on December 21, 2018.¹ In this meeting a Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018" was furnished to the chosen attendees and they were asked to respond to it.

In the interests of transparency we publicly revealed the rules provided in the meeting noting the harm that will be caused due to them.² These same rules, with the exact same

¹ <https://is.gd/ExpressITRulesStory>

² <https://is.gd/IFFITRulesPost>



changes, matching word for word, after publication of the Indian Express report are now being put to public consultation. Such private meetings seeking prior feedback from large, private social media companies undermines confidence in the consultation exercise. It deprioritized ordinary Indians who use the internet as the primary stakeholders in a exercise to change legal rules which would impact their fundamental rights.

Absence of any clear rationale for proposed changes

We find this to be peculiar and urge that the present consultation exercise be recalled. We instead propose that a fresh consultation be commenced with a white paper exercise on user generated content (UGC) that promotes a more rigorous understanding of individual liberties, respect for user rights and the interaction of social media and technology with our democratic framework. This includes the future of the Information Technology Act, 2000 but also examining frameworks of data protection, consumer and competition law. It is a matter of concern that the proposed changes in legal form have been proposed without explaining the rationale and true authority behind them. For instance the proposal for the insertion of Electronic Nicotine Delivery Systems (ENDS) in the list of content that internet intermediaries should prohibit lacks any credible reasoning.

Overall, the present exercise seemingly refers to the speech of the Hon'ble Minister for Electronics and IT, Shri Ravi Shankar Prasad made to a calling to attention motion in the monsoon session of Parliament, on July 27, 2018 on the floor the Rajya Sabha.³ During the course of the discussion various issues as such the impact of the internet on furthering ordinary Indians. These issues include concerns by Hon'ble Members of Parliament regarding: (1) fundamental right to speech and expression; (2) the impact on users' privacy and data protection frameworks; (3) impact of social media on the health of our democracy; (4) concerns of law and order; (5) misinformation campaigns especially as used and implemented or supported by the IT Cells of Political Parties; (6) mob lynchings; (7) data breaches. We should avoid conflation on these issues which deserve to be dealt with thorough examination and detailed rigour.

To meaningfully address these challenges solely tinkering with the intermediary liability provisions, that too by changes proposed through a rule making power, is disturbing. It will not solve these problems since it does not address these issues. On the contrary it will certainly create gravely threaten the fundamental rights of ordinary indians who use the internet. To arrive at balanced and rational outcomes we require a meaningful policy debate rather than hurling towards these proposed changes.

Amendments to rules violate fundamental rights and are ultra-vires parent provision

We submit that the proposed changes are unconstitutional. The proposed changes are in imprecise legal language, that is vague and goes beyond the parent statute. Even if this language in the draft rules is made more specific, we believe that the proposals themselves are disturbing in how they would allow for an authoritarian style of restriction on the privacy and free expression rights of Indians. Particularly they would undermine the spirit and intent of the Supreme Court's judgement in *Shreya Singhal v. Union of India*. We note with concern the continuing use of the unconstitutional Section

³ http://164.100.47.5/official_debate_hindi/Floor/246/F26.07.2018.pdf



66A, and caution against further undermining this historic decision by carrying out the proposed changes.

These proposed changes are susceptible to legal challenge for violating the fundamental rights of Indians including, the right to privacy, free speech, equality and due process. All these problems are explained in detail in our accompanying submissions. We acknowledge the concerns for the need to review our laws however we advise caution against the dilution of intermediary liability exemption. By concentrating on this, the present approach of the Ministry will be inadequate to address the larger challenges confronting government agencies and will only gravely injure our fundamental rights online.

Government must publish white paper on policing challenges concerning content

Towards this, we urge that the present consultation is recalled. Instead MEITY should consider organising a broader exercise commencing with a white paper on the challenges posed by user generated content (UGC) online.

Such an exercise will assist in the identification of benefits and harms -- most importantly the impact on fundamental rights -- and would be a rational approach that would benefit crores of Indians who rely on digital communication technologies as an indispensable part of their lives. Here, MEITY should look to operationalise the defunct CRAC (Cyber Regulations Advisory Committee) which has been statutorily tasked under the Information Technology Act, 2000 to provide the function of guidance as technology and its use evolves with time. We impress that this body must have sizeable membership from experts, academics, technologists and civil society organisations.

This has to include a comprehensive look at the policy frameworks, legal architecture and efforts to improve law enforcement resources and coordination across our federal nation. It has to commence with requiring the public disclosure of the standards, practices and systems in place put by large online platforms to enable us to understand how best to deal with harms and even advancing our fundamental rights. Such an exercise has to reconcile the widespread blocking and over-censorship which is resulting due to overbroad claims of intellectual property infringement.

IFF remains committed to protecting the rights of all Indians and our Constitution and stand ready to serve government offices and institutions in addressing that shared mission. We value the opportunity for any further requests for information, inputs or clarifications and remain available for meetings.

Kind regards,

Apar Gupta,
Executive Director
Internet Freedom Foundation



Detailed Submissions on the Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

Outline of the present submission

The present submissions detail our principal submission that the proposed changes to the Intermediary Rules are unconstitutional. We have in our covering letter dated Jan. 31, 2019 set out the rationale for recalling the present consultation.

We are concerned that the ruling of the Hon’ble Supreme Court in *Shreya Singhal v. Union of India* is not being complied with. This includes continuing prosecutions under Section 66A of the Information Technology Act, where based of our study¹ in a petition by the People’s Union for Civil Liberties the Hon’ble Supreme Court of India has issued notice.² It would be unfortunate if further non-compliance is invited as sought by the proposed changes which would violate it in spirit and letter by undermining the protections crafted by the court by reading down Section 79 of the Information Technology Act.

We propose that the challenges posed by user-generated content on online platforms commence from a whitepaper to study the harms to our fundamental rights. This will require a factual, requiring a full public disclosure by large social media companies of their censorship practices, policies and enforcement.

The present submissions are broken into four principal sections. The first deals with the history of intermediary liability protections given that there is an absence of understanding on their nature and scope. It also includes the policy arguments which have flown into its legal design. The second section looks at the prevailing international standards and the global movement on safeguarding intermediary liability. The third provides specific inputs on each proposed change and the harm which will be caused by them.

1. Background of intermediary liability protection

1.1. The Information Technology Act, 2000 was formed to provide legal recognition to electronic transactions, popularly referred to as “Electronic Commerce”³ based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL).⁴ Section 79 of the IT Act, as it originally stood in the year 2000, provided for a limited exemption from liability to any “network service provider” (defined as an “intermediary”) for any third party information or data made available if the intermediary proves that the offence or

¹ Sekhri, Abhinav and Gupta, Apar, *Section 66A and Other Legal Zombies* (October 31, 2018). IFF Working Paper No. 2/2018. Available at SSRN: <https://ssrn.com/abstract=3275893> or <http://dx.doi.org/10.2139/ssrn.3275893>

² Internet Freedom Foundation, *Supreme Court issues notice to check any 66A Cases #RightToMeme #Section66A* (07 January 2019). Available at SSRN: <https://is.gd/sRIANQ>

³ The Information Technology Act, 2000.

⁴ G.A. Res. 51/162, Model Law on Electronic Commerce, U.N. Doc. A/RES/51/162 (Jan. 30, 1997).



contravention was committed without knowledge or that it had exercised all due diligence to prevent the commission of such offence or contravention.

- 1.2. In the year 2004, the Chief Executive Officer of Baazee.com (an e-commerce portal), Mr. Avnish Bajaj, was arrested for the offer of sale of an obscene video clip made on the company's website by a user of the portal.⁵ This case highlighted legal risks to which intermediaries were exposed to prior to the amendment of the IT Act, for content generated by their users, and consequently the urgent need to provide safe harbour to intermediaries which are driven by User Generated Content (UGC). In order to address this concern and several other lacunae in the then existing legislation, an Expert Committee was formed in 2005 which submitted its report on the proposed amendments to the IT Act.⁶ One of the most significant amendments proposed to the IT Act in the Report of the Expert Committee is extracted below:

“Section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases. EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 has been used as guiding principles. Power to make rules w.r.t the functioning of the “Intermediary” including “Cyber Cafes” has been provided for under Section 87.”

- 1.3. The Expert Committee on the amendments to the IT Act stated in its Report that the principles of EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 shall be used as “guiding principles” in amending Section 79 of the IT Act.⁷ The EU Directive clearly stated that monitoring obligations of a general nature shall not be imposed in intermediaries, also noting that:

“(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.”

⁵ See Gupta, Apar, *Liability of Intermediaries in India - From Troubled Waters to Safe Harbours* (January 17, 2007). Computer and Telecommunications Law Review, Vol. 13, No. 2, p. 60, 2007. Available at SSRN: <https://ssrn.com/abstract=1682468>

⁶ Department of Information Technology, Ministry of Communications & Information Technology, Report of the Expert Committee on Proposed Amendments to Information Technology Act 2000, 46 (Aug. 2005).

⁷ Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (June 8, 2000).



Hence the very intent of the law of intermediary liability exemptions is to further international human rights standards principally, “the observance of the principle of freedom of expression”.

- 1.4. In accordance with this recommendation, the scope of the definition of “intermediary” was expanded as follows vide the Information Technology (Amendment) Act, 2008⁸:

“Intermediary” with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.”

- 1.5. Section 79 of the IT Act was amended to include sub-section (1), which exempts all “intermediaries” from liability for any third party information, data, or communication link made available or hosted by him, notwithstanding anything contained in any law for the time being in force. Section 79(1) of the IT Act exempts an intermediary from liability for any third party information, data, or communication link made available or hosted by him subject to the intermediary proving under sub-section (2) of Section 79 that:

- 1.5.1. The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
- 1.5.2. The intermediary does not initiate the transmission, select the receiver of the transmission, and select or modify the information contained in the transmission; and
- 1.5.3. The intermediary observes the standards of due diligence prescribed by the Government.

- 1.6. In exercise of the powers conferred by sub-clause (c) of sub-section (2) of Section 79 read with Section 87(2)(zg) of the Act, on April 11, 2011. These rules were studied by the Committee on Subordinate Legislation, of the 15th Lok Sabha which by its report dated March 21, 2013 *inter alia* made the following recommendations:⁹

- 1.6.1. Ambiguity in terms under Rule 3: “The Committee expect the Ministry of Communications and Information Technology to have a fresh look at the Information Technology (Intermediary Guidelines)

⁸ The Information Technology (Amendment) Act, 2008.

⁹ Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013),



Rules, 2011 and make such amendments as necessary to ensure that there is no ambiguity in any of the provisions of the said rules.”

- 1.6.2. Necessity of safeguards for takedown: “The Committee feel that there is need for clarity on the aforesaid contradictions and if need be, the position may be clarified in the rules particularly on the process for take down of content and there should be safeguards to protect against any abuse during such process.”
- 1.6.3. Disabling content under Rule 3(2): “The Information Technology (Intermediaries Guidelines, Rule 3) provides a framework for the due diligence to be observed by the Intermediaries. However, as far as the legal enforceability of these guidelines is concerned, replies of the Department of Electronics and Information Technology present a conflicting picture.”
- 1.6.4. Operationalise the Cyber Regulatory Advisory Committee (CRAC) under Section 88: “The Committee would impress upon the Ministry of Communications and Information Technology (Department of Electronics & Information Technology) to make the CRAC functional and benefit from its advice particularly in the context of having a fresh look at the rules and amendment of rules recommended in this report.”

To our knowledge, none of these recommendations have not been acted upon or even found their place within the instant proposals mooted by MIETY till date.

- 1.7. On March 24, 2015 the Hon’ble Supreme Court of India delivered a landmark judgement of *Shreya Singhal v. Union of India*¹⁰ on free expression online, with specific findings on Section 79 and the Intermediary rules. It held that:

“117. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

¹⁰ Available at <https://is.gd/ShreyaSinghalFulltext>



118. The learned Additional Solicitor General informed us that it is a common practice worldwide for intermediaries to have user agreements containing what is stated in Rule 3(2). However, Rule 3(4) needs to be read down in the same manner as Section 79(3)(b). The knowledge spoken of in the said sub-rule must only be through the medium of a court order. Subject to this, the Information Technology (Intermediaries Guidelines) Rules, 2011 are valid.”

119. Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relating to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment.”

Given the *Shreya Singhal* judgement determined not only the Intermediary Rules, 2011 but even read down Section 79 which is the parent provision giving rise to the rulemaking, strict compliance with both its letter and spirit becomes absolutely essential.

2. International standards and global trends on Intermediary Liability

- 2.1. There has been considerable work on the nature of intermediary liability protections internationally. This section in brief highlights global principles drawing from international human rights standards and the recent work of scholars working in this domain.
- 2.2. There is specific comment on the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, dated 6 May 2011 on the importance of free expression online that states in Paragraph 2 itself that, “The Special Rapporteur believes that the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies. Indeed, the recent wave of demonstrations in countries across the Middle East and North African region has shown the key role that the Internet can play in mobilizing the population to call for justice, equality, accountability and better respect for human rights. As such, facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.” This report holds a high persuasive value as it is based on the interpretation of various human rights instruments to which India is a State party. These include, the International Covenant on Civil and Political Rights which has been referred to by various Supreme Court decisions.¹¹

¹¹ See eg. *Francis Coralie Mullin vs The Administrator* (1981 AIR 746); *Vishaka v. State of Rajasthan* (1997 6 SCC 241) [both cases refer to the ICCPR and UDHR].



- 2.3. More recently this has been further noted in Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, dated 11 May 2017 has recommended that, “40. States often require the cooperation of intermediaries to enforce regulations on private networks and platforms. Internet and telecommunication service providers, for example, are required to comply with local laws and regulations as a condition of their operating licences, a legitimate requirement which becomes problematic when the local laws or their implementation are themselves inconsistent with human rights law.” More importantly the report also notes that private actors cannot meaningfully assess the legality of content and there is a need for any interference with free speech to be on the touchstones of proportionality and necessity (at Para 85).
- 2.4. In line with several international human rights texts two important frameworks have been proposed:
- 2.4.1. The Manilla Principles which present best practices guidelines for limiting intermediary liability for content and to promote freedom of expression and innovation. We urge that all six principles in this framework should form an informed basis of any informed rule making on Intermediary liability. They state that:
- “Principle 1: Intermediaries should be shielded by law from liability for third-party content.
Principle 2: Content must not be required to be restricted without an order by a judicial authority.
Principle 3: Requests for restrictions of content must be clear, be unambiguous, and follow due process.
Principle 4: Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
Principle 5: Laws and content restriction policies and practices must respect due process.
Principle 6: Transparency and accountability must be built in to laws and content restriction policies and practices.”
- 2.4.2. The Santa Clara Principles on Transparency and Accountability in Content Moderation also present a credible policy proposal how to achieve meaningful transparency and accountability from social media companies and large platforms.
- 2.5. We would also like to refer to some recent scholarship which has emerged from Daphne Keller¹², Kat Klonick¹³, Cindy Coen¹⁴ and Jack Balkin¹⁵. We would impress

¹² Keller, Daphne, *Toward a Clearer Conversation About Platform Liability* (May 7, 2018). Knight First Amendment Institute’s “Emerging Threats” essay series, 2018. Available at SSRN: <https://ssrn.com/abstract=3186867>; and Keller, Daphne, *Internet Platforms: Observations on Speech, Danger, and Money* (June 13, 2018). Hoover Institution’s Aegis Paper Series, No. 1807, 2018. Available at SSRN: <https://ssrn.com/abstract=3262936>



that these legal analysis even though arise in the particular context of Section 230 of the Communications Decency Act in the United States present, “the state of the art” thinking on how to deal with the potential harms caused by speech without undermining the interests of free expression that are furthered by intermediary liability exceptions. We will refer to specific learnings in the counter-comments period to best utilise and match them against the submissions received by MIETY.

3. Specific inputs on proposed changes

Rule	Nature of change	Injury to rights
3(2)(j)	Insertion of prohibition on grounds of public safety in the terms of use with a specific reference to vaping	(1) We firstly wish to draw attention that the review of Rule 3(2) has not been done as per the recommendations of the report of the Committee on Delegated Legislation as noted above. ¹⁶ This adds further discretion and vagueness ¹⁷ in the censorship practices of online intermediaries. (2) The insertion of the term “public safety” and the specific reference to vaping products is in conflict with the existing state of the law. There is no legal prohibition on vaping products by any central agency so far and a Ministry of Health Advisory has no, “binding force” as observed by the Hon’ble High Court of Delhi in Piush Ahluwalia v. Union of India (W.P. (C) 12163/2018) in it’s Order dated 14.11.2018.
3(4)	Inserts a monthly requirement (at the least) to inform	(1) This is a nanny requirement and change in the environment from a public platforms to a guarded school yard in which you are constantly reminded that you are

¹³Klonick, Kate, *The New Governors: The People, Rules, and Processes Governing Online Speech* (March 20, 2017). 131 Harv. L. Rev. 1598. Available at SSRN: <https://ssrn.com/abstract=2937985>

¹⁴ Cindy Cohn, *Bad Facts Make Bad Law: How Platform Censorship Has Failed So Far and How to Ensure that the Response to Neo-Nazi’s Doesn’t Make it Worse*, 2 GEO. L. TECH. REV. 432, 447-50 (2018), Available at <https://is.qd/ZtK6DY>

¹⁵ Balkin, Jack M., *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation* (September 9, 2017). UC Davis Law Review, (2018 Forthcoming); Yale Law School, Public Law Research Paper No. 615. Available at SSRN: <https://ssrn.com/abstract=3038939>

¹⁶ See gen. on delegated legislation: *Agricultural Market Committee Vs. Shalimar Chemical Works Ltd.* [(1997)5 SCC 516] *Hotel Balaji vs State of Andhra Pradesh* (AIR 1993 SC 1048); *Kerala Samsthana Chethu v. State of Kerala* ((2006) 4 SCC 327); *Hamdard Dawakhana v. Union of India* SCR 1960 (2) 671.

¹⁷ See gen. on vagueness: *Supdt Central Prison, Fatehgarh vs Ram Manohar Lohia* [cited as 1960 AIR 633]; *Kameshwar Prasad And Others vs The State Of Bihar* [cited as 1962 AIR 1166]; *S. Khushboo v Kanniammal* [(2010) 5 SCC 600].



	<p>users about the legal requirements such as the terms and conditions and privacy policy</p>	<p>under watch and you better behave yourself. It will turn the internet in India into a corporal environment which is bad for users.</p> <p>(2) Such a requirement is also a pro-active notification which by itself may not be possible by all intermediaries which do not have sign-up processes or have membership sign-ups.</p> <p>(3) Such a requirement also constitutes compelled speech and by itself may fall beyond the mandate of the parent provision being ultra-vires Section 79.</p>
3(5)	<p>Introduces the requirement of traceability which would break end to end encryption.</p>	<p>(1) Many platforms (Whatsapp, Signal, Telegram but even other platforms) retain minimal user data for electronic information exchange and also deploy end-to-end encryption to provide reliability, security and privacy to users. These are used by millions of Indians to prevent identity theft, code injection attacks. Encryption becomes more important as more of life now involves our personal data. Without thought or involving technical experts in an open consultative process, without any data protection law or surveillance reform, this is being tinkered with by introducing the requirement of, "traceability".</p> <p>(2) This has important consequences for everyday users of online services and should also be seen in the context of the MHA notification which activates a 2009 rules which hold the power to direct, "decryption". We do not have any proper parliamentary oversight or judicial check on surveillance and the latest draft rules if they go through would be a tremendous expansion in the power of the government over ordinary citizens eerily reminiscent of China's blocking and breaking of user encryption to surveil its citizens.</p> <p>(3) Implementing such traceability requirements in messages may be technically infeasible for startups and platforms due to the incredible diversity of uses which are facilitated by online services and platforms. This will build and create artificial entry barriers and high costs, and in effect lead to a high disincentive to employ standard encryption frameworks. This will put users and in turn even the communications of Indians at risk. When viewed at a macro level, this will also become a national security risk.</p> <p>(4) Such a requirement again flows outside the breadth of the parent statute, i.e. Section 79 of the Information</p>



		Technology Act, 2000.
3(5) and 3(8)	Requirement to comply within 72 hours for user data Requirement of takedown	(1) Such short timelines for compliance can only be fulfilled by large social media platforms and not the larger category of businesses which fall within the definition of intermediaries. The increase costs of compliance and the threat and risk of loss of immunity will make intermediaries over comply without any objective determination of legality of a request for user data. This will imperil a users privacy and also the innovation necessary to sustain the goals of digital India. (2) Similarly decreasing the timeline for content takedowns from 36 hours to 24 hours has a similar harmful impact on free speech. It should also be remembered that a key reason for the arrest of Avnish Bajaj as noted in the Delhi High Court judgement was the Police allegation that the Ebay portal did not react till 38 hours acting on a complaint by a person even though this fell within the period of weekend. ¹⁸ Such short timelines force undue, burdensome compliance resulting in harsh censorship by intermediaries who fear a loss to their immunity.
3(7)	“The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government”	(1) The localising criteria is poorly reasoned since it is on the basis of 50 lakh users. There is no time period for, “users”, there is no definition of, “users” as individuals and vagueness is the hallmark of this proposed rule. (2) Further there is no identifying criteria for, “list of intermediaries specifically notified by the government” and constitutes an illegal sub-delegation of power. Here rules cannot further sub-delegate powers, especially when such guidance is absent in the parent provision which is Section 79. (3) This proposal falls well outside the scope of Section 79 and further seems to approach the regulation of user generated content from the perspective of localising large platforms forgetting that Indians use many global services which do not have such deep pockets, such as Wikipedia, Stackoverflow or Github which may not be able to comply with the local entity requirements. There are many more examples of such services. (4) This would also by creating a barrier to access for

¹⁸ <https://is.gd/AvnishBajajHC>



		many global online services on the internet who would subsequently geo-block their services in India it would impact an ordinary Indians access, thereby impacting their fundamental right to receive knowledge and information. ¹⁹
3(8)	Longer indefinite retention even data	<p>(1) Increases the data retention period from 90 to 180 days and provides for further discretionary retention on the discretion of “government agencies”. The phrase, “government agencies” is not defined and the specific conditions or any outer limit for data retention at the end of the online platform is also not limited. Hence, there is no limitation on the period for data retention which conflicts with the proportionality requirement in the fundamental right to privacy.</p> <p>(2) Further, a mere letter by any government department, arguably a private platform can be required to store a users data indefinitely, without even letting this user know. It is important to remember that such retention will be even despite the user deleting the data on the servers of the intermediary.</p>
3(9)	Automated filtering and censorship requirement	<p>(1) This proposal would be sledgehammer to online free speech. Not abuse, harassment or threats, but legitimate speech by requiring online platforms to become pro-active arbiters and judges of legality (not their own terms of use which is a contract between the user and a platform).</p> <p>(2) Placing such a requirement for a platform to obtain immunity from prosecution and actively sweep its platform would result in widespread takedowns without any legal process or natural justice. This violates the reasoning of the <i>Shreya Singhal judgement</i> which noted, “it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.” It shifts the duty of the state to a private party.</p> <p>(3) What is worse? It will be done by, “<i>technology based automated tools or appropriate mechanisms</i>”. Such tools have been shown to be faulty, have coding biases and prone to overbroad censorship. Should we subject our fundamental right to free speech on the basis of a developing technology measure? AI censorship is the</p>

¹⁹ People’s Union of Civil Liberties v. Union of India (2003) 4 SCC 399.



		<p>Chinese model of censorship.</p> <p>(4) Automated filtering also is prone to bias and has been shown in studies to disproportionately impact minorities and those who do not conform to mainstream or dominant social identities. Such discrimination would be violative of our constitutional guarantees of substantive equality.</p> <p>(5) Such filtering would also omit any due process for the determination of a legal right²⁰ and would be based off the pervasive surveillance of personal data of users.</p>
--	--	--

To conclude, we restate and urge the proposed changes to the Intermediary Rules are unconstitutional and must be withdrawn. We strongly believe that there is need to walk back to the drawing board.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2013
(Published by MeitY)

²⁰ See on the right to natural justice for a determination impacting a fundamental right: *Olga Tellis & Ors vs Bombay Municipal Corporation* 1985 SCC (3) 545.

MIT/79/054

Comments on MeitY Draft of The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

by

The Bachchao Project¹

January 31, 2019

I. Preliminary

1. This submission presents comments by The Bachchao Project (“TBP”) on the draft of The Information Technology Intermediaries Guidelines (Amendment) Rules (“draft guidelines”), dated 24 December 2018, released by the Ministry of Electronics and Information Technology (“the MeitY”), Government of India.
2. TBP commends the MeitY for its efforts at seeking inputs from various stakeholders on this important and timely issue. TBP is thankful for the opportunity to put forth its views.
3. This submission is divided into three main parts. The first part, ‘Preliminary’, introduces the document; the second part, ‘About The Bachchao Project’, is an overview of the organization; and the third part, ‘Submissions on the issues’, contains our comments on the amendments proposed in the draft intermediary guidelines.

II. About The Bachchao Project

4. The Bachchao Project is a techno-feminist collective that undertakes community-centric efforts to develop and support open source technologies and technical frameworks with the goals of mitigating gender-based violence. TBP works towards securing equal rights for women, LGBTQIA+ and gender non-conforming persons. We conduct research and advocacy in all the above areas and guide communities in determining appropriate technological interventions for themselves.

III. Submissions on the issues

We understand that the MeitY seeks to replace the **Information Technology [Intermediaries Guidelines] Rules, 2011** (“current guidelines”) on account of, *inter alia*, disinformation and ensuing threats to public order and public safety, copyright infringement, and the circulation of content displaying sexual assault, sexual violence and child pornography. We appreciate that the Government of India is taking steps for curbing these and other harms and agree that social media services need to assume greater responsibility for the safety of their users in India. However, we also believe that the draft guidelines are onerous, arbitrarily constructed and deeply concerning. The guidelines do not achieve a balance between regulating harmful content and the fundamental rights of citizens such as privacy and the freedom of speech and expression. Here, we would like to make four observations:

¹ This submission has been authored by Rohini Lakshané on behalf of The Bachchao Project, India.

1. **Fighting misinformation with information:** The issue of malicious rumour-mongering with the intent of causing violence against one demographic or another has existed in India much longer than telecommunication services, the Internet or popular messaging applications such as WhatsApp. While the proliferation of the Internet has brought with it numerous advantages, it also enables disinformation to be spread faster than other modes of communication. A generally prudent approach in this regard would be for law enforcement authorities to fight misinformation with information. Across the world, government bodies, security agencies and persons who hold public office now maintain a social media presence and communicate with citizens in times of distress and emergencies. For example, the Bengaluru Police Department did a commendable job of using popular social media channels to help them control violence, arson and public unrest that immediately followed a Supreme Court verdict in September 2016².
2. **Chilling effect on legitimate speech:** The draft guidelines disproportionately put the onus of determining what content could be “unlawful” and then censoring it, overturning the existing set of checks and balances laid down by the Supreme Court in *Shreya Singhal vs Union of India* (with reference to S. 79 and Rule 3(4) of the Intermediaries Guidelines, under the Information Technology Act). Numerous studies and precedents show that intermediaries already tend to err on the side of caution and comply with takedown requests even when made by entities other than a court law. Intermediaries have also been known to over-comply with such requests and to take down more content than necessary³. A chilling effect on free speech that results from such arbitrary censorship does not augur well for the health of a democracy.
3. **Chilling effect because of the subjectivity of the term “unlawful content”:** It is unclear what would constitute “unlawful content”, “incitement to violence” or “public order” because these terms are nebulous when opened to interpretation and are not strictly defined in the law. **Pornography and hate speech are not well-defined either.**
 - a. S. 67A of the Information Technology Act, 2008 refers to “material containing sexually explicit act, etc”. The term “**obscenity**”, via which **pornography** has come to be viewed is housed in S. 292 of the Indian Penal Code 1860, which does not clearly define what constitutes an obscene act. (“...shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt person...”) Whether or not certain content may be considered pornographic is thus open to a wide variety of legal and non-legal interpretations. In such a scenario the draft guidelines are likely to aggravate the **chilling effect on the sexual expression of women and LGBTQIA+ persons** while we already live in a milieu of several sexual taboos. Open-ended exceptions for

² Bose, Adrija. “How Bengaluru City Police came on social media during the Cauvery crisis”, 2016, *Huffington Post*

https://www.huffingtonpost.in/2016/09/15/how-bengaluru-policed-helped-through-social-media-in-time-s-of-cr_a_21472497

³ Dara, Rishabh. “Intermediary Liability in India”

<http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf> (PDF), 2011, *Centre for Internet and Society*.

censoring “pornography” or “obscenity” have been known to jeopardise access to **information related to sexual and reproductive health, relief from sexual violence, abortion, women’s rights, and rights of gender diverse individuals.**

- b. It is equally tricky to determine if certain content contains **child pornography**. S. 67B of the IT Act, 2008 refers to material “depicting children engaged in sexually explicit act”. However, images of children taken out of context and images meant to be used to specific purposes also end up being used as “child pornography”.
 - c. A report by Chinmayi Arun and Nakul Nayak (2016)⁴ that discusses online hate speech and the law in India notes, *“It is clear that **hate speech law is outdated and affects a wider range of speech than is necessary. The law often fails to prevent violence resulting from incitement, and powerful speakers with the capacity to do so are able to avoid punishment. This is in part due to remedies and strategies enabled by the law, and in part because of institutional failure in the implementation of the law. The law has a detrimental impact on the freedom of expression, since it is often misused by the state or used by third parties to intimidate speakers**”*. In such a scenario, it is not a reasonable expectation that intermediaries be suited to uphold freedom of speech while also determining if certain content qualifies as “hate speech” or “incitement to violence” or a threat to public order.
4. **Privacy concerns:** Women, minors and LGBTQ+ persons are generally at higher risk of the harms resulting from violations of their privacy. The draft guidelines require intermediaries to surveil their users and retain their data without providing safeguards for their privacy. India also **lacks a separate law for information/ data privacy.**
 5. **Effects on communities and small businesses** The Bachchao Project undertakes work to empower women and LGBTQ+ persons in communities, especially those that are marginalised and/ or at risk. We also value and place an emphasis on using FLOSS (free, libre and open source software) and sources of open knowledge such as Wikipedia and its sister projects, and other avenues of open culture. The requirement of proactively finding and censoring content would be **extraordinarily burdensome and expensive for communities and private individuals who are harnessing the availability of the Internet for knowledge production, economic development or other constructive activities. The definition of the term “intermediary” in the draft guidelines is overbroad** and, unfortunately, brings these entities under its dragnet.
 6. **Mandated use on artificial intelligence and automation:** Artificial intelligence (AI), especially in the context of human interactions and language processing, is still in a relatively early stage. Such technology is also likely to be resource-intensive and expensive for entities other than large corporations and affluent individuals. In a diverse country with 448 living languages⁵ and numerous scripts and dialects, we do not support the indiscriminate use of automation, AI or machine-learning (ML) software for identifying and filtering content that could be considered unlawful. Nor we consider that the use of automation is a sound primary strategy to combat

⁴ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882238

⁵ <https://www.ethnologue.com/country/IN>

unlawful content. YouTube's use of content ID to address copyright infringement and Facebook's implementation of PhotoDNA⁶ against child pornography and non-consensual sexually explicit images are excellent examples of the use of automation for legal compliance and the safety of their respective users. However, entities with fewer resources than Google or Facebook are unlikely to have the capacity to implement similar automation without any support.

In addition to the above concerns, unintended consequences of enforcing the draft guidelines are likely to undermine ambitious efforts of the government such as the Digital India programme and the push for a cashless economy. We urge the MeitY to withdraw the draft guidelines, reconsider their basic framework and engage in public dialogue with stakeholders on the issue of intermediary liability.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

⁶ <https://www.pcmag.com/article2/0.2817.2489399.00.asp>

January 31, 2019

To:
Group Coordinator - Cyberlaw and eSecurity Group,
Ministry of Electronics and IT,
Government of India.

CC:
Joint Secretary S. Gopalakrishnan
Ministry of Electronics and IT.

Subject: Access Now comments to Ministry of Electronics and Information Technology's consultation on the draft Information Technology (Intermediary Guidelines) Rules 2018

Sir,

We write to you in connection with the draft rules on this subject which the Ministry of Electronics and Information Technology (MEITY) published in December seeking public comments. This letter contains Access Now's initial comments in response to the draft amendments to the existing Section 79 intermediary liability due diligence rules.

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 10 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT. We also have special consultative status at the United Nations.¹

Presently, officials from the Ministry have explained that the proposed draft amendments to the Section 79 rules and the present consultation come out of a Ministerial position stated in response to a debate in the Rajya Sabha that took place last year on a calling-attention motion on "Misuse of Social Media platforms and spreading of Fake News".

The role and responsibility of social media platforms is a highly contested and critical issue, which is witnessing an evolution in the current context of concerns about disinformation, online harassment, and micro-targeting of users. For some, the scale and reach of social media platforms has increased the intensity of concerns. However, at the outset, we would submit that the draft amendments to these rules are not just restricted in their impact to social media,

¹ Access Now, *About us*, <https://www.accessnow.org/about-us/>.

but also have a bearing on telecommunication service providers, internet service providers, internet cafes, other online applications such as messaging service providers, email service providers, among others. The draft rules must therefore be evaluated on their impact on the full intermediary ecosystem - essentially all the mechanisms and engines of expression that allow communications between users and publication of user generated content to take place.

Access Now submits that measures that seek to tackle concerns around targeted disinformation and online harassment should be developed based on evidence driven discussions with a wide side of stakeholders, and with a commitment to focus on protecting the fundamental rights of users with respect to their ability to express themselves and access information via the internet. We welcome the Government of India's intention to proactively work towards solving this issues, and for giving us the opportunity to provide our comments in this discussion and participate in deliberations at the Ministry. However, we believe that the current proposal to amend the intermediary due diligence guidelines does not adequately explain its rationale or explain the measures proposed to address the issue, and in fact would instead unduly harm fundamental rights - especially those of freedom of expression and privacy.

This is especially concerning given the fact that the March 2015 *Shreya Singhal* judgement of the Supreme Court of India has come to be regarded as a key global judgment on the benchmark standards for online free expression, rest for government standards, and the role of intermediaries and the government in encouraging the exercise of the right to free expression.² Further, the Puttaswamy judgement of the Supreme Court of India, reiterated the fundamental right to privacy for Indians, along with establishing the "necessity and proportionality" norms for government interference in these rights.³ We respectfully encourage the Government of India to abide by these seminal judgements and build on them to establish a truly rights respecting regime in India.

Summary of Recommendations

1. At the outset, we recommend that the Ministry restart the process of amending the intermediary rules, and include civil society, academics and the society at large in the pre-drafting process and not restrict their consultations to only a limited set of stakeholders such as other government departments or only industry.
2. The Government of India must abide by the principles laid down in the seminal judgements of *Shreya Singhal* and *Justice Puttaswamy*, and build on them to establish a truly rights respecting regime in India.

² Available at

<https://www.accessnow.org/supreme-court-of-india-issue-historic-ruling-on-free-expression-but-disappo/>

³ Available at

<https://www.accessnow.org/justice-rohinton-nariman-indian-supreme-court-9-judge-constitutional-bench-declared-hero-recognizing-privacy-fundamental-right/>

3. If looking at the specific amendments proposed, the Ministry of Electronics and IT should:
 - a. Rethink the draft rule 3(5) and bring it in consonance with the principle of necessity and proportionality, to ensure that the right to privacy in India is respected.
 - i. The number of government agencies which are empowered to seek information must be restricted in law, and the judiciary be established as the arbiter in determining the validity of requests seeking information.
 - ii. The government promote encryption, and not provide powers for breaking encryption within this framework, in order to achieve traceability of information.
 - iii. The procedure, grounds and safeguards for governmental access to information is currently established under Section 69 of the Information Technology Act and its rules thereunder. We recommend that these provisions should not be placed under the intermediary rules. We encourage the government to amend the rules under section 69 to better protect privacy and due process, and to start a consultative multistakeholder process in this regard.
 - b. Reconsider the draft rule 3(7), and at maximum, consider a simpler requirement for the appointment of a nodal officer or representative for the purpose of legal summons and process that is resident in India. Other requirements, as provided under the draft rules, of establishing a company under the Indian law, may prove to be burdensome and in particular would harm small organisations, non-profits, and academic endeavours.
 - c. Adopt and extend the benchmark set by the the Supreme Court of India while discussing “actual knowledge” under the intermediary rules. As regards draft rule 3(8), we submit that this burden of actual knowledge and government notification should only be based on judicial orders of content takedown and removal or orders issued lawfully under the Section 69A process.
 - d. Delete rule 3(9) in its entirety, as it would not help prevent the spreading of fake news, but also cause the chilling of free expression, along with establishing a regressive regime of prior censorship in India.
4. We further recommend that the Government of India work towards negotiating bilateral and plurilateral processes with governments for rights respecting channels for exchange of information for law enforcement cooperation, building on proposals for MLAT reform.

Detailed Analysis

Below we analyse the concerning parts of the proposed amendments and their impact of the rights of users in India:

1. Draft Rule 3(5):

“When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”

We submit that the draft amended rule violates the fundamental right to privacy of users in India. This rule does not provide the adequate safeguards required to ensure that the lawful access of information by government agencies under these rules, holds up to the standards of necessity and proportionality,⁴ reiterated by the Supreme Court of India is the seminal judgement of Justice K.S. Puttaswamy vs Union of India.⁵ The judgement holds that

“The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State: (i) The action must be sanctioned by law; (ii) The proposed action must be necessary in a democratic society for a legitimate aim; (iii) The extent of such interference must be proportionate to the need for such interference; (iv) There must be procedural guarantees against abuse of such interference.”

It has been propounded by the court that infringement to the right to privacy must satisfy the standard of necessity and proportionality. This standard provides the requirement of (i) a “law”, (ii) a “legitimate purpose”, (iii) the action being “necessary in a democratic society”, (iv) the interference to the fundamental right being “proportionate to the need of such interference” and (v) “procedural guarantees against abuse”.

The draft rule provides a very vague and broad action matrix of providing “information and assistance”. Evaluation of this matrix on the threshold of necessity and proportionality proves to be an unachievable task, and would be difficult for intermediaries to evaluate. It is important that the action matrix be limited, as the Supreme Court judgement in the right to privacy provides that the burden of proof of necessity and proportionality lies on the government. The same must be said about the requirement for tracing out the originator of information.

The authority to require such assistance has been laid on “any government agency”, which provides the power to a wide spectrum of government actors - and potentially broader than those actually legally authorised for specific investigatory powers under the appropriate laws. It

⁴ Available at <https://necessaryandproportionate.org/principles>

⁵ Available at

https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

is imperative that the number of government agencies authorised under such regulation be limited, and it must be shown that their purposes require such information gathering, and such purposes cannot be achieved by any other means.

The Supreme Court has further laid down that procedural guarantees must be put in place to ensure that the powers of such interference are not abused. The draft rules do not provide any such procedural safeguards, thus rendering the powers under this draft rule subject to abuse. Further, it is imperative that institutional checks and balances be put in place to prevent such abuse of powers. Thus, we submit that the judiciary and the legislature should play an active role in sanctioning and overseeing information access requests by the executive branch, and that government agencies should play the role of an applicant - thus safeguarding the rights of users, and ensuring the prevention of abuse of powers of information access by any government actor.

As David Kaye, the United Nations Special Rapporteur on the promotion and protection of the Right to Freedom of Opinion and Expression noted in May 2015, "...**encryption** and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection". Encryption provides an important tool to users to exercise their right to free expression while also safeguarding their right to privacy. Thus, there lies a higher threshold of necessity and proportionality which must be justified, before interference with encrypted communication can be allowed. The draft rules don't provide any such means of justification on the benchmarks of necessity and proportionality, and we are concerned that the focus on "traceability" by government officials in justifying changes to legal requirements under these rules would directly harm the usage of strong encryption that ensures secure communications.

Finally, Section 69 of the Information Technology Act and its rules [the "Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009] provide the specific sanction and framework for the government to access, intercept or monitor communications between computer resources. We submit that providing such powers under rules made under section 79, which provides conditions for providing safe harbor to intermediaries, breaks away from the structure and powers provided under the Information Technology Act. We believe that the procedure established under the Interception Rules, also does not pass muster on the threshold of necessity and proportionality, and note that the constitutionality of the Section 69 provision and its rules is currently pending before the Supreme Court of India. Therefore, we submit that no provision on access to information by the government should be established - directly or indirectly - under rules made under section 79, and the government should endeavor to amend section 69 and the Interception Rules to put them in consonance with the jurisprudence of necessity and proportionality established by the Supreme Court of India in line with international human rights law standards that apply to communications surveillance.

2. **Draft Rule 3(7) :**

“The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;

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

(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.”

We understand the concern of the Government of India in ensuring compliance of India laws by intermediaries that operate in India but may have been legally incorporated or otherwise established abroad. However, we believe that the compliance burden placed under this draft rule is quite high and disproportionate to the aims set out to be achieved. The requirement of intermediaries only being companies established under the Companies Act in India takes away from the global nature of the internet and fails to recognise the many different entities who act as intermediaries on the internet. Not all internet intermediaries are large technology companies - the ease of the open internet has allowed the flourishing of platforms and services that might be used by a large number of users, but are run by nonprofits, volunteers, and other actors.

We do not believe that ensuring compliance with Indian legal process by requiring some form of legal presence would be an acceptable delegated rulemaking power under Indian law. If the Government of India wishes to undertake this, it would need to propose a legal amendment to the Information Technology Act or another new legal provision that would require parliamentary review and enactment. Even if doing so, we submit that the potential goal of addressing the concern of compliance with local laws can be achieved through other means, such as requiring a nodal officer or representative for the purpose of legal summons and process that is resident in India, rather than requiring the establishment of a new legal entity in India in the form of a company.

Further, we submit that the government must build on robust mechanisms of inter-governmental cooperation, including rights respecting proposals to improve MLATs (Mutual Legal Assistance Treaties).⁶ These treaties would ensure a human rights respecting mechanism between countries to share information, while ensuring proper compliance of laws by companies working across countries.

3. Draft Rule 3(8) :

⁶ For our proposals, see

<https://www.accessnow.org/cms/assets/uploads/2017/07/MLAT-Reform-and-MLAT-Bypasses-one-pager.pdf>.

“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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.”

We submit that this rule goes counter to the jurisprudence established by the Supreme Court of India under *Shreya Singhal vs Union of India*, in addition to international human rights standards and related legal norms. Existing legal and normative frameworks affirm and delineate the application of human rights online. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) - to which India is a signatory - remains applicable for its projection of the rights to opinion and expression across borders and forms of media. Freedom of expression restrictions must meet the “necessary and proportionate” test outlined in Art. 19(3) of the ICCPR. As the UN Human Rights Committee explains in General Comment 34, interpreting Article 19:

“Any restriction on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3.”

Further, as noted by UN Special Rapporteur Kaye, “states should not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means.”⁷

Despite clear tests and internationally applicable codes of conduct, global internet freedom is declining due to increasing government censorship and pressure on intermediaries and companies to take voluntary action for privatized enforcement of vaguely defined restrictions regarding types of information, identities, or modes of communication. In 2016, authorities in 38 countries arrested internet users based solely on social media content.⁸ According to a

⁷ Mapping Report on Freedom of Expression, States and the Private Sector in the Digital Age. Freedex, freedex.org/new-report-on-freedom-of-expression-states-and-the-private-sector-in-the-digital-age/

⁸ Freedom on the Net 2016. Freedom House, 9 Nov. 2017, freedomhouse.org/report/freedom-net/freedom-net-2016

Freedom House report, 65% of the countries surveyed required “companies, site administrators, and users to restrict online content of a political, social, or religious nature.”⁹

We submit that users need assistance in asserting their human rights online. Between February 2016 and early January 2018, our Digital Security Helpline has handled approximately 204 cases, including 102 from Syria, relating to online content that was flagged, removed, or blocked by platforms. Our cases represent a small fraction of instances where users require help with expertise, contacts, channels, confidentiality, or simply trust to approach the companies that make decisions impacting their rights.. This is particularly alarming because activists often rely on internet communication and platforms to document and expose human rights violations.

We submit that India must play the role of a flag-bearer for freedom of expression online, and set standards for expression online which celebrate the fundamental rights of Indians, and allows the exercise of rights in a meaningful manner. We understand that states are required to consider additional measures to help address abuse or other actions that harm their rights, but those measures must be in consonance with the principles of necessity and proportionality.

Important strides have been made by the Supreme Court of India in the seminal judgement of *Shreya Singhal vs Union of India*. We encourage the government to build on these standards in their letter and spirit. The Supreme Court of India while discussing “actual knowledge” under the intermediary rules laid down that the burden of this knowledge should not lie on the companies, and only judicial orders of content takedown and removal shall qualify as actual knowledge in the context of these regulations. This institutional and procedural safeguard prevents over-censorship by government and companies. We encourage the government of India to adopt this standard, and move away from content takedown requests solely by government agencies. This would also put the Indian law in consonance with the suggestions of the UN Special Rapporteur, namely that “*States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.*”¹⁰ At the very least, in the interim the Government of India must ensure that any government orders sent to intermediaries requiring the removal or restriction of access to online content must be lawfully issued under - and limited to the specific scope provided by - Section 69A of the Information Technology Act.

4. **Draft Rule 3(9):**

“The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

⁹ Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy. | Freedom House, 28 Oct. 2015, freedomhouse.org/report/freedom-net-2015/freedom-net-2015-privatizing-censorship-eroding-privacy

¹⁰ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35. Available at <https://documents-ddsny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

We submit that this draft rule provides for prior and automated censorship by intermediaries, which would have the effect of chilling expression online, lead to over-censorship by companies, and result in increased privatised enforcement by technology firms in a way that would harm human rights in our digital age. Access Now is especially concerned about the haphazard, uncoordinated development of regulatory proposals for using automated technology to flag, filter, or otherwise manage content online, without a clear pathway for ensuring the public can evaluate and understand what is being proposed.¹¹ We believe that this represents a serious risk for human rights, in particular to the freedom of expression.

We have noted previously that several proposed models or ongoing experiments for countering violent extremism (“CVE”) on the internet seek to deal with potentially harmful content through algorithmic “de-prioritization” of the content, among other types of interference. This approach can be counterproductive, since machine learning technologies used to flag content can fail to take the context into account. This approach can threaten the freedom of expression by undermining the free and open dialogue that the internet can enable. We strongly believe that companies should not rely exclusively on automated systems for flagging content since understanding context is crucial for determining whether the content will encourage rather than discourage extremism. Instead, programs for CVE should implement a procedure that combines use of algorithms and human evaluation, and, crucially, is situated within a framework that is grounded in international human rights law and standards.

It is our view that any measure to tackle the complex topic of online disinformation must not be blindly reliant on automated means, artificial intelligence or similar emerging technologies without ensuring that the design, development and deployment of such technologies are individual-centric and respect human rights.¹²

The UN Special Rapporteur on Freedom of Expression, Mr. David Kaye, has warned against proactive content monitoring or filtering as “both inconsistent with the right to privacy and likely to amount to pre-publication censorship”. He states that “*Automated content moderation, a function of the massive scale and scope of user-generated content, poses distinct risks of content actions that are inconsistent with human rights law.*”¹³

Further, the draft rules provides for the identification and removal of “unlawful” information. This is a very broad and vague framing which renders itself to misuse, and further over censorship. We submit that companies and the executive branches of governments should not be the arbiter of lawful expression, and the burden must be placed upon a independent adjudicators, preferable the judiciary, to make such judgements.

¹¹ For a more detailed examination of this subject and our policy guidance, see Access Now, A Digital Rights Approach to Proposals for Preventing or Countering Violent Extremism Online, November 2016. Available at <https://www.accessnow.org/cms/assets/uploads/2016/10/CVE-online-10.27.pdf>.

¹² <https://www.accessnow.org/civil-society-calls-for-evidence-based-solutions-to-disinformation/>.

¹³ See note 9.

Further, as per section 79(2)(b), an intermediary should not "select or modify the information contained in the transmission". This is one of the conditions posed for an intermediary to be eligible for the safe harbor provided under section 79. As drafted, this rule would require that the intermediary "select" and "remove" information transmitted, thus disqualifying them from taking the safe harbor provided in section 79. Given that these draft rules are made under the provisions of section 79, it is imperative that the draft rules abide by the provisions of the empowering section of the parent law.

We recommend that this rule be deleted in its entirety, as it would not help prevent the spreading of "fake news", but also cause the chilling of free expression, along with establishing a regressive regime of prior censorship in India.

Conclusion

Finally, we thank the Ministry for the opportunity to participate in the consultation. We recommend that the Ministry restart this consultative policy-making process and pause its proposal to amend the intermediary rules. Any policy discussions on this broad subject must include civil society, academics and the society at large in the discussion and pre-drafting process, and not be restricted to select government departments or only made accessible to certain stakeholders, such as industry.

We hope our recommendations aid the Ministry in ensuring a human rights respecting regime of intermediary liability and information technology law in India.

We stand available to assist the government for any clarification, help and assistance required in this process.

Thanking you,

Yours sincerely,
Raman Jit Singh Chima,
Asia Policy Director

Naman M. Aggarwal,
Asia Policy Associate

Access Now | <https://www.accessnow.org>

Intermediary Amendment Rules	Comments
<p>2. Definitions — (1) In these rules, unless the context otherwise requires,— (a) "Act" means the Information Technology Act, 2000 (21 of 2000); (b) "Appropriate Government" means appropriate Government as defined in clause (e) of sub-section (1) of section 2 of the Act; (c) "Communication link" means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item; the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element; (d) "Computer resource" means computer resource as defined in clause (k) of subsection (1) of section 2 of the Act; (e) "Critical Information Infrastructure" means critical information infrastructure as defined in Explanation of sub-section (1) of section 70 of the Act; (f) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation; (g) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act; (h) "Electronic Signature" means electronic signature as defined in clause (ta) of subsection (1) of section 2 of the Act; (i) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub-section (1) of section 70B of the Act; (j) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act; (k) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act; (l) "User" means any person who accesses or avails any computer resource of intermediary for the</p>	<p>Please also incorporate definitions of : "computer database" [section 43, Explanation (ii)]</p>

<p>purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary;</p> <p>(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.</p>	
<p>Due diligence to be observed by intermediary — The intermediary shall observe following due diligence while discharging his duties, namely: —</p>	
<p>(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person</p> <p>(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —</p> <p>(a) belongs to another person and to which the user does not have any right to;</p> <p>(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;</p> <p>(c) harm minors in any way;</p> <p>(d) infringes any patent, trademark, copyright or other proprietary rights;</p> <p>(e) violates any law for the time being in force;</p> <p>(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;</p> <p>(g) impersonates another person;</p> <p>(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;</p> <p>(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or causes</p>	<p>Culturally [you may please add]</p>

<p>incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.</p> <p>(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p> <p>(k) threatens critical information infrastructure.</p>	<p><i>May be deleted</i></p> <p><i>As defined in section 70 [Explanation]</i></p>
<p>(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2): Provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in subrule(2):</p> <p>(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;</p> <p>(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;</p>	<p>Please delete the word “actual”</p>
<p>(4) The intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.</p>	<p>Please replace with at least every three months</p>

<p>(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.</p>	<p>Please Add: For this purpose intermediary to provide a dedicated email ID or communication address to aid and support such government agencies.</p>
<p>(6) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.</p>	
<p>(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall: (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.</p>	<p>Please Add: (iv)Such nodal person shall have the requisite mandate, authority, etc. to act on behalf of the Parent Company on such issues</p>
<p>(8) 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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State,</p>	

<p>friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.</p> <p>(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.....</p>	<p>Please Add:as identified in sub-rule (8) above.</p>
<p>(10) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.....</p>	<p>Please Add:as mandated under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013</p>
<p>(11) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:</p> <p>Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.</p> <p>(12) The intermediary shall publish on its website the name of the Grievance Officer.... and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule (3) can notify their complaints against such access or usage of</p>	<p>...who is aware of community standards prevalent in India</p> <p>Please replace with the word “procedure”</p>

computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint;

(13)The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
57	MIT/79/057	<p>Respected Sirs,</p> <p>After a bare perusal of the aforementioned rules drafted by the Ministry of Electronics and Information Technology, I wish to convey the following concerns to you:-</p> <ol style="list-style-type: none"> 1. The regulations as a whole do not permit the authors/originators of the objectionable content from defending themselves against allegations before the concerned Grievance Officers, or in case of Governmental agencies that notify the perceivably “unlawful” acts. In order to democratise, and more importantly, observe the Principles of Natural Justice, I urge you to include such a provision. 2. The legal provisions on objectionable content that ought to be censored are not absolute, and require determination by a court of law. As recent as in 2014, in the case of Aweek Sarkar v. State of West Bengal, the test used was the test of “contemporaneous community standards” was said to be the applicable test by the Supreme Court of India. Taking into consideration, the diverse polity with reference to the consumers of online content, it will become immensely difficult to incorporate these standards without a just and fair procedure. <p>I hope that you may consider the above in the finalisation of the draft rules and regulations.</p> <p>Regards,</p> <p>Sankalp Srivastava Pune, Maharashtra</p>

Introduction

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa.

With this submission, the Centre for Internet & Society (CIS) would like to respond to the Ministry of Electronics and Information Technology's invitation to comment and suggest changes to the draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 (hereinafter referred to as the "draft rules") published on December 24, 2018.¹ CIS is grateful for the opportunity to put forth its views and comments.

In this response, we aim to examine whether the draft rules meet tests of constitutionality and whether they are consistent with the parent Act. We also examine potential harms that may arise from the Rules as they are currently framed and make recommendations to the draft rules that we hope will help the Government meet its objectives while remaining situated within the constitutional ambit.

High-level Comments

Below are our high-level comments to the proposed amendments to the Rules under Section 79 of the IT Act.

Need for holistic approach to disinformation

We acknowledge that the intention of the Ministry in planning these amendments, as stated by the Honorable Minister this July in the Rajya Sabha, is to ensure that intermediaries online platforms do not become the venue or conduit for *large-scale Misuse of Social Media platforms and spreading of fake News*.²

It is important to qualify that 'disinformation' can be broken down into different categories. For example, UNESCO has made the following distinction:

¹ Comments/suggestions invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018", Ministry of Electronics and Information Technology, 2018, <<http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9Cinformation-technology-in-termediary-guidelines>>

² Ibid.

- **“Disinformation:** Information that is false and deliberately created to harm a person, social group, organisation or country
- **Misinformation:** Information that is false but not created with the intention of causing harm
- **Mal-information:** Information that is based on reality, used to inflict harm on a person, social group, organisation or country.”³

We feel it is also important to understand that what qualifies as ‘disinformation’ can be heavily context dependent and solutions need to be able to accurately account for this. To this extent - a broad requirement for platforms to proactively filter unlawful content may be simpler for content such as pornography but would be more complicated for child pornography and vastly more difficult for fake content. This is especially true as emerging doctoring techniques, such as those utilised by “deep fakes”, are increasingly indistinguishable from real content and require fact checking and verification to surface if they are or are not real. ⁴

We also recognize that disinformation is a complex issue, and as such requires cooperation from multiple stakeholders including government, civil society, industry, the media, law enforcement authorities as well as the public. Similarly, solutions need to be multipronged with technical, legal, and individual components and need to seek to underscore multiple agendas simultaneously including that of cyber security, national security, democratic values, and the protection of human rights. There is also a significant need for research into disinformation in India.

There are a number of provisions in Indian law that can serve as legal tools for the Government in order to penalize disinformation or mal-information. These include Section 505 of the IPC, and if the disinformation is intended to cause communal strife then other provisions such as Sections 290 and 153A of the IPC are also available. The government furthermore has the ability to block content via Section 69A of the IT Act, intercept, monitor, and decrypt communications via Section 69(1) of the IT Act, and monitor and collect traffic data vis Section 69B of the IT Act. Recognizing that there are a number concerns with the Rules issued under that Section that CIS has previously pointed out,⁵ we would recommend that the government with the guidance of a court apply these provisions as and when justified.

At the same time, mass public awareness needs to be built around disinformation in order to help curb the spread and societal impact of the same. Watchdog organizations and fact checking organizations such as Boom⁶ or Factchecker.in⁷ also play an important role in

³ Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training, UNESCO, (15th November 2018) <<https://en.unesco.org/fightfakenews>>

⁴ Disinformation on Steroids: The Threat of Deep Fakes, Council on Foreign Relations, (16 October 2018) <<https://www.cfr.org/report/deep-fake-disinformation-steroids>>

⁵ V Kharbanda, Policy Paper on Surveillance in India, The Centre for Internet and Society, (August 2015) <<https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india>>; E Hickok, Policy Brief: Oversight Mechanisms for Surveillance, The Centre for Internet and Society, (November 2015) <<https://cis-india.org/internet-governance/blog/policy-brief-oversight-mechanisms-for-surveillance>>; Prakash, Pranesh. "How Surveillance Works in India." The New York Times, <http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india> (2013).

⁶ BOOM Live <<https://www.boomlive.in/about-us/>>

identifying misinformation. Indeed, the government should also focus on enabling mechanisms that verify the authenticity of content as opposed to removing content. Any approach to disinformation must also include robust accountability, oversight, and redressal mechanisms.

The current approach in the Rules places the responsibility of identifying unlawful content as well as the individuals spreading or creating such content fully onto private intermediaries. The Rules also attempt to place blanket and uniform requirements on domestic and foreign intermediaries regardless of function and size. Such a 'one size fits all' framework can risk harming individual freedom of expression and privacy and decentivises smaller intermediaries from setting up platforms as well as foreign intermediaries from operating in India.

Existing Concerns with the Rules

There are a number of concerns that the Centre for Internet and Society (CIS) had raised in 2011 on the draft rules released for consultation⁸, and the 2011 Rules that were notified⁹. A number of these concerns still remain and/or have become compounded with the 2018 proposed amendments. We recommend that the following previous recommendations be carried over to the amendment Rules:

- Rule 3(2) makes unconstitutional obligations on intermediaries by compelling them to advise users not to post “unlawful” content that includes “disparaging”, “racially, ethnically or otherwise objectionable”, “relating or encouraging money laundering or gambling”, which are restrictions beyond what is permissible by Article 19(2) of the Constitution.

Rule 3(2), in placing the aforementioned obligation, also makes no distinction between different types of intermediaries. While these standard obligations may accommodate one type of intermediary, they would not be accommodative of all. For example, an intermediary relying on user-generated content (UGC), would have different terms of use, as opposed an intermediary providing communication services. Forcing umbrella terms of use negates this inherent differentiation, and therefore is impractical.

It was recommended that Rule 3(2) in its entirety be deleted.

- Rule 3(4) (and now the proposed amendment to it), which compels the intermediary to inform its users that the intermediary has the right to terminate the users' service in case the terms of service are violated, assumes that all intermediaries are websites

⁷ FactChecker.in <<https://factchecker.in/about-us/>>

⁸ CIS Para-wise Comments on Intermediary Due Diligence Rules, 2011, The Centre for Internet and Society, (25 February 2011) <<https://cis-india.org/internet-governance/blog/intermediary-due-diligence>>

⁹ Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011, The Centre for Internet and Society, (16 July 2012) <<https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules>>

or applications, has no rational nexus with questions of intermediary liability or due diligence to be observed by intermediary for the purpose of protection from liability, and is *ultra vires* the IT Act.

It was recommended that Rule 3(5) of the 2011 Rules, analogous to Rule 3(4) of the current Rules, be deleted.

- Rule 3(5) is ultra-vires Sections 69 and 69B of the IT Act, rules under which already specify a procedure with certain safeguards for agencies to intercept and monitor information held by intermediaries.

It was recommended that Rule 3(7) of the 2011 Rules, analogous to Rule 3(5) of the current Rules, be deleted.

- Rule 3(10), which mandates intermediaries to report cyber security incidents to the Computer Emergency Response Team (CERT) has no nexus with intermediary liability, and should ideally be a rule issued under Section 70B of the IT Act.

It was recommended that Rule 3(9) of the 2011 Rules, analogous to Rule 3(10) of the current Rules, be deleted.

- By not having a provision that requires intermediaries to inform users when their content is taken down, draft Rule 3(8) enables an “invisible” form of censorship that may be incompatible with the constitutional requirements of due process and natural justice.

Applicability to intermediaries

The current intermediary guidelines, notified in 2011, and the draft rules make no distinction between the different types of entities that qualify as intermediaries under the law, and thus creates uncertainty as to how these regulations apply to them.

For instance, in the 2011 rules, rule 3(2) compels intermediaries to inform their users to not share or upload certain information. We believe that the intention of the rule is to place the obligation primarily on intermediaries that host third-party content. However, the definition of intermediaries under the IT Act includes service providers which may exert zero or minimal control over the actual content they transmit, such as internet service providers, cyber cafes, content delivery networks and backbone networks. Thus, the rules create confusion as to whether these obligations apply to them equally.

Similarly, the draft rules make certain obligations (for instance, for proactively monitoring content under draft Rule 3(9), or for enabling traceability under draft Rule 3(8), etc.) that are only applicable to intermediaries that host third-party content.

We recommend that instead of adopting a one-size-fit-all approach to intermediary liability, the Government devise a separate definition for intermediaries primarily hosting third-party content, and start a consultation process as to how the obligations would differ for different types of intermediaries.

Unclear scope of the term ‘unlawful’

The scope of the term ‘unlawful’ is undefined and used inconsistently throughout the Rules thus resulting in it potentially being broadly interpreted. It is used first in Rule 3(2)(b), as part of the due diligence duties of the intermediary, in consonance with several other terms which indicate the kind of subject-matter that the intermediary would be obligated to *not* host on its platform. Majority of these terms seem to go beyond the constitutional mandate of Article 19(2). Applying the principle of harmonious internal consistency within statutes, the term ‘unlawful’ also seems to assume a similar, overreaching context.

The next place where the term occurs is in Rule 3(8). Here, the intermediary is under the obligation, upon receipt of ‘actual knowledge’ [in lieu of the *Shreya Singhal* judgment], to remove content relating to ‘unlawful acts relatable to Article 19(2). The third use of the term, in Rule 3(9), is again in relation to the duty of the intermediary to apply automated technology to remove ‘unlawful’ content.

These usages render a proper, harmonious reading of the rules difficult. Not only is the term ‘unlawful’ *not* defined in the Rules, or in the parent Act, its usage in two out of the three instances of its occurrence is overbroad. While the merit of the term ‘unlawful’ in relation to Rule 3(2)(b) was not explicitly discussed in the *Shreya Singhal* judgment, it would not imply that the acts mentioned in the rule, not overtly struck down by the judgment, continue to be constitutionally valid. Nevertheless, save Rule 3(8), the interpretation of the term violates the dictum of the *Shreya Singhal* judgment, which had laid down that unlawful acts beyond Article 19(2) cannot form part of the section 79.¹⁰

In relation to the third usage of the term, even if we assume that mandating intermediaries to use automated technology to flag down unlawful content is valid, this still does not lay down the scope of the intermediary’s duty in this regard. This also does not define what is meant by unlawful content. The Indian Penal Code, and several other criminal statutes make certain conduct ‘illegal’ or ‘unlawful’, but there is no general definition of ‘unlawful content’. (For example, even books that are "banned" are not "unlawful content" since there is no provision for declaring them as such: there are provisions for declaring their publication and distribution unlawful and there are provisions for seizing such books.) In other words, what kind of content would the intermediary be obligated to filter using this technology? Would it only be content that relates to unlawful acts as per Article 19(2)? Or would it also include unlawful content as per the interpretation of Rule 3(2)(b)? Or unlawful as per any other law in India? Without any definition, or limiting guidelines to the term therefore, the duties of the intermediaries vis-a-vis its users, and the government is ambiguous.

¹⁰ *Shreya Singhal v. Union of India*, AIR 2015 SC 1523 (Supreme Court of India).

The *Shreya Singhal* judgment upheld the legal proposition that any restrictions not emanating from Article 19(2) could not find place in Section 79 of the Act and as an extension, it should be refrained from being imbibed under the guidelines rules as well. It was clarified that free speech comprises of three elements: discussion, advocacy and incitement; and however unpopular the former two might be, it is the last that can demand a restriction. There was cognizance of the fact that our constitution does not permit the State to place limits on freedom of speech in order to “*promote general public interest.*”¹¹ This is applicable for speech regardless of the mode of communication as supported by the precedent in *Ministry of Information & Broadcasting v. Cricket Association of Bengal*¹² case.

These thoughts have also found support in the 2013 report by the Parliamentary Standing Committee on Subordinate Legislation where the Committee stated that the terms in Rule 3(2) that have been defined under others laws should be incorporated in these rules and the undefined ones should be defined. Such a step would ensure that “*no new category of crimes or offences is created in the process of delegated legislation.*”¹³ Not defining all terms in the Rules is in direct contravention of the Committee’s recommendations.

It is also important to note that “information or content” is not made unlawful under Indian laws, whereas specific **acts** are made unlawful. Even books that are “banned” are not “unlawful content”, since there is no provision for declaring them as such: there are provisions for declaring their publication and distribution unlawful and there are provisions for seizing such books.

Recommendation

It is recommended that phrases employing the term ‘unlawful’ to define acts or speech be deleted in all three instances: draft rules 3(2)(b), 3(8) and 3(9).

Excessive delegation of legislative functions

Delegated legislation is a constitutionally accepted means by which the legislature may delegate a component of its function to an external authority¹⁴, which may include an executive authority, such as the Ministry of Electronics and Information Technology (MEiTy) in this case. However, there are entrenched constitutional limitations on the extent of delegation. The legislature cannot delegate essential legislative functions which includes the

¹¹ Ibid., para 21.

¹² Para 78, *The Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal & Anr.*, (1995) SCC 2 161, (Supreme Court of India).

¹³ Committee On Subordinate Legislation (2012-2013) (Fifteenth Lok Sabha) Thirty-First Report, Lok Sabha Secretariat, New Delhi, (March 2013)
<https://sflc.in/sites/default/files/wp-content/uploads/2013/03/31-Report-_IT_.pdf>

¹⁴ Vishwanathan, T. K. *Legislative Drafting Shaping the Law For the New Millennium.* p. 441-480 Indian Law Institute, New Delhi, 2015.

determination of legislative policy. They also cannot delegate the power to repeal, modify or alter the scope of an existing law.¹⁵

In *State of Karnataka v. Ganesh Kamath*¹⁶ the Supreme Court held that “it is a well settled principle of interpretation of statutes that the conferment of rule-making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent there with or repugnant thereto”. In *KSEB v. Indian Aluminium Company*¹⁷, it held that “subordinate legislation cannot be said to be valid unless it is within the scope of the rule making power provided in the statute”

As per *Indian Express Newspapers Pvt. Ltd. v Union of India*¹⁸, a subordinate legislation can be challenged on any grounds that the parent legislation might also be challenged but also be vulnerable if it does not conform to the parent statute or fail to comply with constitutional requirements. Basically, the agency to which authority is delegated is merely supposed to fill in administrative and procedural details for implementation of the law, not re-write or enlarge its scope.

The original section 79 merely states that the intermediary will not be held liable for any information hosted by her if she complies with the requirements as per the law. The draft rules are not limited to implementing the legislative mandate or filling out details, but instead create a host of new obligations on intermediaries (including proactively filtering content and disabling access in a number of cases) that do not pertain directly to the hosting of information or disabling of the same. These obligations have potential consequences for the safeguarding of fundamental rights enshrined in the constitution, which we will discuss throughout the rest of the document. Even if these obligations were to become law, it would have to be through the passing of a new legislation by the Parliament rather than as an executive notification under Section 79 of the IT Act by a Ministry.

Recommendations:

Even if these obligations were to become law, it would have to be through the passing of a new legislation by the Parliament after legislative debate rather than as an executive notification under Section 79 of the IT Act by a Ministry.

Specific Comments

Rule 3(2)(j)

¹⁵ *Agricultural Market Committee v. Shalimar Chemical Works Ltd* AIR 1997 SC 2502, (Supreme Court of India).

¹⁶ (1983) 2 SCC 40, (Supreme Court of India).

¹⁷ AIR 1976 SC 1031, (Supreme Court of India).

¹⁸ AIR 1986 SC 515, (Supreme Court of India).

“3. (2) Such rules and regulations, privacy policy or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that –

(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;”

Comments

The terms “threaten” or “public health or safety” are not defined under the Rules or in any of the laws referenced by the rules, and are therefore are left open to broad interpretation. Additionally, imposing restrictions on free speech for “public health or safety” interests is not reasonable under Article 19(2), and thus, the draft rule may be deemed unconstitutional.

There are three items whose promotion via an intermediary is prohibited by the draft rules, save as permitted by the Drugs and Cosmetics Act, 1940 (*hereinafter* D&C Act). These are: (i) cigarettes and any other tobacco products; (ii) consumption of intoxicant including alcohol; and (iii) ENDS and similar products.

However, the D&C Act *does not* regulate the promotion/advertisement of cigarettes and tobacco products, nor does it regulate promotion of alcohol. The only relevant matters in this regard under the scope of the Act are the sale of nicotine gum containing up to 2gm of nicotine (as per Chapter IV of the Act) and the regulation of ENDS and like products¹⁹. If the purpose of this clause is to extend the ban on the advertising of alcohol and tobacco products from television to the online platforms, then the clause should refer to the Rules and Notifications issued under the Cable Television Networks (Regulation) Act, 1995 and the Rules and notifications thereunder. The sub-rule, purporting to regulate online advertisements of the mentioned subject matter, however, does not seem to take into account *any* of the relevant regulations dealing with the same.

Moreover, use of the phrase ‘promotion’ instead of ‘advertising’ is over-reaching and therefore a cause for concern. As has been the case, several liquor companies indulge in surrogate advertising for the promotion of their products in the digital media.²⁰ This goes beyond mere product advertising, and results in in-film branding, association with sports events, hosting competitions and so on²¹. Without any limiting framework to the term

¹⁹ Advisory on Electronic Nicotine Delivery Systems (ENDS) including e-Cigarettes, Heat-Not-Burn devices, Vape, e-Sheesha, e-Nicotine Flavoured Hookah, and the like products, Ministry Of Health & Family Welfare, (28 August 2018)

<<https://mohfw.gov.in/sites/default/files/ADVISORY%20ON%20ELECTRONIC%20NICOTINE%20DELIVERY%20SYSTEMS%20ENDS.pdf>>

²⁰ Surrogate liquor advertising: Time for change?, Santosh Jangid, (2 October 2017)

<<http://www.indiantelevision.com/mam/marketing/mam/surrogate-liquor-advertising-time-for-change-171002>>

²¹ Liquor brands override ad bans by leveraging digital, R Maheshwari & PM Dasgupta, (26 November 2015)

“promotion”, the draft rule may result in overbroad interpretations that go beyond standards even laid out by the Advertising Standards Council of India Code²².

Recommendations

- 1) The entirety of (j) to be deleted as it does not fall within the limits of Article 19(2).

Rule 3(2)(k)

*“3. (2) Such rules and regulations, privacy policy or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that –
(k) threatens critical information infrastructure.”*

Comments

The Government as per S.70 (1) of the IT Act, through its official gazette can notify any resource to be critical information infrastructure if *“the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety”*.

Threatening CII, ostensibly, can be read into the endangering national security. However, the use of the term “threatening” is of concern here, since it is unclear what constitutes threatening and how an intermediary would determine this. Further, the term ‘threatening’ is inconsistent with section 66F(iii) of the IT Act which, among other things, punishes acts that adversely affect critical information infrastructure and characterizes the same as cyber terrorism.²³ Moreover, section 70(3) of the IT Act already criminalizes unauthorized attempts to access critical infrastructure.

Recommendations

It is recommended that this clause be deleted as threats to critical infrastructure are already addressed through section 66F and 70 of the IT Act.

Rule 3(4)

“3. (4) The intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to

<<https://brandequity.economicstimes.indiatimes.com/news/digital/liquor-brands-override-ad-bans-by-levera-ting-digital/49923754>>

²² The Code for Self-Regulation of Advertising content in India, The Advertising Standards Council of India (September 2018) <https://ascionline.org/images/pdf/code_book.pdf>

²³ “...and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70”

immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.”

Comments

This rule states that the intermediary has a duty of informing users that in case of non-compliance with rules and regulations, ToS and privacy policy, the intermediary can *terminate* the usage or access rights of the users. These policies are not directly related to intermediary liability exemptions bestowed by S. 79.

The suggested termination procedure also lacks a notice and appeal requirement. In other words, the intermediary is not obliged to give a notice to the concerned user before terminating the access or usage rights or provide them a mechanism to appeal the decision.

Recommendations

It is therefore recommended that this provision be deleted as account restriction does not directly pertain intermediary liability. If this requirement is included, the intermediary must also be required to provide a procedure of notice that includes the reason for termination to the users, and a procedure of appeal against such termination. We would recommend similar safeguards as those laid out by the Manila Principles for content restriction:

- a. *“Before any content is restricted on the basis of an order or a request, the intermediary and the user content provider must be provided an effective right to be heard except in exceptional circumstances, in which case a post facto review of the order and its implementation must take place as soon as practicable.*
- b. *Any law regulating intermediaries must provide both user content providers and intermediaries the right of appeal against content restriction orders.*
- c. *Intermediaries should provide user content providers with mechanisms to review decisions to restrict content in violation of the intermediary’s content restriction policies.*
- d. *In case a user content provider wins an appeal under (b) or review under (c) against the restriction of content, intermediaries should reinstate the content.*
- e. *Where content has been restricted on a product or service of the intermediary that allows it to display a notice when an attempt to access that content is made, the intermediary must display a clear notice that explains what content has been restricted and the reason for doing so.”²⁴*

Rule 3(5)

“3. (5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or

²⁴ Principle 5 and 6 of the Manila Principles. <https://www.manilaprinciples.org/>

investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”

Comments

On receipt of a ‘lawful order’, the intermediary is required to provide ‘such information’ and assistance as asked by ‘any government agency’. In practice this provision could permit government agencies to request access to a broad range and large quantity of data held by intermediaries including both metadata and content data and at a lower standard than that mandated under section 5 and associated 419A rules of the Telegraph Act, section 69 and 69B and associated rules of the Information Technology Act, and section 91 and 92 of the CrPC. Further, if the corporations are not located in India, then Mutual Legal Assistance Treaties, and other treaties and laws would be applicable as well. There are four issues of concern here:

Process: First, the exact nature of a lawful order is unclear as is the process by which such order would be issued. It is also unclear which agencies are authorized agencies under the Rules.

Second, the terms ‘such information’ and ‘assistance’ are undefined and thus could encompass anything a governmental agency wishes to ask. Further, the grounds for such requests are too broad. For example, “protective or cyber security and matters connected with or incidental thereto” is undefined and is not found in other legal provisions.

Third, there are no clear oversight or review mechanisms as found in section 5 and associated 419A rules of the Telegraph Act, section 69 and 69B and associated rules of the Information Technology Act.

Fourth, the Rule further requires intermediaries to comply with orders for information and assistance within 72 hours. Depending on the size of the organization, location, and complexity of the request - it is unclear that all intermediaries would have the resources or the ability to comply with all orders within the 72 hour timeframe. The Rule also does not provide a procedure for an intermediary to request more time if needed. The pressure that this will place on intermediaries means that in practice they may not undertake the due diligence needed to verify requests and information and assistance shared. Furthermore, India’s formal provisions around interception, monitoring, decryption, collection of traffic data, and access to stored information do not place similar timeframes on intermediaries.

Fifth, the Rule does not recognize the MLAT process or recent developments in the modalities of cross-border data sharing such as the US Cloud Act and the ability for the government to use those processes to access information and assistance.

Further, there are several issues with the obligation on intermediaries to enable “tracing out of [...] originator of information”.

First, it is unclear what kind of information the intermediaries will have to share with authorized agencies to comply with such requests. The word “tracing” or the phrase “tracing out of [...] originator of information on its platform” are broad enough to include several kinds of information: for instance, it is unclear whether the Government is seeking to (a) provide particular content to an intermediary and request the identity of the creator of the content, or (b) request communication metadata. In either case, there is no specific reason why the information the Government is seeking under “tracing” cannot be provided under the first part of this provision, i.e. information or assistance requests.

Second, in either interpretation, several categories of intermediaries will be technically unable to comply with the traceability requirement. For instance, ISPs transmitting encrypted traffic from a user to a service have no access to its contents or granular information (say final intended recipient of content when the user is communication with an intermediary). In this respect, the word “platform” is used in the rule, but is left undefined. It is unclear whether the draft rule places obligations on just social media platforms and interpersonal messaging services, or all intermediaries as defined by the law. This vagueness has far-reaching implications on the services provided by internet service providers, backbone networks, cyber cafes, content delivery networks, and a host of intermediaries that exert little control over the content they transmit.

Even when we limit ourselves to communication applications, the current phrasing, i.e. “shall enable tracing [...] as may be required by government agencies [...]”. This makes it unclear as to whether (a) all intermediaries have to enable “tracing” by default and comply with Government information requests in this regard, or (b) enable “tracing” when asked by the Government. For instance, Whatsapp claims that it does not retain logs (metadata) of delivered messages.²⁵ If the draft rule is interpreted as (a), then the draft rules force them to retain communication metadata at all times; and if it is (b), then the company only has to retain communication metadata of only certain individuals when requested by the Government.

In this context, it is useful to note that several privacy-preserving applications and software are technically designed to decrease the information available to the service provider. For instance, Signal messenger has a feature called “sealed sender”, which prevents the Signal server from knowing the identity of the sender of messages, thus reducing the amount of

²⁵ Information for Law Enforcement Authorities, Whatsapp
<<https://faq.whatsapp.com/en/android/26000050/?category=5245250>>

communication metadata available to them.²⁶ The proposed rules create uncertainty as to whether these services are in risk of losing their exemption from liability.

Additionally, tracing of the originator of the concerned information can be done by 'any authorized agency'. So the rule creates a dichotomy between government agencies who can request information and authorized agencies who can request tracing. This dichotomy must be removed and only a list of authorized agencies, priorly notified, must be able to perform either of these functions. It is unclear how this provision works with section 69 and associated rules of the IT Act which enables authorized agencies to request decryption keys from intermediaries.

Recommendation

We would recommend that this provision be deleted, and section 69(1) and 69B of the IT Act, section 5 and 419A rules of the TA, and section 91 and 92 of the CrPc be relied upon for access to information and assistance including traceability. If the information or assistance is required from a foreign intermediary - the MLAT system must be followed. As a note - CIS is cognizant of the challenges in the MLAT system and would also recommend India to start exploring solutions to the MLAT system, including potentially the negotiation of a multilateral data sharing agreement.²⁷

We had recommended that India improve its position in diplomatic negotiations with the US by:

Utilising principles of International Law and concrete principles of human rights as a baseline tool for negotiations: Despite the uncertainty in the hierarchy of various permissive principles for extra-territorial jurisdiction, it is clear that Indian jurisprudence recognises these principles. International Law dictates that the hierarchy would need to be determined based on which country has a greater substantial connection to the crime at hand when deciding a conflicts situation. between a country, which is merely storing data as the processor is a company incorporated there and a country where the crime has been committed or whose citizens have been affected, it is clear that the latter would have a more substantive connection. Echoing these principles either in the MLAT agreement or any agreements entered into under the CLOUD Act should reflect this hierarchy. The argument can be made more cogently if these principles are referred to during the negotiations

Rule 3(7)

The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

²⁶ Technology preview: Sealed sender for Signal, J. Lund, (29 October 2018) <<https://signal.org/blog/sealed-sender/>>

²⁷ A. Sinha, E. Hickok, and Ors., Cross Border Data-Sharing and India: A Study in Processes, Content and Capacity, (27 September 2018) <<https://cis-india.org/internet-governance/files/mlat-report>>

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;
- (ii) have a permanent registered office in India with physical address; and
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.

Comments

Section 79 is an exemption clause relating to intermediary liability; provisions dealing with registration under the Companies Act or having an office in India have no rational nexus with issues of intermediary liability. Thus, these requirements on intermediaries relating primarily to the Companies Act may exceed the scope of the powers of subordinate legislation conferred by the IT Act.

This rule lays down two criteria to identify intermediaries that must maintain a physical office in India, and appoint a nodal officer to work with and respond to requests from law enforcement.: *first*, the number of users and *second*, whether it is list of intermediaries notified by the Government under the rule. As a note, rule 13 of the rules framed under section 69A also require the intermediary to appoint a nodal officer to handle governmental blocking orders.

Unclear requirement of user base: Though it is possible to place requirements on intermediaries based on the size of the user base, it is unclear (i) if this number would encompass all users globally or only the India user base, and (ii) whether this number is the active number of users for a specific period or users registered in entirety. Usually, only the intermediary would be privy to its precise number of users. Thus, to implement this provision, intermediaries would need to be mandatorily required to report their user base on a set schedule. Furthermore, it is unclear how users would be calculated for different types of intermediaries. For example, would the number of “users” for a content delivery network (CDN) be the number of customers they have or the number of end-users they end up serving?

Lack of guidelines for notified list: No mechanism, threshold, or guidelines for the inclusion of intermediaries on the list of notification has been specified, and thus the arbitrariness can be used to target intermediaries that may or may not have the financial standing to maintain a local office in India or support a 24/7 legal team. The cost of incorporating a company or having a permanent registered office in India may also prove to be a deterrent from expanding services in India and stifle innovation and competition. Furthermore, it is unclear why all intermediaries (even those operating services without commercial interests) must register as companies as opposed to another type of entity like a trust.

No distinction between types of intermediaries: By including all intermediaries in its ambit, the draft rule fails to take into account certain intermediaries, such as content delivery

networks and backbone networks, that primarily serve a network function and have minimal or zero control over the information that they transmit.

As an additional note: the use of the term 'law enforcement' is inconsistent with the term 'authorized agencies' used in other provisions in the Rules. Both of these terms - "law enforcement" and "authorized agencies" - leave the question of "who is authorized" unaddressed, leaving intermediaries guessing. Furthermore, the rules do not make any provisions for notifications listing out authorized agencies. Thus, the phrase "authorized agencies" is vague by talking of "authorized" without specifying how one is to recognize which agencies are "authorized" or by whom or under what law.

Recommendations

We recommend that draft rule 3(7) be deleted in its entirety as it exceeds the scope of delegated legislation permissible under Section 79. The nodal person already available to the Government under Section 69A could act as the contact for authorized agencies to seek the assistance of intermediaries for law enforcement purposes.

To achieve the Government's stated objectives, we recommend exploring comprehensive legislation that recognizes the different kinds of intermediaries such as Internet Service Providers, search engines, social networks, content aggregators, etc. and accord responsibility (perhaps even incorporation and physical registration), if at all, on the basis of this differentiation. 2) For certain categories of intermediaries, formulate a criteria based on user size and annual turnover to determine whether or not an intermediary needs to maintain a local office, if at all. 3) Formulate principles by which exceptional cases could be taken into consideration by the government. We recommend that the Government start a consultation process to formulate legislation with the briefly-summarised framework we present here, to which CIS will be happy to provide detailed inputs and specific recommendations.

Rule 3(8)

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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.

Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.

Comments

This provision requires intermediaries to comply with court and governmental orders that are within the ambit of 19(2) of the constitution within 24 hours and extends the data storage period by entities from 90 days to 180 days or as required by the Court or lawfully authorized government agencies. There are a number of concerns with this provision:

Firstly, this draft rule is in direct contravention of the Supreme Court's decision in *Shreya Singhal v. Union of India* which held that "actual knowledge" is only said to be accrued to the intermediary when it is informed of a court order or under asking it remove certain content.

Secondly, Though short time frames to comply with orders is a trend that a number of governments are adopting globally²⁸ research has yet to show the effectiveness of these timeframes, but research has demonstrated that it is extremely difficult for intermediaries to comply with all requests within 24 hours and still maintain a level of due diligence from their side.²⁹ As a note section 69A and associated rules do not place a similar time frame on intermediaries to comply with governmental orders, instead Rule 11 requires that intermediaries act 'expeditiously' but no later than seven days³⁰ and Rule 13 requires intermediaries to acknowledge the order within two hours of receiving the same.³¹

Additionally, the proviso that mandates the intermediary to preserve records for investigation purposes for 180 days does not specify the process for the extension of the retention period, nor does it make it clear who "lawfully authorised" agencies are, or under what law they need to be authorised.

Recommendations

We recommend that:

- The text "or on being notified by the appropriate Government or its agency" should be replaced with "or on being notified by the appropriate Government or its agency about a valid court order". A process for the government to issue such orders from a court to intermediaries should be established. This could be the same process as established under section 69A and associated Rules of the IT Act.

²⁸ For example: 1) NetzDG gives 24 hours to remove content that is 'obviously illegal' and seven days for 'illegal' content. 2) DMCA does not have a particular time-frame, but research shows that the time period is somewhere in between 24-72 hours. 3) EU's code of conduct on countering online hate speech has a time-frame that is less than twenty four hours.

²⁹ V Munjal, A March towards Digitization, PSA E-Newsline, (December 2017) <<http://www.psalegal.com/wp-content/uploads/2017/01/E-Newsline-December-2017.pdf>>; A. Mohanty, An Open Letter to Kapil Sibal on Copyright and Free Speech, SpicyIP (18 May 2012) <<https://spicyip.com/2012/05/dear-mr-sibal-youve-got-it-all-wrong.html>>; S. Pathak, Information and Technology (Intermediaries Guidelines) Rules 2011: Thin Gain with Bouquet of Problems <<http://docs.manupatra.in/newsline/articles/Upload/269ED933-8F47-4EB3-A6C3-DA326C700948.pdf>>

³⁰ "11. Expeditious disposal of request.--

The request received from the Nodal Officer shall be decided expeditiously which in no case shall be more than seven working days from the date of receipt of the request."

³¹ "(2) The designated person of the Intermediary shall acknowledge receipt of the directions to the Designated Officer within two hours on receipt of the direction through acknowledgement letter or fax or e-mail signed with electronic signature."

- The proviso “Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised” should be modified to “Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as communicated to the intermediary through a court order.”
- A procedure for the intermediary to challenge the notification should be established.
- Notification that results from ex-parte hearings should be challengeable by any interested party.
- Notifications should be published on a website like: accessremoval.meity.gov.in to allow for transparency, and so that such notifications may be appropriately challenged through an established legal framework.
- We recommend that the 24 hour timeframe is removed and instead, as in 69A and associated Rules, intermediaries be required to acknowledge receiving the order and act ‘expeditiously’.
-

Rule 3(9)

“3.(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

Comments

We have two broad sets of concerns regarding this draft rule. They can be classified as under:

- 1. Constitutional and legal concerns**
 - a. Vagueness and inaccuracy in the language of the provision
 - b. Inappropriate delegation of a state’s duty to a private actor
 - c. Violation of the right to freedom of speech and expression under Article 19 of the Constitution, and international human rights laws that India is bound by
 - d. Similar laws in Europe which have been criticised on grounds of violating the ICCPR, the Universal Declaration of Human Rights, and similar Europe-level human rights instruments
- 2. Practical and technical concerns**
 - a. Accuracy of automated technologies such as big data analytics and Artificial Intelligence
 - b. Costs and sustainability of deploying automated technologies
 - c. Accountability and oversight of decisions taken by automated technologies

1. Constitutional

(a) Vagueness in the language of the provision

In *Kartar Singh v. State of Punjab*³², the Supreme Court held that as a basic principle of legal jurisprudence, an enactment is void for vagueness if the prohibitions it imposes are not clearly defined. Laws should give a person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly as vague laws are subject to manipulation and might not give fair warning to the innocent.

The wording of Rule 3(9) fails this test due to the absence of the definition of certain key terms. For example the phrase “unlawful information or content” is undefined. While “information” is defined in Section 2(1)(j), “unlawful” is not defined in the IT Act, 2000 or the draft rules. Further, there is no definition of ‘automated technology’ that might be used by the intermediary or definition of ‘appropriate controls’ and there is an absence of guidelines on the timelines imposed on the intermediary to take down the content or further information on a process that might be followed in pursuance of such removal or for appeals (automated or otherwise) for such automated removals.

As highlighted in the high-level comments above, it is also important to note that “information or content” is not made unlawful under Indian laws, whereas specific acts are made unlawful.

(b) Inappropriate delegation of a state’s powers to a private actor

Shifting the burden of adjudicating what is ‘unlawful’ content onto a technology developed or procured by the intermediary is against the constitutional mandate of *Shreya Singhal*. The legislature cannot do indirectly what it cannot do directly.³³ This goes specifically against the interpretation given to section 79 by the Supreme Court in *Shreya Singhal*, viz. “Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material.” Further, the Supreme Court also stated that “The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69A read with 2009 Rules.”³⁴ Therefore, since the section under which these Rules are issued itself has been qualified by the requirement of a court or governmental order, the Rules cannot revive the obligation to remove content in any manner other than through a court.

Further, by unconstitutionally delegating an act that could have potential implications for the freedom of expression to a private actor, the state is indirectly avoiding its responsibilities under Part III of the Constitution and shifting the same to a private actor. It was clearly stated in *Hamdard Dawkhana* that the legislature cannot do indirectly what it cannot do directly.³⁵ Whenever a government body performs a ‘public function,’ they are subject to the entire gamut of fundamental rights, which include the substantive and procedural due process requirements in Article 21, the Right to Equality in Article 14 and the Freedom of Speech and Expression in Article 19. Any individual is entitled to file a writ petition against the state for violation of its fundamental rights. However, judicial precedent on the horizontal application of fundamental rights has still not been clearly delineated. This

³² (1994) 3 SCC 569 (Supreme Court of India).

³³ *Hamdard Dawakhana v. Union of India*, 1960 AIR 554 (Supreme Court of India).

³⁴ *Shreya Singhal*, para 116

³⁵ *Hamdard Dawakhana v. Union of India*, 1960 AIR 554 (Supreme Court of India).

effectively means that any individual whose content has been arbitrarily removed by the intermediary has no constitutionally viable means of enforcing her fundamental right as the specific act of identifying and evaluating the content as illegal and subsequently taking down the material has not been done by the state. As effectively articulated by Seth Kreimer, expert on constitutional law at the University of Pennsylvania, this form of delegation effectively amounts to ‘censorship by proxy.’³⁶

It is also vital to note that legally requiring private actors to make determinations regarding content restriction, can often lead to over-enforcement as the intermediary is incentivised to err on the side of taking down content in order to avoid expensive litigation.³⁷ A study conducted by Rishabh Dara at CIS demonstrated this in the Indian context as it was found that six out of the seven intermediaries who were sent flawed take-down notices by private parties over complied even in cases where the notice had some debilitating flaws.³⁸ This could have a high social cost and an indirect chilling effect on the freedom of expression online, which is compounded by the information asymmetry that exists because the user continues to remain unsure about the process, reasoning and oversight that went into the takedown. As we discuss below, these concerns can become further compounded when the decision is taken by an automated tool without human oversight or intervention.

(c) Violation of the constitutional guaranteed right to freedom of speech and expression under Art. 19

The transgression of constitutionally guaranteed standards of free speech and expression commences with the use of the word ‘unlawful’. As we discussed previously in the beginning of this submission, the use of the word “unlawful” in Section 79(3)(b) of the IT Act was challenged in Shreya Singhal on the grounds that it goes beyond the restrictions delineated in Article 19(2) of the Constitution. The Supreme Court clarified that “unlawful acts” which do not fit under one of reasonable restrictions to the freedom of speech and expression laid down in Article 19(2) cannot form any part of Section 79, and also read down Section 79(3)(b) on those grounds.³⁹

As we discussed at the beginning of this submission, the restriction can only be incorporated through new legislation. **Further, whether the restriction is reasonable or not should be determined on a case-by-case basis.** ⁴⁰**This should be done to ensure that the "practical results" of such actions are duly considered before imposing disproportionate restrictions.**

³⁶ Kreimer, Seth F. "Censorship by proxy: the first amendment, Internet intermediaries, and the problem of the weakest link." U. Pa. L. Rev. 155 (2006): 11.

³⁷ Kraakman, Reinier H. "Gatekeepers: the anatomy of a third-party enforcement strategy." Journal of Law, Economics, & Organization 2, no. 1 (1986): 53-104. ., Lee, D. "Germany's NetzDG and the Threat to Online Free Speech." (2018).
<<https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech>>.

³⁸ Dara, Rishabh. "Intermediary Liability in India: Chilling Effects on Free Expression on the Internet." (2011) <<http://cis-india.org/internet-governance/intermediary-liability-in-india>>.

³⁹ P. 117, 119, Shreya Singhal v. Union of India, AIR 2015 SC 1523 (Supreme Court of India).

⁴⁰ State of Madras v. V G Row [1952] SCR 597 (Supreme Court of India).

(d) Lessons from International Law and Europe

Laws like the NetzDG⁴¹, or the 'fake news' law in France⁴², mandate that the intermediary take down content that is 'manifestly' illegal. The NetzDG has attracted immense criticism from civil society activists. David Kaye, who is the UN Special Rapporteur on freedom of expression penned an open letter to the government of Germany arguing that the vague and ambiguous criteria used in the law is incompatible with Article 19 of the ICCPR which guarantees the right to freedom of expression.⁴³ Permissible restrictions on the internet should be judged on the same parameters as those offline.⁴⁴

Indeed, under article 19(3) of the ICCPR which has been signed and ratified by India, restrictions on the right to freedom of speech and expression must be

1. Provided by Law: It is not sufficient if the restriction on the freedom of expression is formally enacted as domestic law. They must also be sufficiently, clear, accessible and predictable-something that the present guidelines are not due to the presence of vague and ambiguous terms.

2. Necessary for the rights and regulations of others: This incorporates an assessment of proportionality of the restrictions which should have the objective of ensuring that these restrictions " targets a specific objectives and do not unduly intrude upon the rights of targeted persons."⁴⁵ The interest being intruded upon must also be the least intrusive means possible. Without considering and undertaking extensive research and pilot projects on alternative means available to curb the 'fake news' or disinformation issues, the NetzDG, like Rule 3(9) violates the ICCPR.

2. Practical and Technical Concerns

(a) Accuracy of automated technologies such as big data analytics and Artificial Intelligence

The draft rule has suggested that automated technologies be used to conduct this filtering. It has been widely argued that automated technologies are inappropriate for conducting

⁴¹ E. Douek, Germany's Bold Gambit to Prevent Online Hate Crimes and Fake News Takes Effect, (31 October 2017)

<<https://www.lawfareblog.com/germanys-bold-gambit-prevent-online-hate-crimes-and-fake-news-takes-effect>>

⁴² M.R. Fiorentino, France passes controversial 'fake news' law, (22 November 2018)

<<https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law>>

⁴³ Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (1 June 2017),

<<https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf>>

⁴⁴ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)

<https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>.

⁴⁵ General comment No. 34, United Nations ICCPR (CCPR/C//GC/34) (12 September 2011)

<<https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>>.

filtering as it lacks the human judgement to assess context. Further, outsourcing filtering to Artificial Intelligence driven technologies come replete with the problems to endemic to AI.

In a previous report⁴⁶, we had documented the possible sources of discriminatory decisions that may come with any decision made by Artificial Intelligence. The same systemic issues apply in this case. These include

1. Incomplete or inaccurate training data

The data being used for creating training data sets in the case of pro-active filtering might be incomplete or not reflect lacunae in the data collection process. This issue is most acute in the case of supervised learning systems that require labelled data sets, which proactive filtering mechanisms such as the one recommended in this rule would require.⁴⁷ As the labelling of datasets in new contexts, it is likely that the intermediary may use readily available sets that might not provide the complete picture. For example, many natural language processing systems use readily available training datasets from leading western newspapers, which may not be reflective of speech patterns in different parts of the world. A similar automated tool deployed for pro-active filtering by intermediaries raises similar concerns.⁴⁸

For example, there is a growing body of research on the use of automated tools for copyright enforcement and the problems that arise with their use. Research has shown that the use of Digital Rights Management (DRM) systems can have wide sweeping impact on free speech and on fair use.⁴⁹ It has been stated that enforcement algorithms work on rules set in code created by programmers, which are distinct from laws as made and interpreted.⁵⁰ Hence these tools might be programmed to remove infringing content but these tools lack the nuance to understand the context and verify whether the use comes under the fair use principle or if they are licensed.⁵¹ There have been multiple cases where these systems have taken down content that were in protected under fair use.⁵² Additionally, with the safe harbour provisions for the intermediaries to proactively remove infringing content it was observed that the intermediaries are at times using this as an excuse to over regulate, there

⁴⁶ A. Basu, E. Hickok, Artificial Intelligence in the Governance Sector in India, (14 September 2018) <<https://cis-india.org/internet-governance/ai-and-governance-case-study-pdf>>

⁴⁷ Danks, David, and Alex John London. "Algorithmic bias in autonomous systems." In Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, pp. 4691-4697. 2017; Discussion Paper on National Strategy for Artificial Intelligence | NITI Aayog | National Institution for Transforming India. (n.d.) <<http://niti.gov.in/content/national-strategy-ai-discussion-paper>>.

⁴⁸ D. Keller, Problems With Filters In The European Commission's Platforms Proposal, (5 October 2017) <<http://cyberlaw.stanford.edu/blog/2017/10/problems-filters-european-commissions-platforms-proposal>>

⁴⁹ Bar-Ziv, Sharon, and Niva Elkin-Koren. "Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown." *Conn. L. Rev.* 50 (2018): 339.

⁵⁰ Perel, Maayan, and Niva Elkin-Koren. "Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement." *Fla. L. Rev.* 69 (2017): 181.

⁵¹ Depoorter, Ben, and Robert Kirk Walker. "Copyright false positives." *Notre Dame L. Rev.* 89 (2013): 319.. Where the example was given how the online broadcast of Neil Gaiman's acceptance speech was disrupted because the DRM software flagged the images from Doctor Who to be copyright infringement, even though the images were licensed for the use during the awards.

⁵² Bar-Ziv, Sharon, and Niva Elkin-Koren. "Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown." *Conn. L. Rev.* 50 (2018): 339.

are multiple examples of content that were taken down on grounds of copyright enforcement.⁵³

2. Algorithmic Processing

An AI driven solution is an amorphous process-such as the 'risk profile' of an individual or the 'suspicious nature' of certain kinds of speech. While human may not be able to assess vast tracts of data to undertake the amorphous task of pro-active filtering, using source code enables a machine to do so. Through it's hidden layers, the machine generates an output, which corresponds to assessing the risk value of an individual, or in the case of pro-active filtering, certain forms of speech. Rouvroy further chastises 'algorithmic governmentality'-a phenomenon that ignores the subjective forms of speech and the embodied speaker. It reduces speech to quantifiable values-sacrificing inherent facets of dignity-such as their unique singularities, personal psychological motivations and intentions.⁵⁴

A further problem with algorithmic processing comes at the stage of developing the technology as the human monitoring the trial-runs and incorporating the results into the decision trees might suffer from some pre-existing sources of bias.⁵⁵ Facebook, Twitter, Youtube all have used machine learning to detect certain content on their platforms.⁵⁶ Google has also publicly committed to use machine learning algorithms to fight terrorism-related content.⁵⁷ Such techniques and commitments have in part arisen out of the government pressure or mounting number of content-takedown requests around the world (as the Transparency Reports of many of these intermediaries suggest) as well as the growing size of user generated content and user base. However, these have been their own commitments as opposed to compliance with governmental mandates to deploy automated techniques.⁵⁸ Usage of these tools also have had mixed results most of the time. While some have said that the tool has been useful in filtering out terrorist related content and spam, the same can not be said with hate speech⁵⁹, or adult content.⁶⁰

⁵³ For example YouTube facilitated the removal of a documentary film, India's Daughter, based on the gang rape of a twenty-three-year-old student, the screening of which was banned in India due to copyright infringement allegations. YouTube also allowed the censorship of the satirical show Fitnah when it complied with DMCA takedown notices sent by the primary, state-funded Saudi TV channel, "Rotana." See. Perel, M.; Elkin-Koren, N. (2016). Perel, Maayan, and Niva Elkin-Koren. "Accountability in Algorithmic Copyright Enforcement." *Stan. Tech. L. Rev.* 19 (2015): 473.

⁵⁴ Rouvroy, Antoinette. "The end (s) of critique: data behaviourism versus due process." In *Privacy, Due Process and the Computational Turn*, pp. 157-182. Routledge, 2013.

⁵⁵ M. Sears, AI Bias And The 'People Factor' In AI Development, Forbes (13 November 2018) <<https://www.forbes.com/sites/marksears/2018/11/13/ai-bias-and-the-people-factor-in-ai-development/#1dfa830c9134>>

⁵⁶ G. Rosen, F8 2018: Using Technology to Remove the Bad Stuff Before It's Even Reported Facebook Newsroom, (2 May 2018) <<https://newsroom.fb.com/news/2018/05/removing-content-using-ai/>>, How Content ID works, Youtube Support <<https://support.google.com/youtube/answer/2797370?hl=en>>, D. Harvey, D. Gasca, Serving healthy conversation, Twitter Blog, (15 May 2018) <https://blog.twitter.com/official/en_us/topics/product/2018/Serving_Healthy_Conversation.html>

⁵⁷ Content Regulation in the Digital Age Submission to the United Nations Human Rights Council, Special Rapporteur for Freedom of Expression (June 2018) <<https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/Witness.pdf>>

⁵⁸ J. Vincent, Why AI isn't going to solve Facebook's fake news problem, The Verge, (5 April 2018) <<https://www.theverge.com/2018/4/5/17202886/facebook-fake-news-moderation-ai-challenges>>

⁵⁹ B. Dickson, The challenges of moderating online content with deep learning, TechTalks, (10 December 2018) <<https://bdtechtalks.com/2018/12/10/ai-deep-learning-adult-content-moderation/>>

Respecting individual autonomy means, at the very least, ensuring that users have knowledge, choice and control. Pervasive and hidden AI applications that obscure the process of content display, personalisation, moderation and profiling and targeting can undermine the ability of individuals exercise their right of freedom of opinion, expression and privacy.⁶¹

(b) Costs and sustainability of deploying automated technologies

To assess the scale and sustainability of any initiative, we need to look both into financial costs and extent of disruption the proposal causes to existing business processes. So far, application of automated technology to filter/monitor content on social media platforms, has only been undertaken by the largest companies, with large-scale resources acting as the prerequisite.⁶² In light of this, mandating resort to these tools would be problematic because

- The research on the proper implementation of this technology remains incomplete
- Presumably (if the mixed results from the big companies is any indication), the resources and scale required for the smaller intermediaries to work this technology would be unreasonably high and unprofitable for their overall business.

Second, the requirement to “proactively” identify and remove “unlawful” content is technically impossible for certain intermediaries, such as ISPs, including Whatsapp transmitting encrypted traffic and interpersonal communication platforms which offer end-to-end encryption and would necessitate a rehaul of of their business practices and security protocols.

(c) Accountability and oversight of decisions taken by automated technologies

We accept that bias would exist if any decision outsourced to an algorithm were undertaken by a human being. The key difference between that and discrimination by AI lies in the ability of other individuals to compel the decision-maker to explain the factors that lead to the outcome in question and testing its validity against principles of human rights. A defining feature of Artificial Intelligence is the algorithmic ‘black box’ that processes inputs and generates usable outputs.⁶³ Ensuring accountability is an imperative that is challenging when the “values and prerogatives that the encoded rules enact are hidden within black boxes.” However, given the metaphorical ‘black box’ that converts inputs into examinable outputs,

⁶⁰ H. Bergstrom, Should Artificial Intelligence Be Used to Moderate Online Content?, Diplomatic Courier, (12 December 2018)
<<https://www.diplomaticcourier.com/2018/12/12/should-artificial-intelligence-be-used-to-moderate-online-content/>>

⁶¹ Promotion and protection of the right to freedom of opinion and expression (A/73/348)
<<https://undocs.org/A/73/348>>.

⁶² Content Regulation in the Digital Age Submission to the United Nations Human Rights Council, Special Rapporteur for Freedom of Expression (June 2018)
<<https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/Witness.pdf>>.

⁶³ Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

implementing workable accountability and evaluation standards for algorithms engaging in pro-active filtering remain a challenge.

The following gaps in accountability would exist if automated pro-active filtering by intermediaries were to be enabled:

- The reasoning and process followed in developing the algorithm
- The time limits, reasoning and process followed by the human beings on the moderation team in response to algorithmic output
- Appropriate avenues and processes for appeals and grievance redressal

Recommendations

We recommend that this provision be deleted in its entirety. There is a dire lack of research on the potential impacts of using automated technologies for pro-active filtering. We have outlined the adverse legal and societal impacts that this technology may have—all of which have been documented above. We also recommend that there must always be a human moderator taking the decision unless concrete research emerges showing that automation and the consequent creation of ‘black-boxes’ can generate more accurate and equitable patterns. We recognize that human moderation may not be able to keep up with the pace of discourse on social media and may be inaccurate but we hope that the mechanisms detailed below along with robust reinstatement systems providing clearer notification when content is removed and the reasons underpinning said removal.

We recognize, however, that the spread of fake news and misinformation via platforms needs to be curbed. There are three potential alternatives that might be considered, even though they are replete with potential concerns. Therefore, we recommend them as potential areas for research for government, civil society and industry, rather than as suggestions for implementation:

User-filtering:

As per a paper written by Ivar Hartmann advocating for this method, user filtering is a process that can be used for gatekeeping as it concerns the control of information flow.⁶⁴ In some ways, it re-configures power dynamics as the ‘gated’ become ‘gatekeepers.’⁶⁵ Essentially, this decentralized process of filtering exists in a scenario where the users of an online platform collectively accomplish an objective that regulate the flow of information. Users collectively agree on a set of standards and general guidelines for filtering.⁶⁶ Rough consensus or ‘incompletely theorized agreements’ where users agree on a set of (relative)

⁶⁴ I. A. Hartmann, Let The Users Be The Filter? Crowdsourced Filtering To Avoid Online Intermediary Liability, <http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/IPP2014_Hartmann.pdf>

⁶⁵ Karine Barzilai-Nahon, Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control, 59 Journal of The American Society For Information Science and Technology 1493, 1496 (2008).

⁶⁶ I. A. Hartmann, Let The Users Be The Filter? Crowdsourced Filtering To Avoid Online Intermediary Liability, <http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/IPP2014_Hartmann.pdf>

particulars rather than a set of (relative) abstractions can promote coordination even among users that have widely disparate ideologies, convictions and identities.⁶⁷

In addition to the potential fetters to achieving this 'incompletely theorized agreements,' Hartmann himself acknowledges two potential drawbacks of user-filtering:

1. **Incentives to engage in filtering:** This is linked to the problems of coordination. All users engaging in the filtering have a set of personal values that may not necessarily be shared. While clearly objectionable content such as child pornography, filtering certainly becomes more challenging in the context of hate speech. It remains to be seen how far community-centric standards can deal with this issue.
2. **Potential for over-filtering:** Hartmann conceives the possibility that as the power dynamics shift and users are given more power, they may apply stricter standards and filter more content. He cites the example of mothers who mobilized against the posting of breast-feeding pictures.⁶⁸

In addition, in the user-filtering model, the issue of appropriate appeal and grievance redressal mechanisms also crops up. Legally valid mechanisms that can enable aggrieved persons to challenge take-down decisions must be conceptualized.

Self-Regulation

This would require conceptualizing a scenario where status quo continues and intermediaries regulate speech on their platforms, as Google and Facebook have been doing. This has its disadvantages as it effectively grants autonomy to intermediaries, who are large business corporations and might incorporate self-regulation as part of their business strategy calculus as opposed to an independent societal prerogative.

Ghonim and Rashbass have indicated three ways in which self-regulation might be made more transparent and accountable⁶⁹:

1. The platform must publish all data related to all public posts so that the consumer is made aware of reach—both geographic and demographic and how a story attained 'viral' or 'trending' status.
2. They should publish the intricate details of their content regulation policies—including processes followed, hierarchies in the decision-making process followed, the substantive parameters involved and points-of-contact for grievance redressal.
3. Even if implemented effectively points 1 and 2 may not enable the public to keep pace with the existence and dissemination of posts on social media.⁷⁰ Therefore, Ghonim and Rashbass suggested that all platforms should develop an Algorithm Programming Interface (API) or 'Public Interest Algorithms' that capture the relevant

⁶⁷ Sunstein, Cass R., *Incompletely Theorized Agreements* (1995). *Harvard Law Review*, Vol. 108, No. 7, p. 1733, 1995.

⁶⁸ Emil Protalinski, *Breastfeeding women protest outside Facebook offices*. Available at: <http://www.zdnet.com/blog/facebook/breastfeeding-women-protest-outside-facebook-offices/8673> (last visited Apr 26 2012)

⁶⁹ https://www.washingtonpost.com/news/democracy-post/wp/2017/10/31/its-time-to-end-the-secrecy-and-opacity-of-social-media/?utm_term&utm_term=.6b7ef451d550

⁷⁰ <https://thewire.in/tech/beyond-twitter-russia-make-social-media-incorporated-work-democracy>

inputs and outputs used by the platform and make their data public so it may be easily consumed by the public.⁷¹

Co-Regulation: Models for multi-stakeholder co-operation on developing frameworks, standards and best practices for combating the issues that come with the use of social media in India today might be a useful starting point. The outcome may result in an universal code that guides a combination of self-regulation and user-centric filtering or in informal modes of cooperation. Either way, it is worth pursuing as a potential future research agenda.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

⁷¹https://www.washingtonpost.com/news/democracy-post/wp/2017/10/31/its-time-to-end-the-secrecy-and-opacity-of-social-media/?utm_term&utm_term=.6b7ef451d550

Comments on the (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

Rishab Bailey, Smriti Parsheera, Faiza Rahman

National Institute of Public Finance & Policy (NIPFP)*

31 January 2018

This note contains our comments on the (Draft) Information Technology (Intermediaries Guidelines (Amendment) Rules, 2018 (Draft Rules) that have been issued for public comments by the Ministry of Electronics and Information Technology. We begin by briefly setting out the context of Section 79 of the Information Technology Act, 2000 (IT Act) under which these rules are sought to be framed. This is relevant for explaining our overarching comments on the Draft Rules as well as the provision-wise comments contained in the subsequent sections.

1 Context of Section 79 of the IT Act

In its original form, Section 79 of the Information Technology Act, 2000 (IT Act) provided that an intermediary was not to be held liable for any offences committed by a third party under the IT Act, if *it could demonstrate* that the offence was committed without its knowledge or that it had exercised all due diligence to prevent the commission of the offence.¹

The basic aim of the provision was to extend the common law doctrine of pub-

*Rishab Bailey, Smriti Parsheera and Faiza Rahman are technology policy researchers at NIPFP, New Delhi. The views expressed are personal.

¹The term “intermediary” was defined in Section 2(w) of the IT Act as any person who on behalf of another receives, stores or transmits a message or provides any service with respect to that message.

lisher/distributor liability to the Internet. A distributor of illegal content in the physical world is not liable for the content, if she had no knowledge of it. On the other hand, a publisher, having knowledge and control of the illegal content, would be liable. For instance, a newspaper delivery service is not liable for a defamatory article published in the newspaper, even if it has acted to disseminate the newspaper (unless it received notice thereof). The publisher of the newspaper however would be liable. Holding the newspaper delivery service liable would be inequitable – it is not the decision of the delivery service to choose the relevant content. It would also be impractical – every newspaper delivery service would have to scrutinise the content of every newspaper and make a judgment on whether the content could possibly violate another’s rights.

While the logic behind the introduction of Section 79 was clear, there were problems with the wording of the section. This issue came to the fore in the case of *Avnish Bajaj v. State of Delhi* (116 (2005) DLT 427) where the management of an online auction site were proceeded against for the sale of pornographic material by users of the platform. In an application brought for quashing of the charges before the Delhi High Court, the Court noted that “By not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene.”²

In 2012, the Supreme Court overturned the findings of the High Court holding that vicarious liability cannot be fastened to Avnish Bajaj, and he could not be held guilty under the Information Technology Act as the company was not arraigned as an accused (*Aneeta Hada v. Godfather Travels*, Cr. A. No. 838/2012).³

Section 79 was amended vide the Information Technology (Amendment) Act, 2008,⁴ which introduced the present language of the provision. The changes in the section are notable. *First*, the new section introduced the possibility of safe harbour for offences committed under general laws (and not just the IT Act). *Second*, the section introduced a function based approach – where if the intermediary had (a) merely acted as a conduit or cache provider; (b) had not initiated the transmission or selected the receiver, or selected or modified the information

²The court found that no case was made out against the CEO of the auction website under the Indian Penal Code but that trial could proceed for offences under the Information Technology Act. Notably, in this instance no case was lodged against the web portal itself, and Section 79 of the IT Act was not specifically argued before the High Court.

³In a connected case, *Sharat Babu Digumarti v Govt. of NCT of Delhi* (Cr. A No. 1222/2016), the Supreme Court set aside criminal proceedings against another manager of the same online auction portal, on grounds that charges could not be brought under Section 292, Indian Penal Code due to the presence of a special statute in this regard.

⁴Originally introduced in Parliament as the Information Technology (Amendment) Act, 2006.

contained in the transmission, it could claim exemption from liability (subject to also adhering to due diligence and other guidelines laid down in this regard). In addition, the safe harbour could not be claimed if the intermediary conspired, aided, abetted or induced the relevant offence, or if it did not expeditiously act to remove the illegal content upon receiving ‘actual knowledge’ of it. *Third*, the amendment reversed the burden of proof requirement – the intermediary was no longer required to show it had taken all necessary measures to prevent the commission of the specific offence – it merely had to exercise due diligence and follow the guidelines laid down by the Government. The provision was later supplemented by the Information Technology (Intermediary Guidelines) Rules, 2011, which laid down the scope of due diligence expected to be adhered to by intermediaries.

In the course of its deliberations on the amendment of the provision, the Parliamentary Standing Committee examining the IT (Amendment) Act, 2006, noted that the term “intermediary” was of extremely wide import and could apply to virtually any online service provider. In examining the rationale for introduction of the safe harbour provision, the Standing Committee noted the representation of the Department of Information Technology, Government of India, which stated that the provision had been introduced as “...any of the service providers may not be knowing exactly what their subscribers are doing. For what they are not knowing, they should not be penalised. This is the provision being followed worldwide” (Parliamentary Standing Committee, 2007).⁵ From the aforesaid, it appears that the provision essentially seeks to protect intermediaries for actions that they are not directly involved in, i.e. where they merely carry content on behalf of third parties.

2 Comments on the overall approach

The increasing importance of the Internet in the daily lives of the citizens and the vital role it plays in enabling communications, democratic participation as well as economic and developmental benefits, is well recognised. The Internet’s vital role as a medium for dissemination of speech has also been recognised by the Supreme Court in *Shreya Singhal v. Union of India* (WP (Cr). No. 167/2012). Observing that the Internet provides a “*marketplace of ideas*”, the Court struck down Section 66A of the IT Act on grounds of grounds of vagueness and arbitrariness in the

⁵Interestingly, the Central Bureau of Investigation (CBI) had, in its deposition before the Standing Committee, sought to create a differentiation between online market places and other types of intermediaries. Per the CBI, only entities in the former class should be forced to undertake due diligence to avail of exemptions from liability.

wording of the provision and the scope for its abuse. The validity of Section 79 of the IT Act was also challenged in this case. In this context, the Supreme Court (a) ‘read down’ the phrase ‘actual knowledge’ in Section 79 to mean that intermediaries need only act to take down content subsequent to directions of an authorised agency of the Government or an appropriate court order; and (b) limited the scope of take downs under the section to those offences that fall strictly under the ambit of reasonable restrictions permitted under Article 19(2) of the Constitution.

The decision of the Court in the *Shreya Singhal* case bears significant relevance for the examination of the (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (the “Draft Rules”), not least as they seek to create a new route of taking down content under Section 79, which is not in line with the dicta of the Supreme Court. We also find that the proposed amendments to be extremely wide in their scope and well beyond the bounds of what is envisaged in Section 79. The proposed requirements to establish a physical office in India, enabling traceability of all originators of information, and offering information and technical assistance to Government agencies, cast a host of substantive obligations on a wide range of online actors. In doing so, the proposed Draft Rules are overstepping the mandate of the primary law, which would be in violation of the principles of delegated legislation. Finally, the proposed changes would result in disproportionate and unnecessary interference with expression and privacy rights of citizens. One must also take into account the possible costs to businesses and effect that the proposed amendments may have on the online ecosystem in India, as detailed further on in this submission.

While there is clearly a need for appropriate regulation of the online space, disproportionate and horizontally applicable obligations (i.e. requirements that are equally applicable to all intermediaries without distinction) are not the appropriate way to approach the issue (for the reasons outlined further in this response). Such an approach will hamper the growth of the online ecosystem in India and result in a chilling of fundamental rights in the online space.

The proposed amendments touch upon a number of legitimate issues in the online space – such as tracing of perpetrators of online crimes; access to encrypted data under appropriate circumstances; and role of big Internet companies in regulating content on their platforms. We recognise the importance of these concerns and the fact that the Government is duty bound to create an appropriate framework for protection of users in the online space. Therefore, the fact that deeper thinking on optimum regulation of the online space is necessary is not in doubt. What is of concern, however, is the process being followed in the present case – in terms of various substantive and complex issues being dealt with through an executive

order under Section 79 of the IT Act; and the substance of some of the proposed rules – in terms of their effects on digital rights, particularly privacy and freedom of speech and expression.

We detail below some of the overarching arguments relating to the proposed amendments, before moving on to discuss the individual proposals contained in the Draft Rules.

2.1 Scope of subordinate legislation

It is a settled legal principle that delegated legislation cannot do something not contemplated by the enabling legislation (Court, AIR 1971 Gau 110). The Supreme Court in Supreme Court of India (CA No. 3359/1997) has also held that “*the delegate which has been authorised to make subsidiary Rules and Regulations has to work within the scope of its authority and cannot widen or constrict the scope of the Act or the policy laid down thereunder. It cannot, in the garb of making Rules, legislate on the field covered by the Act and has to restrict itself to the mode of implementation of the policy and purpose of the Act.*” As noted earlier, Section 79, which is the enabling provision for the Draft Rules does not contemplate the numerous substantive obligations sought to be imposed by way of the present amendment. Notably, the provision does not envisage the proactive identification and removal of unlawful content by the intermediary (Rule 9 of the Draft Rules); calling upon intermediaries to provide assistance or information unconstrained by any procedure (Rule 5 of the Draft Rules); or alternate routes for blocking of content (as required under Rule 12 read with Rule 3 of the Draft Rules). Each of these concerns is explained in the rule-wise comments in the next section.

The Government cannot, under the guise of implementing “due diligence” or other norms, put in place a range of substantive obligations that have nothing to do with whether an intermediary actually acted as an publisher qua the content and/or acted to aid the commission of the offence in any way. By way of example, should the Government have free reign to impose substantive obligations on the broad set of actors classified as intermediaries through the present rules, could they conceivably change the tax status of intermediaries, put in place data protection law, etc.,⁶ all under Section 79 of the IT Act - which would be improper and ultra vires the enabling provision of the parent statute.

⁶In this regard, it may be noted that the existing Intermediary Guidelines Rules, 2011 merely require intermediaries to follow the substantive obligations imposed under the IT (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011. They do not, of themselves, impose substantive obligations of data protection on all intermediaries.

The fact that Section 79 does not contemplate the substantive obligations mentioned above is further demonstrated by:

- The judgment of the Supreme Court in *Shreya Singhal v. Union of India* (WP (Cr). No. 167/2012), where the Court clarified that the “actual knowledge” requirement in Section 79(3) implied that an intermediary could only be required to take down content after either receiving a court order or on receiving a lawful notification from the appropriate Government agency as it is very difficult for an intermediary to judge as to which takedown request is legitimate or not when they receive millions of such requests.⁷ The Supreme Court in *Shreya Singhal* also stated that the intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69A and rules under it, a provision which is closely related with Section 79 of the IT Act.⁸
- The IT Act already contains separate provisions that enable the Government to seek information or assistance from intermediaries, and that enable/require blocking of content. The proposed amendments therefore seek to replicate these powers (but with reduced checks and balances). For example, Section 69A of the IT Act and the rules thereunder already provide for a process for blocking of online content (which can take place only through a reasoned order, after complying with several procedural safeguards including a hearing to the originator and intermediary). Similarly, the rules notified under Section 69A of the IT Act specify the relevant authorities to seek information and assistance from intermediaries, subject to certain conditions.

2.2 A calibrated regulatory approach

Section 2(w) of the IT Act defines an intermediary as “*any person who on behalf of another person receives, stores or transmits that record or provides any service*” with respect to any electronic records. The term therefore includes a range of entities, such as internet service providers, cyber cafes, search engines, social media websites, private messaging services, e-commerce websites, etc. Notably, the definition of intermediaries does not restrict itself by function – implying that all participants in the Internet ecosystem, across the layers of the Internet are included within its ambit.⁹ By extension, the current intermediary liability rules,

⁷Paragraph 117, (*Shreya Singhal v. Union of India*, WP (Cr). No. 167/2012).

⁸Paragraph 116, (*Shreya Singhal v. Union of India*, WP (Cr). No. 167/2012).

⁹The wide scope of the definition was in fact noted by the Parliamentary Standing Committee examining the Information Technology (Amendment) Act, 2006. (Parliamentary Standing Committee, 2007).

as well as the proposed provisions of the Draft Rules also extend to all categories of intermediaries, irrespective of the nature of their functions or size (except in case of Rule 7). This framework does not differentiate between the roles played by different categories of online intermediaries, and or even network and transport layer intermediaries.

However, the call for comments accompanying the Draft Rules clearly indicates that the impetus for the Draft Rules stems from a Parliamentary motion on “Misuse of social media platforms and spreadig of fake news”, which led to a resolve by the Government to strengthen the legal framework to make social media platforms more accountable. Given the stated intention, the sweeping coverage of all types of intermediaries under the Draft Rules becomes particularly problematic. The Draft Rules contemplate a broad range of obligations, which as we explain later are not always appropriate or relevant for all types of intermediaries.

In the past, the Government has put in place guidelines under Section 79 that are applicable only to a specific class of intermediaries. The Information Technology (Cyber Cafes) Rules, 2011, for instance, apply only to cyber cafes. They put in place specific restrictions and obligations on the design, use, etc. of cyber cafes. Just as the same obligations should not be made applicable to all other types of intermediaries, cyber cafes and other intermediaries should also not be brought under the ambit of regulation that primarily seeks to target social media platforms.

The practice of having clearly differentiated obligations being imposed on intermediaries based on their operation and nature is also followed in other jurisdictions. The European Union’s E-commerce Directive (2000), on which Section 79, IT Act was modeled,¹⁰ distinguishes between intermediaries that provide hosting services¹¹, caching services¹² and those that act as mere conduits.¹³ This directive lays down a range of differentiated obligations for each category of intermediaries as a pre-condition to availing the safe harbour from liability.¹⁴

¹⁰Refer to the Report of the Parliamentary Standing Committee examining the Information Technology (Amendment) Act, 2006.(Parliamentary Standing Committee, 2007).

¹¹Services whose functions consists of the storage of information provided by a recipient of the service(Article 14)

¹²Services whose functions consists of transmission in a communication network of information provided by a recipient of the service(Article 13)

¹³Services whose functions consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network(Article 12)

¹⁴In order to avail of the safe harbour mere conduit intermediaries must not initiate the transmission, select the receiver of the transmission and select or modify the information contained in the transmission. Cache providers must not modify the information, must comply with conditions on access to the information, must comply with rules regarding the updating of the information, must not interfere with the lawful use of technology, widely recognised and used by industry,

In addition to the general European framework as detailed above, many European countries have also put in place specific legislations pertaining to specific online sectors and intermediaries. Germany, for instance, has recently passed its Network Enforcement law (NetzDG) that requires social networks to put in place procedures to remove or block access to content that is manifestly unlawful¹⁵ within 24 hours of receiving the complaint and remove all unlawful content within 7 days of receiving the complaint.¹⁶ However, notably, the legislation has limited the application of these obligations to large social networks with more than 2 million registered users in Germany and specifically excludes intermediaries offering journalistic or editorial content and those designed to enable individual communication or the dissemination of specific content from its remit.¹⁷ This law also requires social networks receiving more than 100 unlawful content related complaints per year to produce half-yearly reports on the handling of such complaints. Notably, in order to address concerns pertaining to overblocking the law imposes fines not for the failure to remove or block individual content, but only for the failure to institute and maintain robust procedures or organisational deficiencies (Guggenberger, 2018).

The European position detailed above is somewhat different from the position taken in the United States where Section 230 of the Communications Decency Act, 1996 (CDA), creates a horizontal system where all intermediaries are given safe harbour from prosecution irrespective of their role in the network. However, the immunity is not applicable to four cases (i) Enforcement of federal criminal laws, (ii) intellectual property laws, (iii) state laws, or (iv) electronic communications privacy laws (v) knowingly hosting third-party content that promotes or facilitates sex trafficking.¹⁸

to obtain data on the use of the information, and they must act to expeditiously remove or to disable access to the information it has stored upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Finally, in order to claim safe harbour, hosts should not have actual knowledge of the illegal act and, as regards claims for damages, should not be aware of facts or circumstances from which the illegal activity or information is apparent; and upon obtaining such knowledge or awareness, must act expeditiously to remove or to disable access to the information.

¹⁵Unlawful content is defined in the context of the requirements of certain offences described in the Criminal Code (Section 1(3) of the Germany (2017)).

¹⁶Section 3 of the Germany (2017)

¹⁷Merchandise platforms, gaming communities and professional networks such as Amazon World of Warcraft, LinkedIn and Whatsapp are likely to be exempt from these provisions (Guggenberger, 2018).

¹⁸This exception was brought in through the recent enactment of the the “Allow States and Victims to Fight Online Sex Trafficking Act of 2017” (commonly known as “FOSTA”)

Similar to the IT Act, the CDA also defines “interactive computer services”¹⁹ broadly to include intermediaries such as Internet service providers, websites, mobile apps, and any other platforms that transmit user-generated content. This legal protection holds even if the intermediary is aware of offending content or acts voluntarily to make editorial judgments on the content of its platform (Kosseff, 2017). Some have opined that this horizontal framework has led to the creation of an online system where anti-social acts are rife given that platforms have no real incentive to control their users or what they post.

That said, the US also imposes differential standards of online care on various intermediaries through a host of other laws and regulations. Important amongst these are:

- Children’s Online Privacy Protection Act, 1998 (COPPA): COPPA and the rules made under it are applicable to commercial websites directed to children below 13 years of age that collect or maintain personal information, and websites that have actual knowledge that they are collecting or maintaining personal information from a child below 12. It requires such websites to setup and maintain procedures to protect the confidentiality, security, and integrity of children’s personal information and obtain parental consent before collecting personal information of a child or allowing them to access facilities offered by the website(‘Children’s Online Privacy Protection Rule’, 2013).
- Digital Millenium Copyright Act, 1998 (DMCA): With regard to copyright infringing material, “safe harbour” is granted to intermediaries that do not receive a financial benefit directly attributable to the infringing activity, in a case in which the intermediaries have the right and ability to control such activity. In order to avail this immunity, intermediaries are required to publicise and implement a notice and takedown regime for removing alleged infringing content and a procedure to identify and remove repeat infringers (Map, 1998).

In light of the above, we submit that the legal framework ought to incorporate a differentiated approach to casting obligations on intermediaries based on the nature of activities being carried out by them and the risks and challenges arising from those activities. As explained above, intermediaries are of different types and provide a range of functions pertaining to the online environment. Many of them are not visible to the user (for instance root servers, internet exchange points,

¹⁹Section 230(f)(2): “The term ‘interactive computer service’ means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

gateways, backhaul providers etc.). These intermediaries assist in the delivery of communications from one node to another but do not themselves directly interact with the content. On the other hand some intermediaries, such as cyber cafes and wi-fi hotspots, merely provide a location for accessing online services. These types of intermediaries must be differentiated from those that actively host information or take the form of platforms where users can interact (such as WhatsApp, Facebook, Instagram, etc).²⁰

Putting in place equivalent substantive obligations on all categories of intermediaries makes little sense given the range of functions performed by them. It may also be practically impossible for certain intermediaries to implement the measures contemplated by the proposed amendments. For instance, it is unclear how a cyber cafe would enable the tracing of the originator of a message (contemplated by the proposed Rule 5 of the Draft Rules). Similarly, Rule 9 of the Draft Rules requires all intermediaries to invest in developing and deploying robust automated tools capable of both screening all content posted on intermediary platforms and accurately identifying and removing unlawful online content. Such a requirement imposes investment-heavy obligations on small intermediaries and start-ups.

This implies either a need to reassess the principal provision contained in Section 79 of the IT Act (to create a legislative framework for imposing differentiated obligations on different categories of intermediaries), or as indicated above in the context of cyber cafes, putting in place differential obligations in the form of due diligence and other guidelines based on the type of intermediary and the specific harm sought to be prevented against. At the very least, any intervention that is intended to apply to a specific category of intermediaries, such as social media platforms, should not be extended to all other categories of intermediaries. This issue is however being raised in addition to the broader criticisms of the Draft Rules, which remain valid even if the present proposals were to be made only in respect of regulation of social media platforms.

²⁰Interestingly, the Delhi High Court in *Christian Louboutin v. Nakul Bajaj* (2018) has also recognised how even online platforms can have a range of functions and business models. In this case, the Court again relied ultimately on the specific functions performed by the intermediary qua the offensive content to decide if it could avail of immunity from prosecution or not. Noting the role played by the online platform in identifying, promoting, and enabling sellers to sell their products in India, the Court held that the platform had crossed the line from being a passive to an active participant in the commission of the offence.

2.3 Existence of private censorship

One of the main concerns with the Draft Rules stems from the manner in which it is likely to result in intermediaries becoming a proxy for the exercise of online censorship by the State. Highlighting the problems with requiring platforms to go “further and faster” in policing Internet speech, Keller (2018) notes that the incentive of the platform would always be to err on the side of taking down content that may potentially appear to be offensive, inciteful, obscene or unlawful in other ways, in order to preserve itself from potential liability. Over zealous implementation along with over reliance on technological tools for the detection of content to be removed would lead to the curtailment of online speech. Examples of this include reported instances of YouTube taking down videos of Syrian atrocities posted by a UK human rights watchdog due to its inability of its algorithms to distinguish between the propaganda content and legitimate news reporting. Similarly, Facebook was found to have removed posts documenting the ethnic cleansing of Rohingyas as it had classified Rohingya organisations as dangerous militant groups (Keller, 2018).

While resisting legal mandates for policing of content by intermediaries is of paramount importance, and remains the focus of the present submission, it is also important to acknowledge that online services already exercise a level of private censorship function of their own violation. The range of controls over content posted on their platforms may include decisions on what content should go up (proactive monitoring) as well as the content that must be taken down (reactive monitoring). This is driven by internal policies, which in turn are shaped by the platform’s perceptions of what may be deemed as appropriate content by State agencies, advertisers and the sensibilities of their users.

With increasing fears of heavy-handed regulation by Governments, such voluntary controls are only going to increase. For instance, Facebook founder recently referred to their intention to focus more strongly on measures such as “*proactively enforcing our policies to remove more harmful content, preventing borderline content from spreading, giving people more control of their experience, and creating independent oversight and transparency into our systems*”. (Zuckerberg, 2018). The definition of what is considered to be harmful or unwarranted content by different platforms and the mechanism through which those policies are implemented, including the rights available to the user in the process, therefore becomes extremely important. These concerns are all the more relevant in case of large dominant platforms where the absence of a voice on those platforms could amount to effective exclusion from the overall discourse.

In the United States, voluntary enforcement mechanisms adopted by interme-

diaries draw support from the “good samaritan” provision contained in Section 230(c)(2) of the CDA. The provision exempts providers and users of an interactive computer service from “*any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected*”. The intent of bringing such a provision in the law was to *remove the disincentives to self-regulation* by intermediaries for the fear that it would lead to them being categorised as publishers hence attracting a stricter liability regime (Leary, 2018).²¹ The IT Act in India, however, does not contain such an enabling provision for self-regulation by intermediaries.

Given the context stated above and the prevalence of voluntary take down mechanisms under the policies of various service providers, it would be useful to start a separate conversation on the merits and demerits of such private forms of censorship and the constraints and mechanisms that should govern such activities. This should also include a discussion on building independent and effective mechanisms for providing redress to individuals and organisations that are adversely affected by such voluntary initiatives to control online content.

3 Rule-wise comments

This section provides our rule-wise comments on the proposals contained in the Draft Rules. The comments are applicable both to the new provisions sought to be introduced through the amendments as well as the existing provisions of the Information Technology (Intermediary Guidelines) Rules, 2011, which merit a reconsideration on account of developments like the Supreme Court’s decision in the *Shreya Singhal* case.

3.1 Rule 3(2)

Rule 3(2), requires every intermediary to inform users not to publish any information that violates the various categories of proscribed information. The list of proscribed content includes:

²¹This provision was brought about to counter the position adopted by the court in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995) imposing liability for defamatory content on a provider that actively screened and edited messages posted on its bulletin boards.

- content that “belongs to another person and to which the user does not have any right to”;
- content that is “grossly harmful”, “harassing”, “blasphemous”, “invasive of another’s privacy”, “disparaging”, “hateful” or “otherwise unlawful in any manner whatsoever”;
- content that “harms minors in any way”;
- content that infringes intellectual property rights or other proprietary rights;
- content that “impersonates another person”;
- content that “insults another nation”, etc.

We believe that the aforementioned list of information (that intermediaries are required to caution users against publishing) is arbitrary and vague. The list of proscribed information includes categories such as blasphemy, hateful or disparaging content. All of these being phrases that are not specifically defined or indeed criminalised in Indian law. We explain this further using the example of the term ‘blasphemy’, which is generally understood as the act of insulting or showing irreverence towards a god, or claiming the attributes of a deity. It has, however, been opined that blasphemy as a term is unfamiliar to the Indian legal and constitutional landscape (Bhatia, 2016). While certain statutes such as Section 295A of the Indian Penal Code contain variants of blasphemy laws, even these provisions do not criminalise blasphemy per se.²² For instance, Section 295A can be invoked only where there is a “calculated tendency” to disrupt public order (Ramjilal Modi v. State of UP, 1957 AIR 620). There must be a rationale nexus between the act committed and the breach of public order that such acts may lead to. Further, as noted in *Shreya Singhal*, mere advocacy of a unpopular opinion cannot be considered an offence (there must be an incitement to violence).

In creating an offence, the language used by the law must be clear and precise so as to give the public an indication of the elements of the offence (*Shreya Singhal v. Union of India*, WP (Cr). No. 167/2012). Provisions criminalising activities cannot be open ended, vague or undefined. While we note that Section 79 does not per se criminalise the actions mentioned in the provision (as was done by Section 66A of the IT Act), nonetheless, Rule 3(2) does entail an interference with rights of citizens. It requires them to exercise self-censorship of content that violates the broad phrases used in the provision.²³ Ultimately, there are consequences to the broad phrasing of the terms used in Rule 3(2), in light of redress functions

²²Also refer S 124A, 153A, 153B, 292, and 293 of the Indian Penal Code.

²³In addition to which intermediaries are also to take action in the context of these phrases, as required under Rule 12 of the Draft Rules.

specified under Rule 12, which renders them susceptible to arbitrary use. Words such as “harassing”, “hateful”, “disparaging”, etc. are all ambiguous terms which may have different meanings to different people and in different contexts. For instance, some comments can have a public purpose even if disparaging in character – for instance, a review of a book, movie or product may contain negative or disparaging remarks, but should not be censored just for this reason. The Supreme Court was clear in the *Shreya Singhal* case (in the context of whether persistently sending a message to a person would amount to inconvenience), that there must be a demarcating line conveyed by the expressions used in the section that clearly provides what specific behaviours are barred.

In this context, it must be kept in mind that analogous terms/phrases used in Section 66A of the IT Act were read down by the Supreme Court in the *Shreya Singhal* case. Notably, the Supreme Court has held that “*unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79...with these two caveats we refrain from striking down Section 79(3)(b).*” This implies that terms used in the Draft Rules that do not find backing under the constitutional schema established by Article 19(1) and 19(2) must be excluded. Accordingly, undefined and arbitrary terms that are not specifically offences under Indian law (such as blasphemous content, disparaging content etc.) must be removed from the Draft Rules.

While one cannot disagree that users must be made aware of their online responsibilities and the fact that Indian laws do apply online, it is questionable if the appropriate method to do this is to cast obligations on *all* intermediaries to do so. This not only places a cost on intermediaries, it is questionable whether it will serve any purpose given that literature demonstrates that most people do not in any event read the terms and conditions, privacy policies etc, made available on websites and other digital applications (Consumer Policy Research Centre, 2018); (McDonald & Cranor, 2008); (Solove, 2013); (The Internet Society, 2012). The requirements in Rule 3(2) may therefore serve no practical purpose. The Government should instead consider alternative and more effective methods of encouraging *relevant* intermediaries to educate the public. Specific provisions (and obligations) may also be brought in concerning intermediaries and platforms that specifically target youth or children, subject to a careful analysis of the costs and benefits of such initiatives.²⁴

²⁴As discussed previously, asymmetric obligations could be imposed on certain specific intermediaries through appropriate statutory changes.

3.2 Rule 4

The requirement for all intermediaries to inform users, once a month, of the need to comply with terms of usage is impractical and is unlikely to serve the intended purpose for the reasons mentioned below.

1. *Excessive notifications can be counter-productive:* As mentioned previously, research findings are clear in that providing excessive notifications to individuals can be counter-productive. Users generally do not read lengthy terms and conditions and bombarding them with information from multiple intermediaries will only mean that the likelihood of a user reading or understanding any specific notice is reduced (Consumer Policy Research Centre, 2018); (McDonald & Cranor, 2008); (Solove, 2013); (The Internet Society, 2012). Given the vast number of intermediaries that mediate access on the Internet (through multiple layers of the Internet), putting in place a notification requirement that applies to all intermediaries is impractical and disproportionate. Users will quite simply not care about the notices – whether in the form of pop-ups / links / email or SMS communications being sent to them, from dozens, hundreds or thousands of intermediaries they interact with on a monthly basis. Equally, the rule will also mean that services that a user may have registered for but no longer actively uses will also have to continue sending notices to the user. The proposed obligations will therefore impose a compliance cost on intermediaries and users, which does not appear to be supported by expected benefits.
2. *Ambiguity in establishing user-intermediary relationship:* The Rule implies that every intermediary (which includes a range of entities from cyber cafes to telecom service providers to social media websites to normal websites) will have to provide notice to every person who accesses or avails their services in any manner, and irrespective of the reasons for the same, the nature of the service being used or the duration of usage. It is unclear how every intermediary should comply with these requirements. As explained previously, the Internet comprises a range of intermediaries across its different layers. Often users will not know of the specific intermediaries that are being used to access any particular content. In addition, the term ‘user’ is also defined broadly to include any person who accesses or avails the computer resource of an intermediary. This creates some ambiguity about the circumstances in which a user-intermediary relationship can be said to be existing. For instance, in case of content delivered through a content delivery network (CDN) will the CDN provider and the user be deemed to have an intermediary-user relationship requiring the CDN to send notices to the user (separate from that

sent by the host of the website)? Equally, will cyber cafes be required to send notices to every user on a monthly basis?

3. *Privacy of users*: Often intermediaries will not have contact or other details of users (for instance, if its just a simple web blog with no login or subscription requirements). A literal reading of the Rule will mean that even web services that do not require any user registration etc. will be required to send notice to every person who accesses their services. Putting in place a requirement for intermediaries to actively source and retain user data, purely for the purpose of sending them the mandated information, will have repercussions on privacy of individuals as well as the businesses of many intermediaries. This will represent both a business cost as well as a potential litigation cost for intermediaries (as by collecting more personal information, they expose themselves to greater risks of loss, misuse, etc. of the personal information). Individuals on the other hand, will be forced to give out personal details to every intermediary they encounter in the online space. This may practically mean thousands of entities will have access to personal details of every user, irrespective of whether the user wishes to provide them or not. The rule as presently drafted is therefore arguably disproportionate and unnecessary and therefore in violation of the dicta of the Supreme Court in Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors (WP (Civ). No. 494/2012), wherein it was made clear that any interferences with privacy rights must be necessary in a democratic society i.e. it must inter alia satisfy the tests of necessity and proportionality.

In the circumstances, the requirements of Rule 4 appear impractical and unnecessary. Further, it may compromise privacy of individuals and act as a deterrent for businesses. It is therefore submitted that the proposed amendment to Rule 4 of the Draft Rules (i.e. the requirement of periodic notice) should be deleted. Finally, while there may be genuine reasons to ensure that certain types of intermediaries (such as social media websites) do put in place adequate notices for certain categories of users (such as children), more targeted and meaningfully constructed mechanisms will need to be developed for this purpose.

3.3 Rule 5

Rule 5 requires all intermediaries, upon receiving a lawful order, to provide “such information and assistance” as required by “any government agency” within a

period of 72 hours.²⁵ The intermediary is further required to enable tracing the originator of the information on its platform as may be required by legally authorised agencies. We believe this provision needs to be reconsidered for the following reasons:

1. *Expands the scope of permissible restrictions to right to privacy and free speech:* We note that Rule 5 expands the scope of permissible restrictions to the right to privacy and speech by permitting government agencies to seek information and assistance from intermediaries apropos of “protective or cyber security and matters connected with or incidental thereto.” Phrases such as “cyber security”, do not occur in Article 19(2) and were not considered as a legitimate state aim to restrict the right to privacy by the judges in *Puttaswamy*. Accordingly, we believe this phrase should either be removed from the proposed Rule 5 or should be connected to the permissible restrictions under Article 19(2).
2. *Circumvents procedural safeguards under S. 69 and rules thereunder:* As far as Rule 5 requires intermediaries to provide information and assistance to relevant government agencies, the Government and its agencies already have requisite powers under Section 69 of the IT Act²⁶ (refer Section 69(3)(a) to (c)) and rules notified thereunder in the form of the IT (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 (2009 IT Rules). In addition to the substantive provisions of Section 69(3)²⁷ Rule 3 of the 2009 IT Rules, specifically empower a competent authority (specific officials of the government) to pass directions pertaining to the decryption, interception, monitoring of information in any computer resource of an intermediary. Rule 13 of the 2009 IT Rules also requires intermediaries to provide “all facilities, cooperation and assistance” for interception / monitoring / decryption, as may be required by the relevant order of the competent authority.²⁸

²⁵The information and assistance called for may be related to (but is not restricted to) matters concerning security of the state, cyber security, investigation / detection / prosecution / prevention of offences, protection of cyber security and matters connected thereto.

²⁶As well as Section 69B of the IT Act

²⁷Which require an intermediary (or any other person in charge of a computer resource) to provide access to information in a computer resource, intercept/monitor/decrypt the information in a computer resource, provide the information stored in a computer resource

²⁸In addition, both generic laws such as the Criminal Procedure Code (CrPC) and sector specific regulations also give relevant government authorities the power to call for information / assistance from intermediaries. For instance, Section 91 of the CrPC permits authorities to summon any document or thing from a relevant person, if necessary or desirable for the purposes of an investigation / inquiry, etc. As far as sector specific regulations are concerned, the licenses issued to telecom and internet service providers by the Department of Telecommunica-

Importantly, the 2009 IT Rules contain certain safeguards before interception / decryption directions can be issued. For instance, Rule 8 of the 2009 IT Rules requires the competent authority to consider alternate means of sourcing the information prior to issuing such directions, while Rule 13(3) ensures that the intermediary is only required to provide information “to the extent the information is encrypted by the intermediary or the intermediary has control over the encryption key”. Thus, the powers of calling for assistance and information are limited by certain procedural and substantive fetters in the 2009 IT Rules.

The IT Act therefore clearly envisages a situation where law enforcement and other government agencies may require an intermediary to provide them user information, whether encrypted or not - and has dealt with this comprehensively under Section 69 and the rules thereunder and in accordance with the Supreme Court decision of *PUCL*. The instant rules, therefore, seek to bypass the already established procedures for lawful interception in the IT Act for government agencies to secure information from computer resources of an intermediary. It is therefore submitted that government cannot put in place an alternate process, indirectly through delegated legislation, which does not incorporate the procedural safeguards discussed above or substantive checks and balances.

3. *Usage of vague and undefined terms:* The scope of the term “information or assistance” is undefined and vague. This would permit, for instance, the government to mandate the insertion of backdoors in all digital platforms, which would be both unconstitutional (being a disproportionate interference with privacy rights) and harm network security more generally (Bailey, Bhandari, Parsheera, & Rahman, 2018). It is settled law that any interference with privacy rights of individuals must (a) be permitted by a law, (b) pursue a legitimate goal, (c) be proportionate, and (d) establish procedural guarantees to check against abuse of state power (Bhandari, Kak, Parsheera, & Rahman, 2017). Permitting state agencies to seek virtually any “information or assistance”, and that too without specifying a process for the same, violates both the proportionality and procedural guarantee related tests laid down by the Supreme Court in *Puttaswamy*.
4. *Ignores differences between various intermediaires:* As far as the requirement to enable tracing the originator of a message is concerned, it is submitted

tions contains various provisions pertaining to interception/technical assistance to be provided by the licensees to relevant government agencies. Further, certain other categories of intermediaries such as online banking systems, payment interfaces, etc., have assistance and information provision related obligations imposed on them by specific sectoral regulators.

that it is both disproportionate and impractical to impose such an obligation on all intermediaries. Not only is the requirement a substantive obligation that should be imposed through relevant statutory amendment (rather than through delegated legislation), the rule is also questionable in that it lays out no procedural fetters on the exercise of state power. As mentioned previously, all interferences with privacy rights must be proportionate and have relevant procedural fetters in place to prevent misuse of state power. The present rule lacks in both these aspects laying it open to a constitutional challenge. The proposed Rule 5 may also be susceptible to challenge in so far as it appears to do away entirely with the possibility of anonymous speech in the online space. As recognised by the United States Supreme Court in *McIntyre v Ohio Elections Commission* (No. 93-986, 1995), anonymity can serve as “a shield from the tyranny of the majority”. In this case, the Court noted the importance of protecting unpopular opinions or opinions by unpopular people who may not voice their views if forced to identify themselves. Clearly therefore, anonymous speech can also play a vital role in democratic life. Completely restricting the possibility of anonymous speech as the present rule seeks to do is therefore disproportionate and cannot be considered “necessary in a democratic society”.

It is also critical to consider the practicality of implementing Rule 5 and its possible effects on the online environment. The proposed provision will apply across the board to all intermediaries - which as mentioned previously, can be of multiple types. Intermediaries of the cache / conduit variety or indeed intermediaries such as cyber cafes may not have the ability to trace the originator of messages. While certain platforms may indeed have this ability, and in certain situations the government and its agencies may need to trace the originator of messages, this obligation ought not to be imposed on all intermediaries across the board. The provision also fails to consider the use of various technical tools by users such as encryption, VPNs etc., or indeed the fact that data packets may be routed outside India (even if originating or terminating in the country) thereby rendering the tracking process impractical (if not impossible). By forcing all intermediaries to record every transaction taking place on their systems or put in place other methods of tracing the originator of any information, the rule disproportionately interferes with both privacy rights of individuals and places an unnecessary cost on businesses).

We suggest therefore that the government consider amending the IT Act appropriately to bring in place differentiated obligations for different types of intermediaries based on their function, size, etc. Further, any requirements to trace messages

must comply with the norms of the Supreme Court laid out in the Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors (WP (Civ). No. 494/2012) case - notably, interferences with privacy rights must be proportionate and have sufficient procedural fetters to prevent against abuse or arbitrary application.

3.4 Rule 7

The proposed Rule 7 seeks to ensure that all intermediaries with more than 50 lakh users in India or in the list of intermediaries to be notified by the government are to:

- establish themselves as a company in India;
- have a permanent registered office in India, with a physical address; and
- appoint a person for coordination with law enforcement agencies.

We believe that the proposed Rule ought to be reconsidered for the reasons specified below.

1. *Difficulties of identifying user base:* In addition to the arbitrariness of the cut-off prescribed by the Rule, the Rule does not specifically define how the number of users of an intermediary will be calculated. The provision is therefore arbitrary and vague. Given that online services (and intermediaries) have all sorts of business models and relationships with their users, it is unclear how such a figure will be calculated in practice. For instance, a service like Facebook is primarily used by registered subscribers to post content. On the other hand, a news service, online blog or gaming service may not require subscription or even registration in order for a user to post comments. Some webservices need not have any direct commercial relationship with a user even if hosting their data or enabling access to content, while others may retain minimal or no data from users. It is therefore unclear how the varied types of services / intermediaries will calculate their number of users. It is also unclear if the number of users will be calculated as a historical total, the number of active users in a particular time period, etc.
2. *Requirement to register only as a company is arbitrary:* The requirement to register only as a company (under the Companies Act, 1956, or Companies Act, 2013) is arbitrary and serves no purpose. Intermediaries, given the wide definition in the IT Act, can take a variety of forms. These may be formed as different types of entities - for instance, a newspaper or online portal may be registered as a trust or society per Indian law. It makes little sense to force all such entities to re-form and/or register only as companies.

3. *Lack of clarity of purpose:* It is unclear what specific problem the government is attempting to solve by mandating a physical presence for all intermediaries within India. Given the absence of any explanatory statement with the draft proposal for amendment, there is no clarity on why the government wants to introduce a specific requirement of a physical presence in India. Assuming the enforcement of Indian laws as a reason, this can occur through alternative, less intrusive options - including the use of MLATs and other such mechanisms (Bailey & Parsheera, 2018). Further, many intermediaries are also under the ambit of sector specific regulation (for instance, banking and payments related intermediaries are already regulated by the Reserve Bank of India, Securities and Exchange Board of India, etc.) which already imposes necessary enforcement related requirements, including through norms of incorporation, data localisation norms, the ability of regulators to access information etc. (Bailey & Parsheera, 2018) A generic requirement for all intermediaries of a particular user base to incorporate in India is therefore an excessive and disproportionate step.
4. *Need for a differentiated approach:* The Rules do not lay down any criteria or basis of which the government can “specifically” notify an intermediary. This is likely to lead to arbitrary and capricious decisions. Given the provision appears to be aimed at targetting specific social media companies that operate in India - it may be preferable to ensure more targetted rules are put in place that incorporate a greater number of factors (than just total number of users) to consider as the basis for implementing special obligations. This may ideally be done through an amendment to the IT Act or another appropriate legislation.

In the circumstances, we suggest deleting or substantially amending the proposed Rule 7 in light of the discussion above.

3.5 Rule 9

The proposed Rule 9 requires all intermediaries to deploy technology based automated tools or appropriate mechanisms to proactively identify and remove / disable access to unlawful information and content. It is submitted that this requirement is excessive and disproportionate, will serve little practical purpose and should therefore be reconsidered for the reasons detailed below.

1. *Proactive identification and removal of unlawful online content not contemplated by enabling legislation:* Neither the IT Act nor the enabling provision for these rules i.e Section 79 of the IT Act contemplates the proactive

identification and removal of unlawful online content by intermediaries, It is therefore submitted that the proposed Rule 9 imposes new substantive obligations on intermediaries, inasmuch as it requires intermediaries to “proactively” identify and remove content. While the term has not been defined in the rules, it could mean either a requirement of pre-censorship (before the content is uploaded) or immediate takedown (before a complaint regarding the content has been made).

A requirement of pre-censorship of all online content would be particularly problematic. While the IT Act adopts the policy of requiring intermediaries to simply follow a blocking order passed by the appropriate government or a court of law, Rule 9 requires intermediaries to invest in developing and deploying automated tools capable of both screening all content posted on intermediary platforms and accurately identifying and removing unlawful online content. Therefore, it is submitted that such a new substantive obligation upon intermediaries, which is clearly a deviation from the policy adopted by the enabling legislation, should not be imposed through the Draft Rules, i.e a delegated legislation under Section 79 of the IT Act. If necessary, such a move should be proposed via amendments to the IT Act and be debated by the members of the Parliament before it is enacted.²⁹ Further, it may be noted that the amendment to Section 79 in 2008 specifically changed the section so as to remove the previous requirement of proactive screening of content. Adding such a requirement through the present rules vitiates against legislative intent and would again take us back to situations such as the *Avnish Bajaj* case described previously.

2. *Prior censorship of content may be disproportionate:* The requirement for prior scrutiny of all online content may be a disproportionate interference with privacy and expression rights of citizens. Given the possibility of intermediaries taking other kinds of action so as to limit the harm caused by online offences (for instance, through appropriate take-down processes that include requirements for judicial order, etc)., it is unclear why such an invasive method is being considered. Pre-screening of all content before it can be transmitted or published is a serious infraction of fundamental rights and therefore ought to be reconsidered. This is particularly so in the case of particular types of content such as news media - which is a perishable commodity (therefore delays in publication may deprive it of all value). It is worth keeping in mind that the European law on which Section 79 is based specifically bars the imposition of a specific duty to monitor (refer Article 15, E-Commerce Directive 2000/31/EC). This provision was examined by

²⁹Please refer to the submission under the head “Scope of subordinate legislation”

the European Court of Justice (ECJ) in *Scarlet Extended SA v. SABAM* (C-70/10, 2011), where the Court *inter alia* found that a general requirement to monitor (or an injunction that would require the respondent to ensure no further intellectual property violations on its online platform) would be unfair, disproportionate, and excessively costly.³⁰ Further, case law in Europe indicates that the standard of judicial scrutiny in case of pre-publication interferences is very high. “The provision on which the preventive measure is based must be formulated with sufficient precision to clarify the type of restrictions authorised, their purpose, duration, scope and control, and to enable the citizen to foresee the consequences of a violation of a prior restraint” (Oster, 2015).

3. *Possible concerns regarding private parties pre-screening online expression:* There may also be a concern that mandating private parties to exercise a pre-screening or pre-censorship function would imply a lack of transparency in the decision making process, and that too without any further recourse to an affected individual. Having such a private system of censorship would also take away from the signalling function of open/public adjudication, as well as the system of checks and balances inherent in our constitutional make-up. In a system as envisaged by the proposed amendment, the intermediary would act as the agency in charge of examining/catching perceived offences, making a decision to censor content, and then acting on this decision - all without a mandate to give the affected individual any hearing.

The devolution of such functions also violates the principle that delegated powers cannot be further delegated. State agencies are authorised under the relevant statutes to act to stop commission of offences in the online space. It may be argued that the proposed rule amount to a case of a State agency delegating its function of investigating and preventing online offences to private parties. One must also consider that in certain situations it is also possible that the intermediary may be an affected party (for instance, certain content may drive content to its platform). It is settled that no person should be a judge in their own cause, and accordingly, intermediaries should not be put in a position of having to decide whether certain content is legitimate and whether or not to take it down.

4. *All intermediaries may not be able to make such technical determinations:* It is not possible for an intermediary to make nuanced decisions on the commission of many offences. Often offences (such as that of copyright violation,

³⁰One may also note that the travaux préparatoires to Article 19 of the International Covenant on Civil and Political Rights - to which India is a signatory - indicate that an absolute prohibition on prior restraints on expression was intended under this provision (Oster, 2015).

distributing obscene content, etc.) require a consideration of context as well as multiple competing rights (Eg: fair use v. copyright). All intermediaries will not have the capacity or ability to make such technical determinations. This is likely to result in a scenario where it makes sense for an intermediary to be cautious and act to censor any content, leading to a chilling effect on expression rights. In the alternative, only big intermediaries with the ability to put in place big legal teams will be able to carry out business in the online space. In this context, even the Supreme Court has noted that “*the delicate task of deciding what is artistic and what is obscene has to be performed by courts and as a last resort by the Supreme Court and therefore, the evidence of men of literature or others on the question of obscenity is not relevant*” (Ranjit Udeshi v. State of Maharashtra, 1965 AIR 881).

5. *AI can be an imperfect solution:* It is submitted that while AI and machine learning tools may prove helpful in some contexts, not only they are they still imperfect (by way of example, AI still struggles with understanding humour or sarcasm³¹) putting in place a requirement for all intermediaries to apply such tools is impractical and likely to severely hamper the business of small and medium enterprises who may not have the ability to comply with this obligation in the same way as the bigger companies such as Google and Facebook. There is also considerable literature on the inherent biases of algorithms and automated tools (including the possibility of overbroad or mistaken censorship by automated tools). The reliability, accuracy and biases of AI based tools (and the effects on society of relying on such tools) must be considered when making it mandatory for such tools to be deployed. There is also the issue of transparency and accountability of such mechanisms. Public adjudication serves a specific democratic function under our constitutional scheme and this cannot be shortcircuited through the imposition of the kind of obligations under the proposed Rule 9.

If the automated tools requirement is considered to be a form of private policing of online speech, the requirement of automated tools (like machine learning or AI) would amount to use of technological tools to make decisions reserved for the State. Further, given that the proposed Rule 9 lays down no standards for the functioning of the AI / machine learning tool, different intermediaries will utilise different types of tools that may lead to different and arbitrary results. Will the question of liability then be determined based on the technical standard or efficiency of the tools or the capacity of the intermediary in questions? For instance, would it amount to differential standards for a small local intermediary versus large players with greater

³¹(Spivack, 2016); (Deign, 2018)

capacity?

3.6 Rule 12

Rule 12 permits any individual “who suffers as a result of access or usage of computer resource by any person in violation of rule (3)” to contact an intermediary to complain about the content. The Grievance Officer appointed by the intermediary is required to resolve the complaint within one month. This in practice will presumably imply that the offending content should be censored / taken down (in addition to any other action deemed suitable) following a determination of its legality by the intermediary. This will therefore require the Grievance Officer of an intermediary to scrutinise every complaint received, apply her mind to the matter and make a determination of whether the content complained of violates the (extremely broad and ambiguous) terms used in Rule 3.

It is submitted that such a scheme - of permitting censorship/take-downs by an intermediary upon receiving requests from the public was expressly barred by the Supreme Court in *Shreya Singhal*. In the said case, the Supreme Court held that the only two ways in which online content could be taken down by an intermediary would be subsequent to appropriate orders of an authorised government agency or a court. Intermediaries cannot be required to take-down content subsequent to a private complaint.

In this context it is important to remember that Section 79 is not intended to act as a provision that grants substantive rights of censorship to an intermediary or for that matter any member of public. The IT Act does not envisage intermediaries acting as private police or a pre-publication online censorship wing of the government. As recognised in paragraphs 116 and 117 of *Shreya Singhal*, not only are intermediaries not supposed to apply their own mind to whether content should be blocked or not, they cannot be expected to do so as it would be exceedingly difficult for them to act on the millions of requests made and to judge which requests are legitimate or not.

Therefore, by enabling private complaints flowing from Rule 3 to be made under Rule 12, the Rules go well beyond both the law laid down by the Supreme Court of India and the language/intent of the parent enactment itself.

Further, a notice and take-down mechanism as envisaged under the Rules would render the blocking mechanism prescribed under Section 69A, IT Act otiose/superfluous.³²

³²The rules under Section 69A of the IT Act (the IT (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009, allow “any person” to make a complaint in

This was one of the primary reasons behind the Supreme Court reading down the “actual knowledge” provision in Section 79 in the *Shreya Singhal* case. In some cases alternate remedies are already available. For instance, given the existing censorship options available under the IT Act, it is clear that a new, backdoor method of censorship (Rule 3(2)) cannot be introduced through the means of subordinate/delegated legislation.

Finally, the proposed take-down mechanism under Rule 12 read with Rule 3, fails to provide for any hearing to an affected party (who disagrees with a complaint made, and the subsequent take-down of content by the intermediary). The system also lacks the safeguards present in the take-down system implemented under the Copyright Act and rules thereunder - notably the absence of a put-back provision in the event of a failure (by the complainant) to produce a relevant court order within a specified time period.³³

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

respect of online content to nodal officers appointed by the government. Thereafter, the rules provide for an application of mind by the relevant government agencies/authorities before the intermediary is informed of the specific content that needs to be blocked.

³³Section 53 and Rule 75 of the Copyright Rules, 2013 establish a notice-take down mechanism in the context of copyrighted content, which requires the intermediary to take down purportedly illegitimate content after receiving a complaint from a rights holder. The complainant is thereafter required to produce a relevant court order mandating take down of the content, within a period of 21 days from making the initial complaint. A failure to produce the court order means the content can be restored by the intermediary.

References

- Aneeta Hada v. Godfather Travels. (Cr. A. No. 838/2012). Supreme Court of India.
- Avnish Bajaj v. State of Delhi. (116 (2005) DLT 427). High Court of Delhi.
- Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018, August). Use of personal data by intelligence and law enforcement agencies. Retrieved from <https://bit.ly/2CEzCoN>
- Bailey, R. & Parsheera, S. (2018, October). Data localisation in india: questioning the means and ends. *NIPFP Working Paper 242*. Retrieved from <https://bit.ly/2R8Q8IW>
- Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017, September). An analysis of puttaswamy: the supreme court's privacy verdict. *Law, Economics, Policy Blog*. Retrieved from <https://bit.ly/2Mxb3Pi>
- Bhatia, G. (2016). Blasphemy law and the constitution. Retrieved from <https://bit.ly/2U95qJy>
- Consumer Policy Research Centre. (2018). *Australian consumers soft targets in big data economy*. Retrieved from <https://bit.ly/2wvd87q>
- Court, G. H. (AIR 1971 Gau 110). Prabir kumar basu v. dto, darrang.
- Deign, J. (2018, August). Can artificial intelligence understand humour? *The Financial*. Retrieved from <https://bit.ly/2SggXt7>
- Germany. (2017). The network enforcement act (netzdurchsetzungsgesetz, netzdg). Retrieved from <https://germanlawarchive.iuscomp.org/?p=1245>
- Guggenberger, N. (2018, February). Netzwerkdurchsetzungsgesetz. *Stanford CIS World Intermediary Liability Map*. Retrieved from <https://wilmap.law.stanford.edu/entries/network-enforcement-act>
- Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors. (WP (Civ). No. 494/2012). Supreme Court of India.
- Keller, D. (2018). Internet platforms: observations on speech, danger, and money. *Hoover Institution Essay, Aegis Series Paper No. 1807*. Retrieved from <https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money>
- Kosseff, J. (2017, June). Twenty years of intermediary immunity: the us experience. *scripted*. Retrieved from <https://ssrn.com/abstract=3225773>
- Leary, M. G. (2018). The indecency and injustice of section 230 of the communications decency act. *Harvard Journal of Law & Public Policy*, 41. Retrieved from <http://www.harvard-jlpp.com/wp-content/uploads/2018/03/LEARY-FINAL.pdf>
- Map, S. C. W. I. L. (1998). Digital millennium copyright act 1998, 17 u.s.c. section 512. Retrieved from <https://wilmap.law.stanford.edu/entries/digital-millennium-copyright-act-1998-17-usc-ss-512>

- McDonald, A. & Cranor, L. (2008). The cost of reading privacy policies. *I/S: A journal of law and policy for the information society*, 4(3), 543-568. Retrieved from <https://bit.ly/1qbLQJ9>
- McIntyre v Ohio Elections Commission. (No. 93-986, 1995). United States Supreme Court.
- Children's Online Privacy Protection Rule. (2013). Retrieved from <https://bit.ly/2SnntyB>
- Oster, J. (2015). *Media freedom as a fundamental right*. Cambridge University Press.
- Parliamentary Standing Committee. (2007). *Report on the information technology (amendment) act, 2006*. Retrieved from <https://bit.ly/2DFqv9f>
- Ranjilal Modi v. State of UP. (1957 AIR 620). Supreme Court of India.
- Ranjit Udeshi v. State of Maharashtra. (1965 AIR 881). Supreme Court of India.
- Scarlet Extended SA v. SABAM. (C-70/10, 2011). European Court of Justice.
- Sharat Babu Digumarti v Govt. of NCT of Delhi. (Cr. A No. 1222/2016). Supreme Court of India.
- Shreya Singhal v. Union of India. (WP (Cr). No. 167/2012). Supreme Court of India.
- Solove, D. (2013). Privacy, self management and the consent dilemma. *Harvard Law Review*. Retrieved from <https://bit.ly/2RHEVOA>
- Spivack, J. (2016, December). A robot walks into a bar: the limits of ai and semiotics of humour. *Georgetown University Blog*. Retrieved from <https://bit.ly/2HJCNkN>
- Supreme Court of India. (CA No. 3359/1997). Agricultural Market Committee vs. Shalimar Chemical Works Ltd.
- The Internet Society. (2012). *Global internet user survey, 2012*. Retrieved from <https://bit.ly/2whTrQx>
- Zuckerberg, M. (2018). A blueprint for content governance and enforcement. Retrieved from <https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/>

S.No	Ref. No.	Comments
60	MIT/79/060	<p>Sirs,</p> <p>In response to the invitation for comments and suggestion from all relevant stakeholders on theDraft of the Intermediary Guidelines 2018, we wish to submit the following:</p> <ol style="list-style-type: none"> 1. That we work in the area of free speech and seek to safeguard freedom of expression in India. 2. That we wish to place on record our grave apprehensions that the proposed changes to the Intermediary Guidelines, taken in its entirety, will seriously impair freedom of expression in India. 3. That the draft guidelines propose an incorporation clause for more than 50 lakh users and several internet companies may be forced to disconnect from India as a result. This will inevitably cause an ‘islanding’ of India and cut off its citizens from a vast repository of knowledge and information available to all citizens. It will put an end to the access Indian citizens have to the world wide web and further exacerbate the digital divide, not just within India but also between Indian citizens and the world. 4. That it is also unfortunate and ironic that, on the one hand, the Indian government seeks to bring in a digital India and on the other, makes it difficult for companies to function here freely and fairly. 5. That the draft guidelines prescribing due diligence will result in pre-censorship of content. In addition, these provisions are vague and arbitrary and an attempt to bring back the provisions of Sec 66 (a), which had been struck down for being unconstitutional in the Shreya Singhal judgement. To incorporate this again into these draft guidelines for intermediaries is an attempt to bring back the draconian provisions of Sec 66 (A) and all its attendant violations of free speech. 6. That the rationale for the draft guidelines seems to be to curb fake news and ensure the accountability of social media platforms to the law. But both issues will not be served by these draft Information Technology (Intermediary Guidelines) Rules 2018. Indeed, every transparency report by major social media platforms have disclosed that the Indian government has made the highest number of requests for disclosure of accounts, for data, for takedown of content and blocking of sites. In this context, any further changes will only serve to strengthen already existing provisions without any guarantee that

The Global Network Initiative's Submission on the Draft Amendments to the Information Technology (Intermediaries Guidelines) Act

The Global Network Initiative (GNI) welcomes the opportunity to provide input to the Indian Ministry of Electronics and Information Technology (MeitY) on the draft amendments to Information Technology (Intermediaries Guidelines) Act. We appreciate that MeitY is consulting openly with affected companies, civil society, and other experts.

GNI is concerned the amendments, as drafted, would place significant pressure on a wide range of information and communications technology (ICT) companies to monitor users' activities, remove content, and hand-over data in ways that could unnecessarily and inappropriately impact users' freedom of expression and privacy. Given the potential significance of the concerns articulated below, which are shared across GNI's wide membership of leading experts from civil society organizations, academia, ICT companies, and the investor community, we encourage MeitY to reconsider these amendments.

About GNI

GNI is the world's preeminent multi-stakeholder collaboration in support of freedom of expression and privacy online. GNI's members include leading academics, civil society organizations, ICT companies, and investors from across the world. All GNI members subscribe to and support the GNI Principles on Freedom of Expression and Privacy ("the Principles"), which are drawn from widely-adopted international human rights instruments. The Principles, together with our corresponding Implementation Guidelines, create a set of expectations and recommendations for how companies should respond to government requests that could affect the freedom of expression and privacy rights of their users. The efforts of our member companies to implement these standards are assessed by our multi-stakeholder board every other year.

GNI encourages governments to be specific, transparent and consistent in the demands, laws and regulations that impact freedom of expression or the right to privacy, including restrictions of access to content, restrictions of communications, and demands that are issued regarding privacy in communications.

GNI's Work on Intermediary Liability in India

GNI members have been investing in, researching, engaging in, and contributing to the ICT sector in India since 2012. In March 2012, GNI co-organized a multi-stakeholder roundtable with the Centre for Internet & Society called "India Explores the Balance Points between Freedom of Expression, Privacy, National Security and Law Enforcement." This event brought together representatives from government, industry, civil society, and academia and provided important insights that were captured in the subsequent report, "[Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online](#)." GNI has also previously submitted comments to the Law Commission of India's Consultation on Media Law in August 2014.

At the behest of our membership, GNI commissioned a report, published in 2014, "Closing the Gap: Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose," which found that online platforms that support user-generated content can become an important part of India's Internet economy and contribute approximately INR 2.49 lakh crore (USD 41

Billion) by 2015—in addition to the contribution of other elements of the Internet economy. Additionally, the positive productivity effects of online intermediaries were found to be significant, creating an even greater impact in India in areas like e-sales and e-procurement compared to their impact in Europe or the United States. The report highlighted the cases of local companies who had suffered due to uncertainty related to legal liability in India.

A year after that report was published, it was cited in briefings in the *Shreya Singhal v Union of India (2015 SCC 248)* litigation, which resulted in a landmark decision by the Supreme Court of India clarifying intermediary liability under Section 79 of the IT Act. GNI appreciates that the proposed amendments to the Intermediary Guidelines may be intended, in part, to codify and clarify the implications of that ruling. However, we are concerned that the proposed amendments are so vague and potentially broad in several places that they actually have the opposite effect.

Arbitrary Time-Periods

The proposed amendments to Rule 3(5) of the Guidelines introduce a new 72-hour time-period for providing “information or assistance” in response to requests from “any government agency,” and the newly proposed Rule 3(8) allows the “appropriate Government or its agency” to issue removal orders to companies requiring they remove content, deemed illegal under the proposed regulation, within 24 hours from receipt of the order. According to the GNI Principles, members are expected to “interpret government restrictions and demands, as well as governmental authority’s jurisdiction, so as to minimize the negative effects on freedom of expression.” These arbitrary and rapid timelines will create significant challenges for appropriate review of removal orders. In addition, the potentially significant legal penalties for noncompliance will put increased pressure on companies to comply with these orders.

While we appreciate the Indian government’s interest in ensuring prompt action in response to legal orders, we would note that most large platforms already act expeditiously in response to clear orders appropriately issued from duly empowered government authorities. There are nevertheless instances when such orders may be incomplete, issued inappropriately, or are overly broad. It is important that companies are allowed to review orders and seek clarity, where appropriate, in order to avoid unnecessarily impacting user rights. This is especially important considering that, if content is removed or user data improperly shared, it may take a substantial amount of time and effort for appropriate redress to take place, if it can take place at all.

Automated Proactive Content Filtering

Rule 3(9) of the Draft Rules, by requiring intermediaries to actively monitor and filter content, transforms them from neutral providers of access to services into censoring bodies. Intermediaries are likely to err on the side of over-censoring the content shared on their platforms in order to comply with this rule. This over-censoring in fear of repercussions under the IT Act will lead to a chilling effect on the freedom of speech and expression of the users in India, who will face a contraction in their ability to share views and content online.

In particular, we are concerned about the language in Rule 3(9) that requires intermediaries to deploy “technology-based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful

information or content.” Broad applications of automation should be carefully weighed against the risks such tools pose to freedom of expression. As GNI civil society member Center for Democracy and Technology (CDT) pointed out in a [recent publication](#), companies and policy makers should recognize the limitations of such technological tools in deciphering nuance and context of text-based human communication.

GNI does not believe that governments should mandate the use of filters or other automated content evaluation tools in laws regulating speech. If companies decide to use automation to facilitate content moderation, they should do so in a transparent, accountable manner, while maintaining an appropriate degree of human review. The process of deciding what content is addressed using automated tools, which tools are used and how, and the extent and scope of human review, should be carefully thought through in an open, transparent, participatory manner involving relevant stakeholders, so as to minimize potential human rights impacts.

Definitional Challenges

In its amended form, the Guidelines provide very limited definitional clarity as to which government agencies are appropriately empowered to exercise the various authorities related to user data requests and content removal. In addition, there is little clarity as to the content which might qualify for removal according to clauses (a) through (k) under Rule 3(2). In addition, we are concerned that some items on the list of prohibited content may fall outside of Section 19(2) of the Constitution, raising questions about the extent to which the amended Guidelines conform to the requirements in the Supreme Court’s *Shreya Singhal* decision.

In addition, Rule 3(8) requires intermediaries to remove or disable access to unlawful acts as required by court order or by the appropriate Government or its agency. However, this provision formulates no checks and balances to ensure that this power is used sparingly and in a just manner. The provision also mandates storage of such information and associated records for a longer period of 180 days and even authorizes this period to be lengthened. Yet the provision does not formulate sufficient safeguards to ensure that the power to extend retention of data is used by government agencies in a fair, transparent and sparing manner. For all of these reasons, Rule 3(8) may fail the constitutional requirement of due process, and should be deleted from the Draft Rules.

These definitional issues are likely to lead to legal uncertainty, as well as potentially overly-aggressive interpretations by companies that could result in the removal of content which would infringe on the users freedom of expression. In addition, the proposed amendments to Rule 3(5) requiring intermediaries to “enable tracing out of such originator of information on its platform as may be required by government agencies” creates a vague and potentially broad new obligation that could have significant impacts on user privacy. The tracing of originators without sufficient limitations and safeguards would constitute a violation of users’ right to privacy, and will affect the way that people use the Internet in India. In addition, it is important for MeitY to evaluate the technical limitations in terms of implementing and enforcing such an obligation on intermediaries.

Incorporation Requirement

There are stringent requirements for companies with more than 50 lakh users to incorporate locally and have a permanent registered office per clauses (i) and (ii) of Rule 3(7).

Additionally, companies are required to appoint legal points of contact and alternates “for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.” This constitutes a highly onerous obligation on international companies who provide services globally but do not find it feasible to incorporate in every country of operation. It would also affect the Internet users’ online experience by limiting the online services available in India. The lack of clarity as to how MeitY will determine the number of Indian users of any given company, as well as the possibility that the Government of India can also arbitrarily add companies to this list, poses particular challenges for small and medium-sized enterprises in particular who may not have resources to establish a permanent office in India, or may lack the infrastructure to deal with the 24/7 requests and properly assess related human rights impacts. The impact of these aspects of the amendments may be to discourage such companies from potential business opportunities at the cost of compliance with the Guidelines. These requirements are likely to lead to further balkanization of the Internet and have an adverse impact the economic potential of, as well as the digital integration in, India.

Conclusion

As noted above, the proposed amendments raise significant issues that must be addressed before they are enacted into law. At a minimum, amendments should: (i) ensure key provisions, such as the definitions of illegal content and appropriate authorities are refined and clarified; (ii) allow for appropriate company review of and, where appropriate, legal challenges to content removal or user-data request orders; (iii) eliminate, or significantly limit, situations where companies will be ordered, expected or encouraged to implement “proactive measures”; and (iv) revise and clarify provisions under which companies will be expected to designate legal entities for 24/7 coordination with local enforcement agencies.

GNI recognizes the importance of taking measures to prevent the dissemination of illegal content online and stands ready to continue engaging with relevant actors, including MeitY, to ensure that our collective efforts to address this challenge remain effective, efficient, and consistent with applicable human rights principles.

Comments on “The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, Draft, V1.0” by India Internet Foundation (IIFON)

India Internet Foundation (IIFON) is honoured to be part of the public consultation process initiated by MeitY on Draft of Intermediary Guidelines 2018. It is indeed a time warranted change and IIFON supports the spirit of changing the guidelines. At the same time IIFON believes that more specifics are required while drafting new guidelines by taking into consideration the technical developments in pipeline or already done which has a potential impact on the proposed guidelines.

IIFON constituted a team of experts to look into the draft guidelines from IIFON trustees and ISOC Kolkata Chapter leadership and after deliberation the team feels that a revisit by MeitY on the rules mentioned below will be highly beneficial.

1. Rule (5) of the Diligence guidelines specifies that the Intermediary has to produce/ track the source of any objectionable content on demand from the respective state authorities. However, end-to-end encrypted messaging services like WhatsApp by design practice the “right-to-forget” at the server itself. It is claimed by these services that in such case the server is not aware of the content being forwarded through it. Neither the content, nor the ephemeral session keys are available with messaging server. Given this scenario, how does the authority enforce the laws effectively? The matter should be dealt with more technological insight into the systems in vogue. This may impact the core design of the protocols of these messaging services involving third-party. It is also not clear whether a Third-party has to validate these features with the authorities to start/ continue its functioning. It is not clear, what happens if the third-party deploys a technology that puts hindrances in satisfying such requirements. Hence, in the backdrop of the above, it is requested to revisit the concerned proposed rule once again.
2. Rule (7) may not be a suitably strong condition to exercise liability clauses on the third-party. The issue is, it is not clear to what extent the nodal agency will be responsible to cater the demands of Indian authorities. Furthermore, if the operational server is in foreign geography, it needs to be clearly understood whether a nodal office be sufficient enough to hold responsible and accounted for any mishap. The prime consideration in such a scenario (third party server in foreign geography and a nodal agency is in India) is whether the Indian authorities will be able to force the nodal agency to provide the required leads (session information, user credentials, information content etc.) available in the server residing in foreign geography. Hence, in the backdrop of the above, it is requested to revisit the concerned proposed rule once again to avoid leaving open any potential escape path while the state is in crisis.

3. Rule (9) may be too much to ask from the intermediaries. The text in the draft has already emphasized the non-human-in-the-loop operation where all storing and forwarding is automated. Given the present state of machine intelligence, it may be non-trivially hard for the intermediaries to specifically classify all the contents that may be deemed as unsuitable by the authorities. Especially, preventing spread of fake information about some entity or facts automatically may not be an easy clause to oblige. (In many cases, there may not be enough contents in the web to check and decide on the legitimacy of information being spread.) However, it may be possible in certain cases of obscenity, etc. Enforcing this clause may portray a wrong message. Note that, the intermediary is neither the generator of those messages, nor has an active role in the generation process. Intermediaries may feel that the responsibility regarding failure to prevent a social engineering evil is being passed to them. This may impact image of the state in international arena and also in terms of Indian interaction with the international business.

Thanks once again for the opportunity to comment and share our views.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Comments on
“Draft Information Technology
[Intermediaries Guidelines (Amendment) Rules], 2018 ”

Executive Summary

- I. The objective of the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (“the Draft Rules”) seems to be to counter disinformation / fake news on social media and messaging platforms (among other things like – circulation of obscene content and recruitment of terrorists). However, the Draft Rules have exceeded the power of delegated legislation and are violative of the fundamental rights to free speech and privacy.
- II. The obligations of intermediaries need to be classified based on their roles and their control over content. Mere conduits like TSPs cannot have the same obligations as a social media platform.
- III. The Draft Rules have gone against the dictum of the judgment of the Supreme Court in *Shreya Singhal v Union of India*. The broad list of information characterized as “unlawful” provided in Sub-Rule 2 of Rule 3 has terms and expressions that are vague and ambiguous and would result in violating the right to Freedom of Speech and expression of a citizen as guaranteed by the Constitution.
- IV. Restrictions on content/ speech cannot be beyond what is laid down in Art.19(2) of the Constitution. It was held in *Shreya Singhal* that “*Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79*”. Thus, the rules cannot mandate restrictions on content beyond those enumerated under Art.19(2) of the Constitution.
- V. Proactive monitoring of content is in effect a mandate on the intermediary to decide on the legitimacy of any content posted by a third party and this is violative of the fundamental right to freedom of speech and expression.
- VI. Traceability cannot be mandated as per these Rules as it is beyond the rule making power of the Government. No steps should be taken that violates the right to privacy of citizens and affects the security of users. Requirement of monthly notification will result in excessive communication from intermediaries to users and lead to consent fatigue.

We fear that the rationale for these proposed amendments to 'strengthen the legal framework and make the social media platforms accountable under the law', in the light of the spread of fake news, will not be served by such arbitrary and sweeping provisions. We request you to protect the principles of open and accessible internet, safe harbour granted to intermediaries and the fundamental rights of privacy and freedom of speech and expression of the internet users in India.

While being cognizant of national security interests, we appeal for a less-invasive and proportional means of regulation of the internet.

Summary of Recommendations

- One size fits all approach for regulation of intermediaries is problematic and the obligation of intermediaries should be dependent on their role and the control that they have over content
- Intermediaries should be free to come out with their own Terms of Service and the content of such terms should not be mandated. Any restriction on content should not go beyond those laid out under Article 19(2) of the Constitution.
- The intermediary should not be required to actively monitor posted content using automated tools or any other mechanism.
- The intermediary should not be mandated to determine on its own whether any given content is legal or not.
- Fundamental right to privacy of users have to be protected and there should not be any mandate to weaken the encryption of communication tools.
- Traceability of user goes beyond the rule making power of the Government and cannot be mandated.
- Safeguards guaranteed under Section 69A should not be violated by these Draft Rules.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Comments in Detail

The Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (“the Draft Rules”), were issued by the Ministry of Electronics and Information Technology (“MeitY”) on the 24th of December, 2018. The Draft Rules seek to amend existing ‘due diligence’ guidelines [The Information Technology (Intermediaries Guidelines) Rules, 2011 (“the Current Rules”)] which are to be followed by ‘intermediaries’ [as per the Information Technology Act, 2000 (“IT Act”)]. Section 79 of the IT Act provides for a safe-harbour to intermediaries for, “*any third party information, data, or communication like made available or hosted by him*”. Intermediaries are required to observe due diligence while discharging their duties under the IT Act and observe guidelines as laid down by the Central Government.¹

In a press note issued by MeitY,² it has been mentioned that social network platforms are required to follow due diligence as provided in Section 79 of the IT Act and the Rules notified therein, subject to the import of Article 19(2) of the Constitution. They have to ensure that their platforms are not used to commit and provoke terrorism, extremism, violence and crime. The press note also states that instances of misuse of social media platforms by criminals and anti-national elements have brought new challenges to law enforcement agencies, such as inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, incitement of violence, public order, fake news etc. The press note points to fake news / rumours being circulated on WhatsApp and other social media platforms for various mob-lynching incidents reported across India in the last year - “*A number of lynching incidents were reported in 2018 mostly alleged to be because of Fake News / rumours being circulated through WhatsApp and other Social Media sites.*” As MeitY has not issued any other official statement behind their intent in revising the intermediaries guidelines under the IT Act, the Draft Rules will have to be read in conjunction with the press note for a critical examination of the proposed changes therein.

Section 79 of the Act was introduced to provide a “safe harbour” for intermediaries to protect them from liability on account of user generated content. However, the Draft Rules could result in eroding this safe harbour. The Rules would have implications on social media and messaging platforms as well as community run platforms like Wikipedia and Diaspora. The Draft Rules in their current form could also have a chilling effect on free speech and infringe the privacy rights of

1 Section 79(2)(c) of the IT Act, 2000.

2 The press note issued by MeitY, available at <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>. Last accessed on 27 January 2019

citizens.

A. Obligation on Intermediaries remains same irrespective of roles

At first instance, it is important to highlight the definition of the term ‘intermediary’ as per the IT Act, as the Draft Rules are applicable to only this category of service providers. Section 2(1)(w) of the IT Act defines an intermediary as - “with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.” On a careful reading of the definition, it is clear that the following service providers are intermediaries as per the IT Act: (a) all social media platforms; (b) messaging services; (c) e-commerce marketplaces; (d) telecom and Internet service providers; (e) search engines; (f) web-hosting services; (g) online payment sites; and (h) cyber cafes (this is an indicative list and not an exhaustive list). All these service providers will be required to abide by the provisions of the Draft Rules as they are intermediaries as per the IT Act.

Most of the changes proposed by the Draft Rules, such as monthly notification requirement;³ traceability of originator of information;⁴ take down of content and preservation of information;⁵ and deployment of automated tools for disabling content;⁶ seem to be targeted toward a select group of intermediaries - social media platforms and messaging applications. This becomes clearer when read alongside the press note issued by MeitY on the Draft Rules.

The above listed requirements, by their very logic, don’t apply to other categories of intermediaries such as telecom service providers (“TSPs”), Internet service providers (“ISPs”), web hosting service providers and cyber cafes. Application of the Draft Rules to such intermediaries is disproportionate and doesn’t serve the purpose for which these changes are being introduced. This is one of the major concerns with incorporating requirements such as traceability of originator and proactive filtering of unlawful content within the Intermediaries Guidelines under the IT Act. Making the safe-harbour protection of certain intermediaries (like TSPs, ISPs and cyber cafes) conditional on requirements which they cannot adhere to is contrary and counter productive.

3 Rule 3(4) of the Draft Rules

4 Rule 3(5) of the Draft Rules

5 Rule 3(8) of the Draft Rules

6 Rules 3(9) of the Draft Rules

We recommend that MeitY should first identify the categories of intermediaries that the Draft Rules would apply to (such as social media platforms and messaging services) and then create separate conditions for distinct categories, so as not to have a blanket requirement for all intermediaries. As established, the definition of ‘intermediary’ is wide in its ambit. Due to the differences in the way that these unrelated intermediaries function, a one-size-fits-all approach to their regulation will lead to excessive regulation without appreciating the context of their operation. We recommend that the Draft Rules be tweaked to clarify the categories of intermediaries that different provisions would apply to, so that the guidelines become more coherent and consistent with the different roles played by dissimilar intermediaries in the digital sphere.

For an example of a regime which prescribes separate conditions for intermediary safe harbour based on the role the intermediary, we can look at EU’s Directive on electronic commerce (Directive 2000 / 31 / EC of the European Parliament and the Council).⁷ Section 4 under Chapter II of the EU e-commerce directive prescribes conditions for the liability of intermediary service providers. Different conditions are applicable to distinct categories of intermediaries according to their functions. These are: intermediaries who are:

1. ‘mere conduits’: a service provider which merely provides access to a communication network (TSPs, ISPs and Web Hosting Service Providers);
2. engaged in caching services: intermediaries who temporarily store information for the sole purpose of making more efficient the information's onward transmission to other recipients of the service; and
3. providing hosting services: intermediaries who store information at the request of the recipient of service (social media platforms, online payment sites, market-places etc.).

According to the EU Directive on e-commerce, hosting service providers are liable only when they have actual knowledge of illegal activity or information and do not expeditiously remove content on obtaining such knowledge. This requirement doesn’t apply to providers of caching services and those that are mere conduits. In effect, conditions applicable to TSPs, ISPs and Web Hosting Service Providers for their safe harbour are not the same as those applicable to Social Media or Messaging Applications.

Regulations meant to make social media platforms and online communication applications more accountable for the information circulated on their services should not impose arbitrary conditions on all intermediaries in the digital realm. Doing so would result in an incoherent regulatory regime.

⁷ The EU Directive on electronic commerce, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN>. Last accessed on 27 January 2019.

Appreciating the distinct roles played by various intermediaries in the online space, categorization of intermediaries based on their functions is the need of the hour.

B. Ambiguous and vague terms

The Draft Rules contain mandates regarding a broad category of content that is classified as unlawful. Such a broad category of content described using terms such as “grossly harmful”, “harassing” and “blasphemous” could result in a chilling effect with intermediaries being forced to remove even lawful content. The Hon’ble Supreme Court had struck down Section 66A of the IT Act in *Shreya Singhal v Union of India*, (2015) 5 SCC 1.⁸ However, terms used in Section 66A such as “grossly harmful” and “harassing” are still used in the Draft Rules. The Hon’ble Supreme Court held that “Section 66A is unconstitutionally vague” The Draft Rules have persisted with the same terminology that was found to be flawed by the Supreme Court and have thus ignored the dictum of the judgment.

The Hon’ble Supreme Court held that “It is obvious that an expression of a view on any matter may cause annoyance, inconvenience or may be grossly offensive to some. A few examples will suffice. A certain section of a particular community may be grossly offended or annoyed by communications over the Internet by “liberal views” such as the emancipation of women or the abolition of the caste system or whether certain members of a non proselytizing religion should be allowed to bring persons within their fold who are otherwise outside the fold. Each one of these things may be grossly offensive, annoying, inconvenient, insulting or injurious to large sections of particular communities and would fall within the net cast by Section 66A. In point of fact, Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the Section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total.”⁹ Use of vague and ambiguous terms in the Draft Rules will lead to a chilling effect on free speech.

C. Violation of Right to freedom of speech and expression

Article 19(1)(a) of the Constitution of India provides citizens the right to freedom of speech and expression. The broad set of unlawful material as listed in sub rule (2) of Rule 3 of the Draft Rules

⁸ Available at <https://indiankanoon.org/doc/110813550/>. Last accessed on 29 January 2019.

⁹ Paragraph 83 of *Shreya Singhal v. Union of India* [(2015) 5 SCC 1].

could restrict this freedom to a great extent.

The Hon'ble Supreme Court has held in *Express Newspapers (Private) Ltd. and Anr. Vs. The Union of India (UOI) and Ors. AIR 1958 SC 578* that if any limitation on the exercise of the fundamental right under Art. 19(1)(a) does not fall within the four corners of Art. 19(2), it cannot be upheld. The Hon'ble Court further held that there can be no doubt that freedom of speech and expression includes freedom of propagation of ideas.

In *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors (1995) 5 SCC 139*, the Hon'ble Supreme Court held that:

“Article 19(1)(a) not only guarantees freedom of speech and expression, it also protects the rights of an individual to listen, read and receive the said speech”.

The automated removal of content created by a user is a clear restriction of this freedom of speech and expression and can only be done if it falls under reasonable restrictions imposed under Art. 19(2) of the Constitution. Hence the broad list of information as listed in Sub-Rule (2) of Rule 3 characterized as unlawful is ultra vires of the Constitution of India.

D. The Draft Rules are beyond the rule making powers of the Government

Central Government obtains the source of power to issue these rules from the provisions of the IT Act. The rule making power has to be strictly confined to the boundaries specified as per the Act and cannot result in expanding the scope of the Act. Chapter XII of the IT Act (as amended) provides exemption from liability of intermediaries in certain cases. This exemption is subject to certain conditions to be observed by the intermediaries. The Government obtains the source of power to issue these rules from two provisions of the Act :

Section 79(2)(c) requires the intermediary to observe “*due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.*”

Section 87(2)(zg)– states that rules may provide for “*the guidelines to be observed by the intermediaries under sub-section (2) of section 79*”

Thus the rule making power of the Central Government is limited to prescribing other guidelines in this behalf. These guidelines can only be related to “due diligence” to be observed by the intermediary while discharging its duties under the Act.

The duties of an intermediary under the Act are restricted to the following:

1. Under Section 67C of the IT Act, the intermediary is required to “*preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.*”
2. Section 69 of the Act contains the power to issue directions for interception or monitoring or decryption of any information through any computer resource. Under Section 69(3), “*The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1) extend all facilities and technical assistance to—*
 - (a) *provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or*
 - (b) *intercept, monitor, or decrypt the information, as the case may be; or*
 - (c) *provide information stored in computer resource.*”
3. Section 69A of the IT Act contains provisions for blocking public access of any information through any computer resource. Under this Section, the intermediary is required to comply with such directions issued by “*the Central Government or any of its officers specially authorised by it in this behalf*”.
4. Section 69B of the IT Act contains provisions for monitoring and collecting traffic data or information through any computer resource for cyber security. Section 69B(2) states that “*The intermediary or any person in-charge of the computer resource shall, when called upon by the agency authorised, provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.*”

The Central Government can prescribe guidelines only in respect of the above duties of the intermediaries. But these rules have widened the scope of the IT Act by legislating on information that can be posted by a user and listing a broad category of information that can be considered as unlawful. This is not connected to the duties to be discharged by the intermediaries under the Act in any way. Sub-rules (2) and (7) of Rule 3 of the Draft Rules go beyond controlling intermediaries and result in controlling the users who post content.

The Hon'ble Supreme Court has held in *State of Karnataka and Anr. Vs. Ganesh Kamath and Ors.* (1983) 2 SCC 40 that:

“it is a well settled principle of interpretation of statutes that the conferment of rule-

making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent there with or repugnant thereto”.

The Hon'ble Supreme Court has held in *Agricultural Market Committee Vs. Shalimar Chemical Works Ltd. (1997)5 SCC 516* that:

“The delegate which has been authorised to make subsidiary Rules and Regulations has to work within the scope of its authority and cannot widen or constrict the scope of the Act or the policy laid down thereunder. It cannot, in the garb of making Rules, legislate on the field covered by the Act and has to restrict itself to the mode of implementation of the policy and purpose of the Act.”

In view of the law as laid down in the aforementioned judgments, the Central Government has acted beyond its powers vested by the IT Act in framing the Draft Rules.

The rule making power of the Central Government is limited to due diligence of the intermediary **while discharging his duties under this Act** and also prescribing other guidelines **in this behalf**. These guidelines can only be related to “due diligence” to be observed by the intermediary while discharging its duties under the Act. But the Draft Rules have widened the scope of the Act by listing a much broader list of information that can be considered as unlawful. The definition of “due diligence” should be limited to having a policy, enforcing that policy and expeditiously removing infringing material when ordered by a court of law or the appropriate government.

E. Burden on the intermediary

The Draft Rules try to broaden the scope of the IT Act by placing burdensome obligations and restrictions on the intermediaries to proactively monitor user generated content which is not warranted by the IT Act. As provided in Sub-Rule 9 of Rule 3, the intermediaries have to deploy tools for removing unlawful content. Thus, the rules purport to burden the intermediaries with the obligation of deciding the unlawfulness of any content posted online, thereby according a judicial role which could only be done by a competent court. The Act specifies offences in the nature of civil as well as criminal offences. These have to proceed before the concerned forum. The intermediary cannot be burdened with a policing effort.

The Draft Rules have in effect tried to circumvent the *Shreya Singhal* judgment, wherein the Court read down Section 79(3)(b) and Rule 3(4) of the Information Technology (Intermediaries

Guidelines) Rules, 2011, interpreting the actual knowledge requirement to only mean a court order and/ or an order by the appropriate government or its agency, which must strictly conform to the standards laid down in Art. 19(2) of the Constitution. The automated system replaces the notice and take down requirement from the 2011 Rules that was read down with an automated system in respect of a broad set of unlawful information.

F. Privacy of users and traceability

Rule 3(5) of the Draft Rules places an obligation on intermediaries to provide information and assistance to government agencies concerning the security of the state, cyber security, and investigation or prosecution of offences. This rule seeks to amend Rule 3(7) of the Current Rules by inserting changes such as:

1. Imposition of a time limit of 72 hours for providing assistance to government agencies;
2. Requirement to provide assistance to ‘any government agency’ from the erstwhile ‘government agencies who are lawfully authorised’;
3. Requirement to provide assistance to government agencies for ‘security of the state’;
4. Any request for assistance made by government agencies can now be sent through electronic means in addition to written requests; and most crucially,
5. *“The intermediary shall enable tracing out of originator of information on its platform as required by government agencies who are legally authorised.”*

To address the most sensitive part of these proposed changes i.e. the traceability requirement, it is important to reproduce the definition of the term ‘originator’ as per Section 2(1)(za):

“Originator means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated stores, or transmitted to any other person by does not include an intermediary”

The most concerning aspect of this requirement is how it will affect intermediaries like WhatsApp and Signal who provide personal communication services (over the Internet) which are end-to-end encrypted i.e. wherein even the service provider does not have access to the content of messages / information which flows through their platform. For reference, *“WhatsApp’s end-to-end encryption ensures only you and the person you’re communicating with can read what’s sent, and nobody in between, not even WhatsApp. Your messages are secured with locks, and only the recipient and you have the special keys needed to unlock and read your messages. For added protection, every*

message you send has an unique lock and key.”¹⁰

Introducing a traceability requirement for end-to-end encrypted services will lead to breaking of such encryption and thus compromising the privacy of individuals making use of such services for their private communication.

In August of 2017, a nine-judge bench of the Supreme Court in *KS Puttaswamy v. UOI*¹¹ (“the Privacy Judgment”), held that “*the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution.*” The judgment comprises of six different opinions, but at various points, the judges have held that informational and communicational privacy forms a part of the overall privacy of a person and unauthorised use or use of such information without the informed consent of users violates their privacy.

In his judgment, F. Nariman J. has stated that one of the aspects that a fundamental right to privacy would cover in the Indian context would be “*Informational privacy which does not deal with a person’s body but deals with a person’s mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of this right*”.¹² Similarly, SK Kaul J. opined that, “*The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed. Thus, for e.g. , if the posting on social media websites is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it.*”¹³

DY Chandrachud J. (for himself and three other judges) in his judgment stated that, “*Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well.*”¹⁴ While discussing the various types of privacy, he observed that communicational and informational privacy are a part of nine primary types of privacy¹⁵ - “*communicational privacy which is reflected in enabling an individual to restrict access to communications or control the use of information which is communicated to*

10 Explanation of the end-to-end encryption used by WhatsApp on its service, available at <https://faq.whatsapp.com/en/android/28030015/>. Last accessed on 28 January 2019.

11 WP (Civil) No. 494 of 2012, available at https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf. Last accessed on 28 January 2019.

12 Id., Para 81 of Justice Nariman’s judgment.

13 Id., Para 70 of Justice Kaul’s judgment.

14 Id., Para 3(H) of the Conclusion to Justice Chandrachud’s judgment.

15 Id., Para 142 Justice Chandrachud’s judgment.

third parties” and “informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information.”

In Puttaswamy, the court also established a four-pronged test for the legitimate invasion of the fundamental right to privacy:¹⁶

- a) The action must be sanctioned by law;
- b) The proposed action must be necessary in a democratic society for a legitimate state aim;
- c) The extent of such interference must be proportionate to the need for such interference. There should be a rational nexus between the objects and the means adopted to achieve them; and
- d) There must be procedural guarantees against abuse of such interference.¹⁷

Thus, any regulation proposed by the Government, which has the purport of violating the privacy of individuals needs to pass this four-pronged test enunciated by the Supreme Court in the Puttaswamy judgment. The traceability requirement proposed under the Draft Rules, will not be a proportionate or necessary measure if it has the implication of breaking end-to-end encryption on messaging services. The Draft Rules also do not provide any procedural guarantees against the possible abuse of a process like traceability of originator of information, as required by the test laid down in the Puttaswamy judgment.

Section 69 of the IT Act gives powers to authorised representatives of Central and State Governments to intercept, monitor, or decrypt information stored in any computer resource¹⁸ in the interest of sovereignty or integrity of India, defence of India, security of the State, public order or for investigation of any offence (among other things). The Rules which lay down the procedure and safeguards for such interception, monitoring and decryption of information¹⁹ (“the Interception Rules”) authorise the Ministry of Home Affairs and the Home Department of the Central and State Governments respectively as the competent government authorities to issue order for such interception of information.²⁰ The traceability requirement under Rule 3(5) of the Draft Rules, if it intends to break encryption or request intermediaries for decryption of information then such

16 Id., Justice Chandrachud’s judgment representing 4 judges [Conclusion Para 3(H)] clubbed with Justice Kaul’s judgment (at Para 71), which forms the majority opinion of the Puttaswamy case on this point.

17 Id., Para 71 of Justice Kaul’s judgment.

18 The definition of ‘computer resource’ as per Section 2(1)(k) of the IT Act is: computer resource means computer, computer system, computer network, data, computer data, base or software.

19 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, available at <http://meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf>. Last accessed on 28 January 2019.

20 Id. at Rule 3.

powers already exist under a separate provision of the parent statute (i.e. as per Section 69 of the IT Act). The scope of decryption cannot be enlarged in subordinate legislation under a different provision (i.e. Section 79 of the IT Act in relation to the Draft Rules). Any changes addressing the decryption of information will necessarily have to be amendments to either Section 69 of the IT Act or / and the Interception Rules notified therein. Delegated legislation cannot go against the substantive provisions of the statute and they must be read in context of the primary / legislative act. In *ITW Signode India Ltd. v. Collector of Central Excise [(2004) 3 SCC 48]*,²¹ the Hon'ble Supreme Court stated that, "It is a well-settled principle of law that in case of a conflict between a substantive act and delegated legislation, the former shall prevail inasmuch as delegated legislation must be read in the context of the primary / legislative act and not the vice-versa."

Similarly, Section 69B of the IT Act deals with monitoring and collection of traffic data or information for the enhancement of cyber security in the country. The term 'traffic data' as defined under the Section 69B²² includes any data identifying or purporting to identify any person, location to or from which the communication is transmitted and includes communications origin, destination and time (among other things). The The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 provide the procedure and safeguards for monitoring of traffic data under Section 69B. These Rules authorize MeitY to pass an order for such monitoring. In as much as Rule 3(5) of the Draft Rules pertains to cyber security, it cannot override and enlarge the scope of Section 69B or the Rules framed under it.

Lastly, the Draft Rules seek to expand the powers of the Government for law enforcement by replacing the phrase 'government agencies who are lawfully authorised' to 'any government agency'. Such expansion of the scope of powers of the Government for investigation or prosecution purposes go beyond the scope of the Intermediaries Guidelines Rules under Section 79 of the IT Act and are changes that need to form a part of the parent legislation. As argued, specific provisions of the IT Act provide for procedural safeguards for enabling access to information by law enforcement agencies. These safeguards are missing in the Draft Rules. The Draft Rules potentially go beyond the scope of Section 79 and other core provisions of the IT Act such as Section 69 and 69B of the IT Act.

In *National Stock Exchange Member v. Union of India [125 (2005) DLT 165]*²³ the High Court of Delhi held that, *"...in every legal system there is a hierarchy of laws, and the general principle is that if there is a conflict between a norm in a higher layer of the hierarchy and a norm in a lower*

21 Available at <https://indiankanoon.org/doc/1305345/>. Last accessed on 29 January 2019.

22 See Explanation appended to Section 69B of the IT Act.

23 Available at <https://indiankanoon.org/doc/876340/>. Last accessed on 29 January 2019.

level of the hierarchy, then the norm in the higher layer prevails, and the norm in the lower layer becomes *ultra vires*” the court elaborated on the hierarchy of laws as: 1) The Constitution of India; 2) Statutory Law; 3) Delegated Legislation; and 4) Administrative Instructions.

Thus, it is clear that subordinate / delegated legislation cannot go beyond the scope of the substantive provisions of the main law and in the hierarchy of laws, statutory law will always prevail over delegated legislation.

The government should have an encryption policy, which is lacking at the moment. The government should stop trying to slip through a back door what cannot be done through the front door.

Our recommendations for Rule 3(5) of the Draft Rules are:

1. A requirement of traceability will be in violation of informational privacy, which has been recognized as a fundamental right by the Supreme Court in the Puttaswamy judgment. Thus, we recommend that such a provision should be removed from the Draft Rules.
2. Proposed changes in delegated legislation should not undermine substantive provisions of the IT Act (specifically, Section 69 and 69B of the IT Act). They should not go beyond the purport of their parent provision (Section 79 of the IT Act); and
3. The phrase ‘any government agency’ should be removed and the current language of ‘government agencies who are lawfully authorised’ should remain.
4. This Rule is beyond the ambit of Section 79 of the IT Act. Addition of a requirement of traceability in a subordinate legislation is beyond the rule-making power of the Government.

Local Office, Incorporation and Appointment of Nodal Officer

Rule 3(7) of the Draft Rules requires all intermediaries with more than 5 million users in India to be incorporated, have a permanent registered office in India with a physical address and appoint a nodal officer and a senior functionary for 24-hour coordination with Law Enforcement Agencies (“LEA”). The Current Rules do not have such obligations.

There is ambiguity regarding the meaning of “users” under this Rule. This Rule applies to all intermediaries with more than 5 million (50 lakh) users in India. At present there is lack of clarity about what this number of users refers to i.e. whether it refers to daily, monthly or yearly users, or the number of total registered users. To understand the implication of this requirement, reference to the user base of popular messaging apps is pertinent. WhatsApp, India’s most popular chatting app, has around 200 million users in India. Relatively newer chatting applications Hike and ShareChat

have 100 million users²⁴ and 25 million users respectively.²⁵ The 5 million users specified in the Draft Rules represent a little more than 1% of the Internet user base in India²⁶ which might bring a substantial number of intermediaries under a new set of compliance requirements. This may cause many start-ups to bear the brunt of high costs stemming from incorporation under Companies Act, 2013.

The Draft Rules stipulate appointment of different officers to ensure compliance with the orders / requisitions by law enforcement agencies in accordance with provisions of law or rules. To meet this objective, Draft Rule 3(7) requires the intermediary to appoint a nodal officer and a senior functionary for 24-hour coordination with LEA. Draft Rule 3(12) also mandates the appointment of grievance officer to address the complaints against violation of Draft Rule 3. Multiple appointments may increase procedural burdens for intermediaries and create possibilities of overlap in their functions.

We recommend:

1. To avoid confusion created due to multiplicity of authorities, a single officer can be appointed to fulfil compliance with the obligations;
2. The provision requiring incorporation of intermediaries can lead to compliance burden and should be made voluntary for intermediaries; and
3. Vietnam recently passed the Cybersecurity Law, which requires intermediaries to set up physical offices in the form of a representative office or branch within the country's jurisdiction in order to fulfil their cybersecurity obligations. The law does not require incorporation. Such alternatives can be explored in India.

G. 'Unlawful Information' and 'Proactive Content Filtering'

Rule 3(9) creates a positive obligation (by use of the words “shall” and “proactive monitoring”) on intermediaries to remove content. This implies that even without a court order, intermediaries have to actively search and filter content that is ‘unlawful’.

Online intermediaries are considered channels of distribution that play a merely neutral, technical and non-adjudicatory role. The Rule requires intermediaries to scrutinize user generated content and

24 Hike unbundles its messaging app to reach India's next wave of smartphone users, available at <https://techcrunch.com/2018/01/16/hike-unbundles-its-messaging-app/>. Last accessed on 30 January 2019.

25 ShareChat: The no-English social media app that Indian politicians are flocking to, available at <https://scroll.in/article/897154/sharechat-the-no-english-social-media-app-that-indian-politicians-are-flocking-to/>. Last accessed on 30 January 2019.

26 According to the Mobile Internet Report, IAMAI, 2017 there are 456 million mobile Internet users in India.

determine its legality - a task which must be undertaken by the judiciary considering that there are no clear standards of what is 'unlawful'. This provision of proactive content filtering is against the judgment in *Shreya Singhal v. Union of India*, wherein the Supreme Court had held that intermediaries are neutral platforms that do not need to exercise their own judgment to decide what constitutes legitimate content. The Council of Europe's recommendation on the role of Internet intermediaries asserts that that 'illegal content' should be determined either by law or by a judicial authority or other independent administrative authority whose decisions are subject to judicial review.²⁷ The Global Network Initiative (GNI) in its statement²⁸ on the 'Terrorist Content Regulation', EU's proposed law to prevent the dissemination of 'terrorist content', has highlighted how definitional issues are likely to lead to legal uncertainty as well as potentially overly-aggressive interpretations by companies that could result in the removal of content that should be protected.

The United Nations Special Rapporteur on the protection of the right to freedom of opinion and expression, right to privacy and protection of human rights and fundamental freedoms, in a letter to the Commission of the European Union, raised grave concerns about the 'Terrorist Content Regulation' that stipulates proactive monitoring of content using automated tools. The letter stated that a 'general monitoring obligation will lead to the monitoring and filtering of user generated content at the point of upload. This form of pre-screening would enable the blocking of content without any form of due process even before it is published, reversing the well established presumption that States, not individuals, bear the burden of justifying restrictions on freedom of expression.'²⁹

Implementation of the Rule will lead to massive private censorship as intermediaries will over-censor content to retain their safe-harbour protection under Section 79 of the IT Act. We recommend that 'unlawful' content should be restricted to acts mentioned under Article 19 (2).

H. Automated Tools

Rule 3(9) mandates deployment of technology based automated tools by intermediaries to

27 Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of Internet intermediaries, available at www.coe.int/cm. Last accessed on 30 January 2019.

28 Statement on Europe's Proposed Regulation on Preventing the Dissemination of Terrorist Content Online, available at <https://globalnetworkinitiative.org/wp-content/uploads/2019/01/GNI-Statement-Proposed-EU-Regulation-on-Terrorist-Content.pdf>. Last accessed on 30 January 2019.

29 Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering Terrorism, available at <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=24234>. Last accessed on 27 January 2019.

proactively monitor content. The Council of Europe in their latest recommendation on the role and responsibility of Internet intermediaries has mentioned that States should take into account the fact that automated means, which may be used to identify illegal content, currently have a limited ability to assess context. Such restrictions should not prevent the legitimate use of identical or similar content in other contexts.³⁰ The recommendation also states that any restriction of content should be carried out using the least restrictive technical means and should be limited in scope and duration to what is strictly necessary.

The recent letter³¹ by Special Rapporteurs to the Commission of EU has also warned against the use of automated content tools to take down content. It states that due to AI's inadequate understanding of context, the use of automated tools comes with serious limitations and aggravates the risk of pre-publication censorship. It further mentions that even the use of algorithms with a very high accuracy rate potentially results in hundreds of thousands of wrong decisions leading to screening that is over-inclusive or under-inclusive.

Automated moderation systems that are in use today rely on keyword tagging which is then followed by human review. Even the most advanced automated systems cannot, at the moment, replace human moderators in terms of accuracy and efficiency. This is mainly because artificial intelligence is currently not mature enough to understand the nuances of human communication such as sarcasm and irony.³² It should also be noted that global communication is influenced by cultural differences and overtones which an effective system of content moderation has to adapt to, and given the amateurish stage at which AI is at the moment, it may be short sighted to rely on this technology.

As our societies evolve and change, so does the definition of “grossly harmful / offensive content”. This implies that algorithms have to constantly understand nuanced social and cultural context that varies across regions. Research on AI has not yet produced any significant sets of data for this kind of understanding. The immediate result of using automated tools will be an increase in content takedowns and account suspensions which in turn will lead to over-censorship as has been seen around the world. Legitimate users (content creators) including journalists, human rights activists and dissidents will have their speech censored on a regular basis.

YouTube's “Content ID” system for detecting content that infringes copyright has been deemed

30 See footnote 27.

31 See footnote 29.

32 Despite What Zuckerberg's Testimony May Imply, AI Cannot Save Us, available at <https://www.eff.org/deeplinks/2018/04/despite-what-zuckerbergs-testimony-may-imply-ai-cannot-save-us/>. Last accessed on 30 January 2019.

notorious for over-censoring innocent material. Use of AI without human intervention for detecting hate speech, misinformation, disinformation, trolling, etc which is even more nuanced than identifying copyrighted material will be catastrophic for freedom of speech and expression on the Internet.

The key limitations of natural language processing tools are:³³

1. Natural language processing (“NLP”) tools perform best when they are trained and applied in specific domains, and cannot necessarily be applied with the same reliability across different contexts;
2. Decisions based on automated social media content analysis risk further marginalizing and disproportionately censoring groups that already face discrimination. NLP tools can amplify social bias reflected in language and are likely to have lower accuracy for minority groups who are under-represented in training data;
3. Accurate text classification requires clear, consistent definitions of the type of speech to be identified. Policy debates around content moderation and social media mining tend to lack such precise definitions;
4. The accuracy and intercoder reliability challenges documented in NLP studies warn against widespread application of the tools for consequential decision-making; and
5. Text filters remain easy to evade and fall far short of humans’ ability to parse meaning from text.

Recognising the shortcomings of automated tools, Article 22(1) of the European Union’s General Data Protection Regulation states that “*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*”³⁴ Automated removal of content that falls under freedom of speech and expression would produce a legal effect and could significantly affect such a person.

We recommend that the requirement of deploying automated tools for proactive content filtering should be removed from the Draft Rules.

33 Mixed Messages? The Limits of Automated Social Media Content Analysis Presented at the 2018 Conference on Fairness, Accountability, and Transparency, Natasha Duarte Emma Llansó (Center for Democracy & Technology), Anna Loup (University of Southern California), available at <https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf>. Last accessed on 30 January 2019.

34 Article 22 of the European Union’s General Data Protection Regulation, available at <https://gdpr-info.eu/art-22-gdpr/>. Last accessed on 30 January 2019.

I. Lack of safeguards

Section 69A of the IT Act provides for power to the Central Government to block public access of any information through any computer resource. The blocking of content can be resorted to by the Central Government in cases where it is necessary to do so in the interest of sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to the above. Thus, the blocking of sites are permitted only in the case of exemptions to Freedom of speech provided as per Article 19(2) of the Constitution of India.

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 have been notified by the Central Government to provide the procedure and safeguards for such blocking. These Rules provide a detailed procedure for blocking of access with a designated officer not below the rank of a Joint Secretary entrusted for the purpose of issuing direction for blocking.

It is clear from the provision of Section 69A that the legislature aimed to have sufficient safeguards in place for blocking of the content. These safeguards are not present in the Draft Rules. We recommend ensuring that these safeguards are not violated by any amendment to the Rules.

J. Notice and Consent fatigue

Rule 3(4) of the Draft Rules requires intermediaries to notify their users 'at least once every month' of their privacy policies and user agreements, non compliance of which will result in termination of access and removal of non-compliant content. This requirement of monthly notification is an addition to the Current Rules and will lead to excessive communication from intermediaries to users. Such a notification requirement will lead to consent / user fatigue (excessive content / user notifications leads to dilution of meaningful and informed consent). Consent / user fatigue is a problem that was identified in the report of the 'Committee of Experts under the Chairmanship of Justice BN Srikrishna' ("the Report") which was tasked to draft India's Personal Data Protection Bill. The Report mentions that, "*There is undoubtedly some truth in excessive consent requirements desensitising individuals towards consent.*"³⁵ The Report points to a problem that user fatigue will result in desensitising individuals to privacy harms and will not achieve the goal of informed consent - "...constant intimations for consent may affect user experience and desensitise individuals

35 Last paragraph of Page 39 of the Srikrishna Report, available at http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf. Last accessed on 29 January 2019.

to privacy harms.”³⁶

If the intent behind introducing this requirement is to meaningfully communicate to users their terms of use and privacy agreements, then mandatory monthly notifications will not solve this problem, rather it will prove to be a counter-productive tool and desensitise users to their obligations and possible privacy harms from using services. The issue of consent / user fatigue should be addressed by MeitY under the Personal Data Protection Bill and mechanisms such as better privacy policy designs and effective notification measures such as - dashboards may be looked at (as recommended by the Srikrishna committee in its Report)³⁷

It is also important to point out that the notice and consent model could be used to disclaim liability on the part of the intermediaries, hence for meaningful communication of user agreements and privacy policies (notice requirements) the validity of consent must be carefully determined. “...consent should be freely given, informed and specific to the processing of personal data.”³⁸

There is a concern that genuine messages regarding changes in the terms of service / privacy policy / other documents regarding conduct on the platform would get lost in the barrage of notifications regarding the requirement of compliance with the standard terms. Users are likely to start ignoring these notifications entirely, without having any knowledge about the differences regarding permissible content on different platforms.

We recommend that the requirement of monthly notification should be removed from the Draft Rules as it will not serve the purpose for which it is being introduced.

K. Public health or safety

Rule 3(2)(j) prohibits various alcohol and nicotine-based products. There is no known precedent for banning such categories of content altogether in any medium. There are certain restrictions on the display of such content in motion pictures and there are prohibitions in place against advertising such products, but such content is not banned altogether. The sub-clause, in its current form, can be interpreted to include activities that go beyond advertisement of such content, such a photograph containing consumption of alcohol by a user of a social media platform.

If this sub-clause is retained in any form, then the terms used in this sub-rule need to be changed in order to better reflect their intent, i.e. to ban only advertisement of these products,

³⁶ Id. at page 40.

³⁷ Id. at pages 38-39.

³⁸ Id. at page 26, last paragraph of the page.

Our recommendation is to remove this sub-clause entirely as it violates the freedom of speech and expression guaranteed under the Constitution of India.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Rule-Wise Comments

Rule 3. Due Diligence observed by intermediary

Sub-Rule 1

The one size fits all treatment of intermediaries is problematic as the functions of each class of intermediaries like Telecom Service Providers, caching services and social media platforms are different. The obligations cast on each intermediary has to be based on its role and the kind of control it has over content.

Sub-Rule 2

The rule lists a range of information that users are prevented from displaying, uploading, or sharing through an intermediary. The provision is against the dictum laid down by the Supreme Court in the *Shreya Singhal* judgment that “*Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79*”. The broad list of information deemed to be unlawful goes beyond the restrictions as per Article 19(2) and is unconstitutional. Moreover, the terms and expressions used are vague and ambiguous.

Sub-Rule 4

Rule 3(4) of the Draft Rules requires intermediaries to notify their users ‘at least once every month’ of their privacy policies and user agreements, non compliance of which will result in termination of access and removal of non-compliant content. This requirement of monthly notification is an addition to the Current Rules and will lead to excessive communication from intermediaries to users. Such a notification requirement will lead to consent / user fatigue (excessive content / user notifications leads to dilution of meaningful and informed consent).

It is our recommendation that the requirement of monthly notification should be removed from the Draft Rules as it will not serve the purpose for which it is being introduced.

Sub-Rule 5

The rule as explained earlier could result in violation of the right to privacy of users and thus should be removed.

Sub-Rule 7

The rule lacks clarity as to how the number of users is determined in the case of an intermediary as the users could be registered users or average active users per day / month / year. Moreover, the stipulation for incorporation of the entity puts onerous burden on the intermediary.

Sub-Rule 8

This Sub-Rule has been modified as per the judgment in *Shreya Singhal*. However, the norm for retention of records should be to keep the least amount of data and for the least amount of time based on the purpose for which the data is being kept. There should not be any requirement to store data any longer than necessary.

Sub-Rule 9

Automated tools, especially when these are mandated to filter content deemed illegal under the broad categories stipulated under Sub Rule 3, will lead to muzzling of free speech and result in chilling effect. This restriction is clearly violative of the fundamental right to freedom of speech and expression and goes beyond the restrictions that can be imposed under Article 19(2) as laid down in *Shreya Singhal v UOI* and *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors.*

Sub-Rule (9) of Rule 3, by providing for automated tools to filter content without laying down any procedures and safeguards, results in violation of a citizen's right to freedom of speech and expression.

Sub-Rule 12

The notifications to the designated agent may be restricted only to infringements in the case of Trademarks and Copyright, and in the case of other unlawful activities, when supported by an order from a competent court or appropriate Government.

Feedback on the Draft Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018

At the outset we would like to congratulate the Ministry of Electronics and Information Technology (“MeitY”) for taking this positive step towards seeking public comments towards an important piece of regulation. As the representative of the information technology industry, we also thank MeitY for this opportunity to present our views and suggestions on the draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 (“Draft Rules”) which are intended to amend the existing Information Technology (Intermediaries Guidelines) Rules, 2011 (“Intermediary Guidelines 2011”).

In terms of our approach, given the numerous seminal judgments, orders and guidance from various courts since the Intermediary Guidelines 2011 were first introduced, we believe that a holistic relook at the entire Intermediary Guidelines 2011 is required. Therefore, we have not restricted our comments / suggestions to the Draft Rules alone but have also provided our comments on the Intermediary Guidelines 2011 as a whole.

We have split our response into two parts: (i) Part A provides context to the Intermediary Guidelines 2011 as well as identifies existing interpretation issues with them; (ii) Part B provides a para wise review of the Draft Rules along with our suggestions and comments.

A. Overall Observations

1. Scope of Intermediary Guidelines 2011:

Section 79 of the Information Technology Act, 2000 (“IT Act”), which is the genesis of the Intermediary Guidelines 2011, was introduced to provide intermediaries with exemption from liability / safe harbor in certain limited scenarios.

The purport of this section is to provide intermediaries with ‘immunity from third party information, data, or communication link made available or hosted,¹’ subject to compliance with the conditions specified under Section 79(2)² and Section 79(3)³ of the IT Act.

¹ Section 79(1), IT Act

² (2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

³ (3) The provisions of sub-section (1) shall not apply if-

Therefore, any additional obligation placed on intermediaries beyond the scope of the aforementioned purpose, i.e., providing an intermediary immunity for third party content hosted by it, as such should not be the subject matter of the Intermediary Guidelines 2011 framed under Section 79. Consequently, any provision which is proposed under the Intermediary Guidelines 2011 would need to be tested on the grounds of whether or not it exceeds the realm of Section 79 (if it does so, it will be *ultra vires* Section 79 of the IT Act). For example, Rule 3(5) of the Draft Rules, appears to go beyond the realm of Section 79 of the IT Act. Section 78 of the IT Act already empowers certain police officers to investigate offences under the IT Act. Thus, for the purpose of investigation, other provisions of the IT Act should be invoked and a requirement should not be added in the Intermediary Guidelines 2011 which is issued under Section 79.

Thus, the proposed amendments to the Intermediary Guidelines 2011 should be restricted only to cover those matters that fall under Section 79 of the IT Act.

2. Different Types of Intermediaries:

We understand that one of the purposes of amending the Intermediary Guidelines 2011 is to address the issue of the spread of fake news on social media platforms⁴. However, by adding prescriptive due – diligence requirement on all intermediaries, we believe that one risks making a sweeping generalization about the roles played by different types of intermediaries without taking into account the differences in the nature, function and activities of different intermediaries.

Most intermediaries do not enable users to disseminate or share content with others, or even make content available to the public. Therefore, using the same yardstick to regulate intermediaries who do not make content available to the public would be excessive. Several intermediaries in fact are engaged in business to business (B2B) transactions alone and do not have any role with respect to the circulation of fake news. Some examples of different types of intermediaries are as follow:

- Outsourcing entities (who are only in the business of data processing)
- Accounting software providers
- Payroll management software providers
- Cloud infrastructure providers
- Online payment systems

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:-For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

⁴<http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9Cinformation-technology-intermediary-guidelines> (Last visited January 28, 2019)

While the safe harbor provisions under Section 79 of the IT Act should apply to all types of intermediaries (subject to fulfillment of the conditions stipulated under the section), due to the distinct role played by each type of intermediary, the same due diligence obligations cannot be applied to all. For example, requiring cloud service providers to actively monitor and take down content as required under the Draft Rules would not be applicable or even practically possible. Similarly, requiring an entity in the IT – BPM sector to enable traceability of the data made available to it would not only expose such entity to possible liabilities under data protection laws but also serve no real purpose.

Furthermore, there are several intermediaries who are already regulated under law. For example, payment intermediaries are regulated by the Reserve Bank of India and telecom service providers are regulated by the Department of Telecom. Accordingly, these types of intermediaries are already required to comply with several obligations under applicable laws, many of which are even more stringent than the Intermediary Guidelines 2011. Therefore, a distinction needs to be made in terms of the level of oversight that is applied to such entities and the consequent due diligence requirements that must be imposed on them.

NASSCOM shall be pleased to work with MeitY to help draw up such distinctions in terms of the different types / classes of intermediaries, and identify what corresponding obligations should apply to each.

3. Need for Procedural Safeguards:

In *Shreya Singhal v Union of India*⁵, the Supreme Court (“SC”) refrained from striking down Section 69 A, due to the presence of several procedural safeguards built into the law itself. The court had specifically observed⁶ as follows:

*“It will be noticed that Section 69A unlike Section 66A is a narrowly drawn provision with several safeguards. First and foremost, **blocking can only be resorted to where the Central Government is satisfied that it is necessary so to do.** Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). **Thirdly, reasons have to be recorded in writing** in such blocking order so that they may be assailed in a writ petition under Article 226 of the Constitution.”*

Even though the Draft Rules require that content running afoul of Article 19(2) must be taken down, in terms of process it is devoid of the following procedural safeguards which are otherwise available in Section 69 A:

- Who can pass the orders, as the term ‘appropriate Government or its agency’ has been defined too broadly and is also vague.

⁵ Writ Petition (Criminal) No. 167 of 2012

⁶ Paragraph 109, *Shreya Singhal v Union of India*

- The rule does not specify that a government order to takedown content will be accompanied with the reason for takedown.
- There is no requirement that takedown must be only be issued where strictly necessary.

Given that any takedown request is likely to have an impact on the right to freedom and speech and expression, it is imperative that such safeguard be built into the Intermediary Guidelines 2011 to ensure transparency.

4. Need for clarification of the term 'knowingly host':

In *Shreya Singhal v Union of India*, the SC dealt with Section 79(3) (b) of the IT Act and Rule 3(4) of the Intermediary Guidelines 2011. The requirement of 'actual knowledge' in these provisions was read down to mean 'upon receipt of a court order/notification by an appropriate government or its agency'.

However, given that the SC had only read down the term, 'actual knowledge', in the context of Rule 3(4) of the Intermediary Guidelines 2011, it is not entirely clear what is the meaning of the term 'knowingly host' in Rule 3(3) of the Intermediary Guidelines 2011. Accordingly, there should be clarity provided on its meaning in accordance with the principles laid down in the *Shreya Singhal* case.

Another issue that arises in terms of the judgment is where the SC held:

*"Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). **Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79.** With these two caveats, we refrain from striking down Section 79(3) (b)."*⁷

In continuation of the above, the court concluded:

*"Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that **unlawful acts relating to Article 19(2)** are going to be committed then fails to expeditiously remove or disable access to such material.*

*Similarly, the Information Technology "Intermediary Guidelines 2011" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment."*⁸

⁷ Paragraph 117

⁸ Paragraph 119 (c)

Thus, there is need for clarity as to the scope of the restrictions referred to by the SC. Whether the limitations of Article 19(2) of the Constitution would apply only when the content to which such limitation is applied relates to free speech and expression and not otherwise E.g. actions such as infringement of intellectual property rights, or impersonations of persons are *not* relatable to speech and expression. Accordingly, the restrictions under Article 19(2) of the Constitution should not apply to such content.

Therefore, given the impact of the above issues on the Intermediary Guidelines 2011 as a whole, we believe that there is need for clarity on the aforesaid issues.

Against this background, please see our specific recommendations in relation to the Draft Rules below:

B. Specific Comments on Draft Rules:

1. Rule 3(2) and Rule 3(3)

Rule 3(2) of the Intermediary Guidelines prescribes that an intermediary publish rules and regulations, privacy policy and user agreements informing users not to display, host, etc. certain kinds of content. Rule 3(3) of the Intermediary Guidelines further prescribes that the intermediary shall not knowingly initiate the transmission, select the receiver of the transmission and select/modify the information contained in the transmission in respect of the content specified under Rule 3(2).

In addition to the existing requirement in the Intermediary Guidelines 2011, the Draft Rules introduce⁹ two new categories of such content, being a) content which threatens public health or safety, the promotion of cigarettes or other tobacco products, etc., and b) content which threatens critical information infrastructure¹⁰.

As mentioned above, we have provided our comments on the Intermediary Guidelines 2011 as a whole and not restricted ourselves to the Draft Rules. The following issues arise on a review of these two provisions:

a) **Vagueness:**

Certain categories of content identified under the Intermediary Guidelines 2011, suffer from vagueness, such as:

⁹ Rule 3(2) (j) and (k), Draft Rules

¹⁰ Critical information infrastructure has been defined under the Explanation to Section 70(1) of the Information Technology Act, 2000 as follows: "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety

- (i) Information that is 'grossly harmful,' 'harassing', 'racially, ethnically objectionable' or 'hateful'¹¹
- (ii) 'information which is grossly offensive or menacing in nature'¹²
- (iii) Information that 'threatens public health or safety'¹³

These terms are not defined under any law. In the *Shreya Singhal* case, the SC struck down Section 66A of the IT Act on account of unconstitutional vagueness due to its open-ended and undefined language.

The court held:

*"If judicially trained minds can come to diametrically opposite conclusions on the same set of facts it is obvious that expressions such as "grossly offensive" or "menacing" are so vague that there is no manageable standard by which a person can be said to have committed an offence or not to have committed an offence."*¹⁴

Similarly, what would threaten public health or safety is not clearly and easily understandable.

Submission: We suggest that either the aforesaid categories of information are more tightly defined or they are altogether deleted from the Intermediary Guidelines 2011.

b) Critical Information Infrastructure provisions covered by existing law:

Rule 3(2)(k) and Rule 3(3) of the Draft Rules requires (i) intermediaries to publish rules and regulations, privacy policy or user agreements informing users not to share information which 'threatens critical information infrastructure,' and (ii) directs intermediaries not to knowingly host or publish such information. Failure to comply with these rules entails that an intermediary loses its safe harbor under Section 79 of the IT Act.

We do not believe that there is a specific reason to include this provision into the due diligence that an intermediary should carry out as there are anyway existing provisions under the IT Act and rules framed thereunder which address the issue of threatening critical information infrastructure, namely Section 70, IT Act and the Information Technology (National Critical Information Infrastructure Protection Center and Manner of Performing Functions and Duties) Rules, 2013. Failure to comply with these provisions would attract the appropriate penalties provided under the law and therefore, this should not have a bearing on the safe harbor provided to the intermediary.

¹¹ Rule 3(2)(b), Intermediary Guidelines

¹² Rule 3(2)(f), Intermediary Guidelines

¹³ Rule 3(2)(j), Draft Rules

¹⁴ Paragraph 82, *Shreya Singhal v Union of India*.

Accordingly, for the issue of threats to critical information infrastructure, intermediaries should be liable solely under section 70 of the IT Act and the relevant rules, and their safe harbor vis-à-vis electronic records should remain unaffected.

Submission: We suggest that Rule 3(2)(k) is deleted.

c) Guidelines more restrictive than applicable law:

Certain prohibitions under the Intermediary Guidelines 2011 and the Draft Rules are more restrictive than applicable law and therefore, should not form part of the due diligence required of the intermediary since such action is not prohibited under the various legislations in India.

For example, Rules 3(2)(j) and 3(3) of the Draft Rules *inter alia* prohibit the sharing of information pertaining to the 'promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol.' However, unlike the Cable Television Networks (Regulation) Act 1995 and Cable Television Networks Rules, 1994¹⁵ which prohibit advertising alcohol on television the Draft Rules appear to be encroaching on a state specific policy viz. advertising of alcohol¹⁶ by extending its applicability to online media as well.

d) Requirement not to 'Knowingly host'

In *Shreya Singhal*, the SC had observed that it would be impracticable for intermediaries such as Google and Facebook to act when millions of take down requests were made and the intermediary was required to judge which requests were legitimate and which were not.¹⁷ Accordingly, the SC read down 'actual knowledge' in Section 79(3)(b) of the IT Act and Rule 3(4) of the Intermediary Guidelines 2011 to mean upon receipt of a court order/notification by an appropriate Government or its agency.

However, the SC did not clarify whether the requirement not to 'knowingly host' information as provided under Rule 3(4) of the Intermediary Guidelines 2011 would trigger only upon receipt of a court order/Government notification. Accordingly, as stated above, clarity is required on the meaning of 'knowingly host' under Rule 3(3) of the Intermediary Guidelines in accordance with the principles laid down in the *Shreya Singhal* case.

e) Possible Approach

¹⁵ Rule 7(2)(viii) Advertising Code

¹⁶ Entry 51, List II, Seventh Schedule, Constitution of India

¹⁷ Paragraph 117, *Shreya Singhal v Union of India*

In respect of certain types of content, such as content which violates intellectual property rights, a procedure similar to the 'Notice and Takedown' procedure under the US Digital Millennium Copyright Act ("DMCA") may be considered. We believe that such a process may not only provide a speedy efficacious remedy at the first level to most aggrieved parties but may also reduce the burden on courts in India.

Under the DMCA, briefly stated, the procedure is as follows:

- (i) A complainant submits a take-down notice to the intermediary in a specified form with specified information identifying the work, containing the complainant's contact information, etc.
- (ii) The intermediary takes down the content identified as potentially infringing and notifies the user that it has disabled access to the material
- (iii) Upon receipt of the notice, the user has the opportunity to contest the infringement complaint by way of a counter-notification
- (iv) An intermediary that receives a valid counter-notification is required to forward the same to the complainant along with a statement that it will put the material back in ten (10) business days unless a court order is filed preventing the user from infringing any copyright
- (v) An intermediary that fails to hear from a complainant can enable access to the material 10 - 14 business days later

Submission: We suggest that the Government may review the obligations imposed on intermediaries in India on the above lines.

2. Rule 3(4)

Under Rule 3(5) of the Intermediary Guidelines 2011, intermediaries are required to inform users of possible termination of access/usage rights in the case of non-compliance with its rules and regulations, user agreement or privacy policy. However, the frequency of such notification had not been prescribed. Rule 3(4) of the Draft Rules prescribes that intermediaries must inform their users of possible termination once every month.

We believe that Rule 3(4) of the Draft Rules treats all intermediaries as being alike and the obligation to inform users every month is too onerous for intermediaries and superfluous. Further, there does not appear to be any rationale as to the imposition of a monthly reminder as opposed to such reminders being sent on longer intervals. We believe that a strategy of sending a monthly reminder may be ineffective because:

- (i) It will create warning fatigue amongst users, instead of increasing awareness resulting in the warning itself being disregarded.

- (ii) Repeated reminders may increase the likelihood of categorization of various companies' emails to users as spam, thereby making several platforms less attractive to users.

Submission: We suggest that this amendment should not be included in the Intermediary Guidelines 2011 and intermediaries should be left to determine when they would like to send such notices to their users.

3. Rule 3(5)

The Intermediary Guidelines 2011, in their current form, require that intermediaries provide information or assistance to Government Agencies for the purpose of verification of identity, or for the prevention, investigation, etc. of cyber security incidents and the punishment of offences. Such requests for information or assistance are required to be made in writing clearly stating the purpose for seeking it.

Rule 3(5) of the Draft Rules amends this provision¹⁸ in certain respects:

- (i) *72 hour time limit:* The Draft Guidelines impose a time-limit of 72 hours from receipt of such communication to comply with it.
- (ii) *Traceability:* Importantly, the Draft Guidelines prescribe that the intermediary shall enable tracing of the originator of information on its platform when called upon to do so by government agencies lawfully authorized to request this.

The following issues arise on a review of this provision:

a) ***Vires of Rule 3(5):***

In our view, Rule 3(5) is *ultra vires* Section 79 of the IT Act. As discussed above, the purport of Section 79 is to provide intermediaries with immunity from third party content made available or hosted on their platforms, subject to certain prescribed conditions. The obligation to provide information/assistance to government agencies on intermediaries is beyond the scope of this purpose and is accordingly *ultra vires* Section 79 and should be deleted in its entirety.

Appropriate mechanisms already exist under the IT Act and rules framed thereunder which encompass the provisions sought to be introduced vide this Rule. For instance, Section 69 of the IT Act already empowers the Government to issue directions for interception or monitoring or decryption of information

¹⁸ Rule 3(5), Draft Rules

through a computer resource, subject to the safeguards/procedural requirements in that section¹⁹. Accordingly, there is no requirement to introduce fresh traceability provisions under the Draft Rules.

Submission: *Therefore, on this ground alone, Rule 3(5) should be deleted entirely from the Draft Rules.*

Without prejudice to the foregoing, we have also identified the following issues with Rule 3(5):

b) 72 hour time limit:

The Draft Rules do not provide any justification as to why a timeline of 72 hours would be appropriate. This requirement is unreasonable and suffers from the defect that it does not prescribe a due process requirement, i.e. it does not allow an intermediary to request a hearing, seek clarifications, or adequately respond to a request from a Government Agent/court and requires immediate action on part of an intermediary.

Furthermore, practically, the tight timeline does not take into account the different kinds of intermediaries and cross border data flows.

Submission: *Accordingly, we recommend deletion of this timeline.*

c) Enabling Traceability:

This requirement appears to be in contravention of the right to privacy which was recognized as a fundamental right by the SC in the case of *Justice K.S Puttaswamy (Retd.) v. Union of India and Ors.*²⁰ Accordingly, any infringement of privacy would have to meet the test of

- “(i) legality, which postulates the existence of law;
- (ii) need, defined in terms of a legitimate state aim; and

¹⁹ Section 69 - Power to issue directions for interception or monitoring or decryption of any information through any computer resource
1[1] Where the Central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-
(a) provide access to or secure access to the computer resource generating transmitting, receiving or storing such information; or
(b) intercept, monitor, or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

²⁰ WP (C) 494 of 2012

(iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them”²¹

Submission: We suggest that the requirement to enable tracing the originator of content does not appear to meet the tests of necessity and proportionality and should be deleted.

4. Rule 3(7)

Rule 3(7) introduces certain conditions for intermediaries (1) with more than fifty lakh users and (2) intermediaries specifically notified by the Government of India, to comply with. These conditions are as follows:

- (i) Requirement to incorporate companies under the Indian Companies Act.
- (ii) Requirement to have a registered office in India with a physical address; and
- (iii) Requirement to appoint a nodal person of contact and alternate senior designated official for 24 x 7 coordination with Indian law enforcement agencies and officers to ensure compliance with orders/requisitions made.

Rule 3(7) of the Draft Rules runs completely *ultra vires* Section 79 of the IT Act and does not any nexus with its objective, namely, safe harbor provided to intermediaries for third party information being hosted, dealt with by them.

Without prejudice to the above, our specific concerns with this rule are below:

a) **Excessive Delegation of Powers:**

This rule excessively delegates power to the Government to notify additional categories of intermediaries who have to adhere to the aforesaid conditions. **There is no procedural safeguards in terms of guidance for the types of intermediaries which can be notified.** This would result in business uncertainty for intermediaries. The provision should specify what specific criteria may lead to these requirements becoming applicable to an intermediary rather than being vague.

b) **Potential market barrier:**

The requirement to have a physical presence in India may act as a disincentive for platforms to enter the Indian market, and deprive Indians of access to foreign platforms. Such a policy would go against

²¹ Judgment delivered by Justice Chandrachud on behalf of himself, Chief Justice JS Khehar, Justice Agrawal and Justice Abdul Nazeer

the ethos of a free and open internet. We believe this would also have the unintended effect of reducing competition in the digital economy.

c) **Taxation concerns:**

The requirement to have a physical presence in India is likely to give rise to tax concerns for such intermediaries which in turn would impact the cost of doing business with the end consumers eventually bearing the burden. We believe this would hardly be the intent of the Government given the objectives of the guidelines.

d) **Arbitrary Threshold:**

The threshold of fifty lakh users is arbitrary and devoid of any reasoning.

Submission: For the aforementioned reasons, we would once again like to emphasize the need to delete this particular rule altogether and completely rethink how the objectives behind passing the Draft Rules may be addressed effectively.

5. **Rule 3(8)**

Under the current Intermediary Guidelines 2011, as read down in *Shreya Singhal*, an intermediary on whose computer system unlawful content is hosted, upon receiving actual knowledge by a court order/notification by appropriate Government or its agency must act within thirty – six hours to disable access to such content. Further, an intermediary is required to preserve such information and records for at least 90 days for investigation purposes. The Draft Rules amend these provisions in the following respects:

- (i) The Draft Rules clarify that only unlawful content relatable to specific grounds under Article 19(2) of the Constitution shall be required to be taken down.
- (ii) The Draft Rules *require* that intermediaries comply with such orders within 24 hours
- (iii) The Draft Rules increase the number of days that an intermediary is required to preserve such information/records for investigation purposes from 90 days to 180 days, or ‘*such longer period as required by the court or authorized Government agencies.*’

The proposed Rule 3(8) suffers from the following issues:

a) **Lack of Procedural Safeguards:**

As mentioned above, unlike Section 69 A of the IT Act, even though the takedown provisions contained in this rule refer to unlawful acts contained in Article 19(2) process wise the rule lacks procedural safeguards, as discussed in detail above.

Submission: *We suggest this Rule should be amended to build in adequate procedural safeguards.*

b) Unreasonable 24 hour time period:

The time period of 24 hours to comply with such takedown requests is completely unreasonable and impractical. This period does not account for the time taken to verify authenticity of requests, any human intervention required in the process of takedown, and other delays.

Submission: *We suggest this 24 hour time line should be suitably increased and in case an intermediary requires more time, the guidelines should allow for such a request from the intermediaries.*

c) Procedural Streamlining:

Often intermediaries receive vague notices from various Government authorities under Section 79 of the IT Act without citing specific grounds under which content is found to be objectionable. Further, at times the unlawful content is not specifically identified. This results in intermediaries spending substantial time internally attempting to guess why a particular takedown request has been issued, and which part of the content is actually illegal. This often leads to excessive blocking to ensure compliance with a request.

Submission: *It is suggested that MeitY develops a Standard Operating Procedure and a standardised form through which it can communicate take down requests to intermediaries.*

This form could be adopted at all levels and can consist of the following:

- *Provision of law under the IT Act that the content is sought to be taken down*
- *Nature of illegal content and reasons for blocking*
- *Contact details of person with whom the take down request can be appealed/discussed.*

6. Rule 3 (9)

Rule 3(9) has been introduced by the Draft Rules and requires the intermediary to deploy ‘*technology based automated tools*’ or appropriate mechanisms for ‘*proactively identifying and removing or disabling public access to unlawful information or content.*’

The following issues need to be considered relating to the proposed addition:

a) **Role of Intermediary:**

The proposed actions to be undertaken by an intermediary go against the exact role an intermediary is expected to perform.

As discussed in para 1.d) above, in the *Shreya Singhal* case, the SC specifically recognized that it would be difficult for intermediaries to act when millions of requests for takedown were made and the intermediary was required to judge which requests were legitimate, lawful/unlawful and which were not. In the case of *Kent Ro Systems Ltd. & Anr. v Amit Kotak & Ors*²² before the High Court of Delhi, the court recognized that the question of whether intellectual property had been infringed was a technical question which courts struggled with. The court held that nothing in the IT Act required intermediaries to screen all goods / information hosted on its platform for infringement of the rights of persons who have made complaints in the past relating to infringement.

Thus, Rule 3(9) seeks to cast an unfair burden on intermediaries to proactively screen information, determine whether it is unlawful, and take steps to disable/remove access when it is found to be unlawful. The intermediary is placed in an adjudicatory role, as opposed to a mere conduit of information, in contradiction to the judgments in *Shreya Singhal* and *Kent Ro*.

b) **Disregards different types of intermediaries:**

By imposing such a sweeping requirement, this Rules does not appear to take into account the fact that certain intermediaries do not make content available to the public, for example, cloud infrastructure providers. These intermediaries do not access user data and do not have means of identifying one data set from the other. This obligation casts an unnecessary burden which is practically not going to be possible on such intermediaries to monitor content and take down content.

c) **Risk of Over Blocking:**

²² CS (Comm) 1656 of 2016

If automated detection and filtering measures are incorporated, it could affect the accuracy of the content blocked and result in accidental blocking of legitimate content and over blocking, consequently leading to harm to the end users. Under such cases, the intermediary may also be liable to the users under the proposed Personal Data Protection law.

That said, if a court/Government agency identifies certain categories of content as unlawful content, intermediaries may be able to take down such specified content, such as:

- (i) Child pornography
- (ii) Certain offensive words
- (iii) Content pertaining to dangerous online games such as the Blue Whale game

This route would be preferable as opposed to the intermediary being the judge of what content it must proactively takedown.

Submission: We recommend that Rule 3(9) is deleted in its entirety from the Draft Rules.

7. Rule 3(10)

Rule 3(10) of the Draft Rules requires that the intermediary report cyber security incidents and also share information related to 'cyber security incidents' with the Indian Computer Emergency Response Team ("CERT").

Section 70B (6)²³ of the IT Act and the Information Technology (The India Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 vest CERT with broad enough powers to require intermediaries to report cyber security incidents to it. Accordingly, there is no need to require intermediaries to undertake an independent obligation to report cyber security incidents to CERT under this rule.

Submission: We recommend that Rule 3(10) is deleted in its entirety. Intermediary Guidelines 2011, Rule 3(10) penalizes the intermediary for non-compliance with the said CERT Rules through loss of safe harbor. As stated earlier, there is no nexus of the reporting requirement (in Rule 3(10) to Section 79 of the IT Act.

²³ Section 70B - Indian Computer Emergency Response Team to serve as national agency for incident response

...

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.

Notwithstanding the above, if it is to be retained, we suggest that the rule is amended to cross-refer to the responsibility of intermediaries under Section 70B (6) of the IT Act, instead of introducing a fresh obligation under this rule.

8. Rule 3(11)

Rule 3(11) of the Intermediary Guidelines 2011 prohibits an intermediary from knowingly deploy, install or modify the technical configuration of a computer resource, or become party to any act which may change the normal course of operation of a computer resource²⁴.

The Rule 3(11) suffers from the following issues:

a) Ultra Vires Section 79

Rule 3(11) appears to be ultra vires Section 79 of the IT Act. As discussed above, the purport of Section 79 is to provide intermediaries with immunity from third party content made available or hosted on their platforms, subject to certain prescribed conditions. The obligation under Rule (11) appears to be beyond the scope of this purpose and is accordingly *ultra vires* Section 79 and should be deleted in its entirety.

b) Inhibition of Innovation

This rule has the potential to inhibit innovation and enhancements to computer resources. Intermediaries should have the freedom to make improvements and enhancements to computer resources.

Submission: We suggest Rule 3(11) should be deleted in its entirety from the Intermediary Guidelines 2011.

²⁴ Rule 3(11): The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:
Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

MIT/79/065

Suggestions on the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 released on 24 December 2018

Background and Context

There are approximately 106 million cigarette smokers in India¹, making it home to 11% of the world's smokers. Smoking is a leading cause of preventable death and disease in India - approximately 900,000 people die each year from smoking related illnesses² which costs the government ~\$22.4 billion per annum (based on a 2011 estimate).³

Quitting cigarette smoking or tobacco consumption in any form has no universally accepted method and many patients struggle with cessation. In such cases, it is pragmatic for a doctor to suggest switching to less harmful ways of nicotine consumption with the ultimate goal of quitting. **Nicotine patches or e-cigarettes, therefore, have helped many smokers or tobacco chewers assuage the craving and aided a healthier lifestyle.**

It is important to note here that vaping is not the same as smoking as there is no combustion that is taking place. Combustion from smoking generates significant level of tar, carbon monoxide and other chemicals out of which 69 are known carcinogens. Combustible cigarettes accelerate cancer causes by releasing chemicals. Second-hand smoking or passive smoking from combustion affects not only increases the risk of coronary heart disease by 25-40% - almost the same level as a smoker, but also causes numerous health problems in infants and children, including more frequent and severe asthma attacks, respiratory infections, ear infections, and sudden infant death syndrome. Vaping products on the other hand do not result require combustion to deliver nicotine and as a result do not generate harmful chemicals at the level of combustible cigarettes.

Scientific Evidence

There are many studies that show that vaping is indeed a substantially safer alternative to tobacco consumption and as such should be an essential component for harm reduction. Some of these are as below:

- In its independent evidentiary review, Public Health England has categorically concluded that *“Vaping poses only a small fraction of the risks of smoking and switching completely from smoking to vaping conveys substantial health benefits over continued smoking. The previous estimate that, based on current knowledge, vaping is at least 95% less harmful than smoking remains a good way to communicate the large difference in relative risk unambiguously so that more smokers are encouraged to make the switch from smoking to vaping.”* It has further

¹ See <https://timesofindia.indiatimes.com/india/india-is-second-to-china-in-terms-of-numbers-of-smokers/articleshow/64401783.cms>

² See <https://files.tobaccoatlas.org/wp-content/uploads/pdf/india-country-facts-en.pdf>

³ John RM, Rout SK, Kumar BR, Arora M. Economic Burden of Tobacco Related Diseases in India, New Delhi:Ministry of Health and Family Welfare, Government of India; 2014.

observed that *“To date, the levels of metals identified in e-cigarette aerosol do not give rise to any significant safety concerns, but metal emissions, however small, are unnecessary.”* On assessment of exposure to harmful constituents PHE has observed that *“biomarkers of exposure assessed to date are consistent with significant reductions in harmful constituents and for a few biomarkers assessed...similar levels to smokers abstaining from smoking or non-smokers were observed.”*⁴

- The Royal College of Physicians has also opined that *“Toxin levels inhaled from vaping products under normal conditions are likely to be well below prescribed threshold limit for occupational exposure, which make the probability of significant long-term harm unlikely.”*⁵
- The National Academies of Sciences, Engineering and Medicine (NASEM) has concluded in relevant part that *“there is conclusive evidence that completely substituting e-cigarettes for combustible tobacco cigarettes reduces users’ exposure to numerous toxicant and carcinogens present in combustible tobacco cigarettes”* and there is substantial evidence that completely switching from regular use of combustible tobacco products to vaping results in reduced short term adverse health outcomes in several organs systems. As such, NASEM has concluded that *“e-cigarettes pose less risk to an individual than combustible tobacco cigarettes”* and *“complete switching from combustible tobacco cigarettes to e-cigarettes would be expected to reduce tobacco-related health risk.”* Lead authors of the NASEM report on vaping, Drs. Eaton and St. Helen, also published a follow-on Evidence to Practice article, which recommended that, *“if a smoker’s initial treatment has failed or not been tolerated, or if the smoker refuses to use approved medications and counselling and wishes to use e-cigarettes to aid quitting, physician should encourage the smoker to switch completely to e-cigarettes. We agree with Public Health England that behavioral support should be provided to smokers who want to use e-cigarettes to help them quit smoking, and that health professionals should receive education and training in use of e-cigarettes in quit attempts.”*⁶
- The American Cancer Society has issued a statement that stipulate basis the available scientific evidence the use of vaping is less harmful than smoking cigarettes. It has further observed that despite clinical advice, many smokers *“...will not attempt to quit smoking cigarettes and will not use FDA approved cessation medications. These individuals should be encouraged to switch to the least harmful form of tobacco product possible; switching to the exclusive use of e-cigarettes is preferable to continuing to smoke combustible products.”*⁷
- The American Heart Association has observed that *“E-cigarettes either do not contain or have lower levels of several tobacco-derived harmful and potentially harmful constituents compared with cigarettes and smokeless tobacco. In comparison with NRTs, e-cigarette use has increased*

⁴ McNeill A, Brose LS, Calder R, Bauld L and Robson D (2018). Evidence review of e- cigarettes and heated tobacco products 2018. A report commissioned by Public Health England. London: Public Health England.

⁵ Royal College of Physicians. *Nicotine without smoke: Tobacco harm reduction*. London: RCP, 2016.

⁶ The National Academy of Science, Engineering and Medicine, Committee on the Review of Health Effects of Electronic Nicotine Delivery Systems, Public Health Consequences of E-Cigarettes 11(2018).

⁷ See <https://www.cancer.org/healthy/stay-away-from-tobacco/e-cigarette-position-statement.html>

at an unprecedented rate, which presents an opportunity for harm reduction if smokers use them as substitutes for cigarettes.”⁸

- David B. Abrams from the College of Global Public Health, New York University, writes in the April 2018 issue of Annual Review of Public Health: *“A diverse class of alternative nicotine delivery systems (ANDS) has recently been developed that do not combust tobacco and are substantially less harmful than cigarettes. ANDS have the potential to disrupt the 120-year dominance of the cigarette and challenge the field on how the tobacco pandemic could be reversed if nicotine is decoupled from lethal inhaled smoke. ANDS may provide a means to compete with, and even replace, combusted cigarette use, saves more lives more rapidly than previously possible.”⁹*
- In a recent study published in the New England Journal of Medicine, a randomized control trial of 886 smokers revealed that 18% of smokers who used vaping products remained smoke-free after a year compared to 9.9% of smokers who used nicotine replacement therapy. This clearly shows that vaping products are becoming effective smoking cessation tools and are almost two times more effective than nicotine replacement therapy products.¹⁰

Untenability of Regulation on ENDS in India

We notice a confusion and inconsistency in Draft Rule 3(2)(j) that requires intermediaries to include in their rules and regulations, privacy policy or user agreement the condition that users of the intermediary not host, display, upload, modify, publish, transmit, update or share any information that *“threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder.”*

We believe that the mention on ENDS under Draft Rule 3 (2) (J) is in pursuance of the Advisory issued by the Ministry of Health and Family Welfare on August, 2018.¹¹ It is important to note here that the said Advisory has failed to take into consideration the emerging and arguably authoritative scientific evidence on ENDS or vaping products being a safer alternative to cigarettes.

Further the Advisory encourages States to take measures to prohibit sale (including online sale), manufacturing, distribution, importation and advertisement of Electronic Nicotine Delivery Systems (ENDS) in their respective jurisdictions **except for the purpose and in the manner, to the extent, it is allowed under the Drugs and Cosmetics Act.**

⁸ See <https://www.ahajournals.org/doi/10.1161/CIR.000000000000107>

⁹ Abrams et al, Harm Minimization and Tobacco Control: Reframing Societal Views of Nicotine Use to Rapidly Save Lives, Annu. Rev. Public Health 2018. 39:193–213

¹⁰ See <https://www.bbc.com/news/health-47041111>

¹¹ Ministry of Health and Family Welfare, Government of India. *Advisory on Electronic Nicotine Delivery Systems (ENDS) including e-Cigarettes. Heat-Not-burn devices. Vape. e-Sheesha. e-Nicotine Flavoured Hookah and the like products dt. 28 August 2018.* Accessible as F.No- P -16012 / 19 /2017

However, through its own admission, in the 48th Meeting of the Drugs Consultative Committee on 24th July 2015, the Ministry of Health & Family Welfare held that “*“E-cigarettes are not covered under the definition of the term ‘drug’ and therefore do not come under the purview of Drugs and Cosmetics Act, 1940. E-cigarettes therefore cannot be regulated under the provisions of the said Act.”*”¹²

Therefore, while the Draft Rule **proposes that ENDS can be promoted through an intermediary to the extent that is approved under the Drugs and Cosmetics Act, 1940, but in reality, Drugs and Cosmetics Act doesn’t cover ENDS at all.**

Thus, the prohibition on ENDS or vaping products goes against the findings of existing research and has an unsound and untenable legal basis. At the same time, it is noticed that while Draft Rule 3(2)(j) attempts to prohibit public information that can threaten public health and safety as such, ENDS are not proven to be a public health risk. In fact, the aforementioned evidence proves that it is a reduced risk product which can serve significant public health benefits. This restriction is beyond the reasonable restrictions permitted under Article 19(2) of the Constitution of India and is not in consonance with the judgment of the Hon’ble Supreme Court in the matter of *Shreya Singhal vs. Union of India*.¹³

The Indian Consumer Protection Act of 1986 also recognises the right to information for any consumer as long as it is not false or misleading. Verified and scientific information regarding consumer products should be made available to the public to increase consumer awareness and to facilitate informed decision-making among consumers. **The lack of information regarding a reduced harm alternative to combustible, tobacco-based cigarettes will, therefore, also be a negation of the rights of the Consumer under the Consumer Protection Act, 1986.**

Recommendation

In summation, it is humbly submitted that while the spirit of Draft Rule 3(2)(j) is positive as it endeavours to prohibit public dissemination of information that can endanger public health, the extension of the rule into prohibition of ENDS actually deprives the consumer of an informed choice with respect to a safer and healthier alternative to combustible cigarettes. In fact, this might detract from the government’s overall harm reduction and tobacco control objectives. **Thus, it is suggested that Draft Rule 3(2)(j) be amended and the following clause should be inserted in its place, without a reference to ENDS.**

“(j) threatens public health or safety, including, promotion of products which have a scientifically proven risk to public health or safety”

To this end, we will be happy to assist in any additional drafting exercises, or further input, as may be required.

¹² Central Drugs Standard Control Organisation, Ministry of Health and Family Welfare, Government of India. *Report of the 48th meeting of the Drugs Consultative Committee held on 24 July 2015 at New Delhi*. Accessible at <http://cdsco.nic.in/writereaddata/Report-of-48th-DCC-Meeting.pdf>

¹³ AIR 2015 SC 1523.

MIT/79/067**REPORT****1. Background:**

The Information Technology (Intermediaries' Guidelines) Rules, 2011¹ ("**Intermediary Rules**"), framed in pursuance of S.79(2)(c) of the Information Technology Act, 2000 (as amended) ("**IT Act**") prescribes duties of Intermediaries.

The Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 ("**Draft Intermediary Rules, 2018**") appears to have been prepared after elaborate discussions with multiple stakeholders including various Intermediaries and Law Enforcement Agencies ("**LEA**"). The press release sets out various offences being committed online, which appear to have triggered this exercise of review and modifications. Whilst the Government of India ("**GOI**") intent to ensure protection against misuse of the online domain is apparent, and its stated intent to ensure free speech and expression is encouraging, the balance that is sought to be struck ought to protect victims of heinous crimes from being further victimized through vicious online dissemination.

As with any attempt to just patch a hole or "band aid syndrome" the Draft Intermediary Rules, 2018 suffers from inconsistencies and anomalies. The draft presumes the correctness of a substantial portion of the existing Intermediary Rules and only seeks to make some additions, as per its perception of "need". The same has resulted in several inherent errors in the existing Intermediary Rules being overlooked. If GOI has undertaken this exercise of reviewing the Intermediary Rules, it is expedient for it to review the same in its entirety and not just in bits and pieces.

¹ Available at [http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511\(1\).pdf](http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf);

It may also be expedient, whilst reviewing the Rules to take note of the powers granted under S.67C IT Act², which again has been gravely overlooked and ensure that suitable provisions are incorporated to make it consistent with the requirements of the above provision. This will obviate the need for multiple Rules, which may also result in further inconsistencies.

The said Rules play an important role in an otherwise unregulated domain. It is therefore imperative that the balance is struck, as set out in the press release, between free speech and expression, which does not impinge on other persons' rights. It is also imperative that whilst free speech is protected the same does not shield heinous and criminal offences online such as dissemination of child pornography, content pertaining to violent crimes against women, revenge porn and such or other offensive material. Upon dissemination, such content has the power to cause serious consequences.

It is humbly submitted that the proposed Draft Intermediary Rules, 2018 falls short in meeting the above requirements. The inputs on provisions, which may be considered for review; inconsistencies in the proposed draft and the modifications thereto that may be considered are set out in details hereunder.

² “**67C. Preservation and retention of information by intermediaries.** – (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.”

2. Comments / Action Points requested on the draft Personal Data Protection Bill, 2018³

a. Rule 2 (e): Definition of Critical Information Infrastructure (“CII”):

The above Rule adapts the definition of CII in S.70 of the IT Act, which is reproduced in part, as under:

“70. Protected system.– (1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.–For the purposes of this section, “Critical Information Infrastructure” means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

...”

Issues / Concerns:

Neither the Intermediary Rules nor the IT Act therefore actually set out CII. It may be expedient for reference therefore not only to the IT Act but to the Rules or Government Order (“GO”) or notification setting out CIIs. There appears to be substantial opacity in this regard, as on date with even the website of the National Critical Information Infrastructure Protection Centre (“NCIIPC”) not providing sufficient information in this regard⁴.

³ http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf;

⁴ Transport; Power & Energy; Telecom; Government; Banking, Financial & Insurance Services; Strategic & Public Enterprises; are all listed on the site but without further information of the source of such categorization;

Suggestion:

The definition of CII to refer not only to S.70 IT Act but also to the Rules / GO / notification under which CII have been listed.

b. Rule 2 (f): Definition of Cyber Security Incident:

The intent of the definition appears to be to include all violations under S.43 of the IT Act. However, the definition paraphrases in part provisions of S.43 IT Act.

Issues / Concerns:

The partial reproduction of S.43 without reference to S.66 IT Act is certainly likely to create confusion and inconsistency between the provisions. It is expedient to ensure consistency, as the assumption would be that a Cyber Security Incident would be that which would amount to an offence under the IT Act.

Suggestion:

Cyber Security Incident may be defined:

- a. *“as those incidents amounting to a violation under S.43 IT Act”;*
OR
- b. *“as incidents amounts to an offence under S.66 of the IT Act”;*
OR Preferably
- c. *“as incidents amounting to offences under Chapter XI of the IT Act” (or at least certainly offences under S.66, 66C, 66D, 66E, 66F, 67, 67A & 67B – for Cyber Security Incidents affecting Society or CII are not merely those under S.66 IT Act (which in turn reads S.43 IT Act into it));*

c. **Rule 2 (l): Definition of “User”:**

Though the definition begins with the words “*User means any person accessing or availing any computer resource...*” the continuation of the definition i.e., “*for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary*” does not encompass a passive viewer of online sites but only appears to include active users.

Issues / Concerns:

The above definition needs to encompass a passive user also, as the rules, regulations and policies on any online site is as applicable to a passive user as it is to an interactive one who uploads etc., Further even sites offering static content would fall within the category of “Intermediaries” and hence a user of such sites need to be covered in the above definition.

Suggestion:

The above definition may be expanded to include a passive user also and not just those “*hosting, publishing, sharing, transacting, displaying or uploading information or views*” or “*other persons jointly participating in using the computer resource*”.

d. **Rule 3(j) & (k): Inclusion under the Draft:**

The following Rules have been included as (j) & (k) under the Draft Intermediary Rules, 2018:

“(j). products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;

(k) threatens critical information infrastructure.”

Issues / Concerns:

The above additions are extremely open – ended and are invitations for misuse. Rule (j) for instance may even be invoked to haul up someone posting a picture smoking a cigarette or having a drink at a party. If the intent of GOI was to stop “**commercial**” advertising through online platforms being accessible in India, the same not only ought to be explicitly articulated but also supported by legislative provisions. Neither are done at this juncture.

Similarly, Rule (k) also suffers from ambiguity. Innumerable cases dealt with under the now struck down S.66A IT Act have demonstrates the extent and possibility of misuse of such open-ended provisions. To have a Rule setting out vague terms as “threatens” CII is bound to be misused. It was open to the ministry to add a Rule to protect against terrorist acts, as defined under S.66F⁵ against CIIs.

Suggestions:

- a. Rule (j) to be deleted;
- b. Rule (k) as it is proposed to be deleted;

⁵ The author’s reservations on the legality and validity of S.66F are already articulated extensively in her book “**Technology Laws Decoded**”. It is expedient to remedy the patent errors in S.66F IT Act also but the same are not set out herein as this report is limited to the Draft Intermediary Rules, 2018;

- c. If required, a new Rule may be added specifically protecting against threats amounting to offences under S.66 or S.66F IT Act against “*critical information infrastructure.*”;

e. **Old Rule 3(5) (present proposed Rule 3(4)): Intimation to Users:**

The addition to the Old Rule 5 now mandates intimation to Users “*at least once every month*” that in the event of non-compliance, Intermediary may terminate services.

Issues / Concerns:

It is not clear how such communication is to be made, for online sources or by search engines. The definition of Intermediary being open-ended such requirement would warrant all kinds of digital platforms constantly sending out messages to “users”.

The intent seems to be to ensure that the warnings intended under Rule 3 are actually implemented in letter and spirit. For this a more streamlined implementation option may be adopted.

There is also no mode or manner for ensuring compliance i.e., Government cannot audit or review compliance, as neither the periodicity specifically nor the mode of issuance are stipulated. Even if they were it is not practically feasible for the Government to monitor the innumerable Intermediaries to ensure compliance.

Suggestions:

- a. GOI may consider mandatory compliance by content hosting platforms to carry specific notices or warnings on their landing pages. Or visibly on their sites;

- b. They may also require periodic push notifications to be issued by chat platforms to users;
 - c. Each such notification or warning message ought to specifically address ONE specific violation which should not be committed by users i.e., that “*uploading of child pornography is an offence*” etc., The same would ensure effectiveness of the notice or warning instead of generic warnings about “compliance”;
 - d. The notice may also include the penalties / punishments under law;
 - e. These could be extended to notices of financial frauds / recent bugs or vulnerabilities / or developments materially affecting users of specific sites.
 - f. The requirement may be positioned as a public interest requirement rather than as a punitive measure;
- f. **Old Rule 3(7) (New proposed Rule 3(5)): Assisting Law Enforcement:**

The above Rule has been modified as under:

“(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised. “

The Rule mandates cooperation by Intermediaries within **72 hours**. The modifications appear to have been inserted keeping in mind long-standing concerns of LEAs.

Issues / Concerns:

The importance of the above provision cannot be gainsaid. However this should not result in the following eventualities:

- a. Intermediaries claiming **72 hours instead of 24 hours** (as set out under Rule 8 of the amended Draft Intermediary Rules, 2018) to take ANY action including take down. Whilst the requirements under Rule 5 & Rule 8 are explicit, the above possibility cannot be ruled out. Such nuances may also elude the common man. Hence it is expedient to clarify and ensure compliance for takedowns issued as per due process;
- b. Possibility of abuse by investigating agencies. It may be expedient for effective due process checks and balances to be introduced to ensure that illegal or unregulated requests are not entertained for the sole purpose of victimization – may be for political or other reasons.
- c. Again, the S.66A IT Act instances clearly point to such possibilities. It cannot therefore be ruled out that originators will be called upon to be traced without cases being registered or based possibly on false or untenable cases being registered. At the stage of the request neither the person, who's records are being called for nor the Intermediary would be in a position to contest the same, as no due process procedure for this has been provided.

Suggestions:

- a. Specific clarification to be provided both in Rule 5, as well as in Rule 8 that the necessity of take downs ought to be complied with

within 24 hours or as prescribed under Rule 8 and that nothing in Rule 5 would extend such timelines;

- b. To protect against misuse:
- i. Specific procedures for submitting protest petitions or review of requests from Government Agencies or LEAs may be incorporated;
 - ii. Immediate compliance within the stipulated times to be mandated for registered complaints (i.e., upon registration of First Information Reports or FIRs);
 - iii. Requests to specify if the details sought are pertaining to a suspect or witness or victim;
 - iv. Details of complaint received; details of complainants and the actual content of the complaint to be shared to enable independent review by Intermediaries to the extent of allowing them to file protest petitions when mandated;
 - v. Such review to be undertaken by independent agencies or seniors of the issuing authorities, as would be specified in the Rules;
 - vi. Provision for retention of data including metadata by Intermediaries pending such review to be included independent of Rule 8;
 - vii. Provision for persons who's information is shared by Intermediaries to file protest petitions before the appropriate authority, upon information through LEAs, either to review such order or its own order based on an Intermediary's Petition;
 - viii. Explicit procedures for receipt, retention and deletion of such data upon completion of investigation, where such investigation does not lead to registration of complaints or continuation of investigations and / or when the appropriate authority reviews the agency's order or its own order and holds against such disclosure;

- ix. All of the above to be completed in a timebound manner with the Rules setting out such specified timelines;
- x. Such or other processes or procedures to ensure protection of free speech and protection against misuse of provisions to be incorporated. Else this very provision may result in the “chilling effect” much emphasized in multiple litigations before the Hon'ble Supreme Court;

g. Old Rule 3(6):

Rule 6 under the extant Intermediary Rules reads thus:

“The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.”

It appears that the above provision has been inadvertently deleted in the proposed Draft Intermediary Rules, 2018.

Issue / Concern:

The above provision is material to ensure due adherence to Indian laws by Intermediaries and hence ought to be retained / reinstated, more so when the deletion appears to be inadvertent.

Suggestion:

Reinstatement of the above old Rule 3(6).

- h. **New Rule 3(7): Requirements of Intermediaries with “50 lakh users”:**

The following new Rule has been included in the Draft Intermediary Rules, 2018:

“(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;

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

(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.

The patent intent behind the above provision appears to be to ensure speedy response by those Intermediaries having a large user base of Indians.

Issues / Concerns:

The above inclusion suffers from ambiguity. There is no methodology to gauge the minimum qualifying number i.e., “fifty lakh users in India”. “Users” of online domains may not be a static number always. For instance, a site may have a user visiting it once. It may have fifty lakh views in one month or year and none during the next month or year. With the definition of Intermediaries being so wide, this is so for different domains.

It is not clear at what stage such Intermediaries are required to restructure their organizations to comply with the above Rule. Further the definition of “user” as it stands today only includes persons actively involved on a domain. It is not clear therefore if the above rule would apply even to a static site where users are not allowed to upload or share content.

Hypothetically, even if such requirement were to be clarified as “*any Intermediary who has at any point of time had fifty lakh users or views*” has to forthwith comply with such requirement, incorporation of a company is not an easy task. There are extensive compliances required not only for such incorporation but also for continuation of such corporate entity. If a site for instance had a burst of views or users and then goes defunct, compliance with the above Rule would mandate incorporating a company and then closing the same down.

The Rule also includes the Government listing specific entities to comply with the requirement. The assumption in such instance would be that these entities would consistently have a large Indian userbase. In such instances, creating a local presence would certainly assist law enforcement and regulatory compliance. Whether such compliance would require setting up of a corporate entity again is moot. It appears that such requirement may have been inserted more from a tax angle rather than from a compliance perspective.

Suggestions:

- a. Requirement of “50 lakh users” being the threshold for compliance to be removed;
- b. Requirement for establishing a local corporate entity to be reviewed;
- c. Specific and unambiguous thresholds to be set out for even listing of companies for compliance. For instance, the SEBI Act specifies turnover of Rs. One Crore or more for registration processes to be followed by companies in some instances such as timeshare companies. Such or similar thresholds may be introduced, which are tangible and viable;

- d. Requirement of permanent registered office to be limited to such of those entities specifically listed by the GOI;
 - e. Separate the requirement of local nodal officers or for designated officers to be stipulated by each entity, from the above requirements. For instance sites offering specific services (such as hosting of online video content) may be required to have named nodal / grievance officers and process for escalation with such details being provided online, as is envisaged under present rules. Such requirement ought not to be diluted by clubbing with specific or limited number of entities to be listed by Government or falling within specified thresholds;
- i. **New Rule 3(8) (In lieu of Old Rule 4, which has been deleted):
Removal / Disabling of online Content:**

The following new Rule has been inserted under the proposed Draft Intermediary Rules, 2018:

*“(8) 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 Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ **one hundred and eighty** days for investigation purposes, **or for such longer***

period as may be required by the court or by government agencies who are lawfully authorised.” (emphasis / highlight added)

Issues / Concerns:

The above Rule is merely a redacted version pursuant to the decision in *Shreya Singhal v. UOI (2015)*. The Rule appears to take the stated position in the said decision too literally by reproducing Article 19(2) in its entirety thereby creating more ambiguity than there was prior thereto. It also limits thereby, the rights of Courts to pass orders, as per due process, which Intermediaries will be required to comply with.

The requirement under *Shreya Singhal's judgment* would have been duly met if the requirement for Intermediaries to take down content based on user complaints had been deleted. The above revision appears to complicate and confound the issue.

It is also expedient to review general laws to empower judicial magistrates to pass orders for specific provisions, as general practise illustrations clearly demonstrate the ambiguity with respect to their powers, especially in cases of law and order situations.

Further, reference to Sub Rule 6 of Rule 3 seems irrelevant, as the same related to Reasonable Practises whereas the take down within 24 hours or for that matter retention of evidence has no bearing to the same.

Further the last addition is material to ensure compliance with S.67C IT Act. However GOI may consider including or till such time as the Intermediary is granted leave by the concerned Court to delete evidence.

Once Intermediary has been informed that the evidence pertains to an offence or violation, through a court order or Government agency, it is only just that they then have to seek leave to delete and that such leave ought to be from only a Court of law dealing with the relevant case (and not by the government agency). This will protect victim's interests.

Suggestions:

- a. Restate the old Rule 3(4) with the deletion of user demands for take downs;
- b. Introduce processes however, for what would amount to "knowledge" of Intermediaries – Indian laws may draw from international options and / or set out constitutionally binding processes to ensure that content pertaining to heinous offences such as child pornography or gender neutral victimization through online processes do not mandate the arduous process of obtaining court orders or for filing of Criminal complaints to warrant take downs. A more robust take down process instead of merely reproducing Article 19(2) or having an ambiguous process ought to be considered;
- c. Remove reference to Rule 3(6) as it has no bearing for compliance with the above Rule 8;
- d. Expand the requirement for retention of evidence and to link it to compliance with S.67C, as the same provides for a specific criminal punishment in the event of non-compliance and to allow Intermediaries to delete upon receipt of a Court order only from the competent court dealing with the specific matter.
- e. The above may seem onerous to unstructured Intermediaries but the same is balanced on the anvil of victim needs rather than inconvenience of Intermediaries.

j. **New Rule 3(9):**

The following new Rule has been included under the Draft Intermediary Rules, 2018:

“(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content”

On the face of it, the above Rule appears incomplete. The same may merely be due to the absence of punctuation marks (full stop at the end of the sentence). The above Rule also appears to be pursuant to Supreme Court matters.

Issues / Concerns:

Intermediaries are bound to contest the above on grounds of violation of the protections given to them under S.79(2). The above Rule ought to be specific to clarify that tools required to be deployed are automated and without human intervention followed up through human verification process. The Rule would also have to withstand the test of free speech and Article 19(2) of the Indian Constitution. For this, there has to be put in place checks and balances to ensure victim rights as opposed to rights of users and Intermediaries.

Suggestions:

- a. The ambiguity in the above provision to be rectified;

- b. The provision to clarify that the above would be an automated process which would not amount to pre-censoring through subjective satisfaction of the Intermediary;
- c. Processes for review and reinstatement of legal or genuine content to be provided for to enable free speech;
- d. Whilst the above technology cannot be frozen in time indicative words such as “automated processes enabled through technologies such as Artificial intelligence” etc., may be considered to be included to give more clarity and direction to Intermediaries and to stand the test of judicial review;
- e. Specific objects and reasons for the above inclusion would also be expedient to sustain it legally – this may be included along with the Supreme Court case, if any, which may have prompted this inclusion;
- f. Specific restrictions on Intermediaries from indulging in subjective pre-censoring to also be considered. The same to be balanced with the requirements warranting the inclusion of the above Rule;

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)



Free Software Movement of India

www.fsmi.in

Dear Sir/Madam

The following is the submission of the **Free Software Movement of India** in response to the invitation of comments/suggestions on the Draft Information Technology (Intermediary Guidelines) Rules 2018.

Duties of Intermediaries Under the Information Technology Act, 2000

Intermediary is defined under section 2(w) of the Information Technology Act, 2000 as reproduced below:

(w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecoms service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;

This definition is broad and encompasses services associated with information technology whether virtual or physical.

Section 79 of the Information Technology Act, 2000 lays down conditions under which intermediaries will attract liability as well as the conditions under which liability will not be attracted.

The circumstances under which immunity from liability will be available to intermediaries are:

- the function of the intermediary is limited to providing access to a

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

- the intermediary does not:
 - initiate the transmission
 - select the receiver of the transmission,
 - select or modify the information contained in the transmission
- the intermediary observes due diligence while discharging his duties under the Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

Whereas the circumstances under which the intermediaries will be held liable are:

- the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
- upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful

act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Third party information under this section refers to information dealt with by an intermediary in the capacity of an intermediary.

Section 87(zg) empowers the Central Government to frame Rules regarding the guidelines that intermediaries are to observe under section 79(2).

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

Section 69(3) mandates that The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to:

- provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
- intercept, monitor, or decrypt the information, as the case may be; or
- provide information stored in computer resource.

The caveat here is that the duty of a subscriber, intermediary or any person in charge of a computer resource is invoked only when called upon by an agency referred to in subsection 1.

Failing this, subsection 4 states that:

The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.]

Subsection 1 of section 69 allows any agency authorised by the Central Government by order, with reasons recorded in writing to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

The conditions under which such order may be passed are that the Central Government or any of its authorised officers should be satisfied that it is necessary or expedient to do in the interest of:

- the sovereignty or integrity of India,

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

- defence of India,
- security of the State,
- friendly relations with foreign States or
- public order or
- for preventing incitement to the commission of any cognizable offence relating to above or
- for investigation of any offence.

Thus it can be seen that:

1. Intermediary has a wide definition under the Act (section 2(w)).
2. Intermediaries do not attract liability where they play no role in the generation of information (section 79(2) and (3)(a)).
3. Intermediaries will attract liability under section 79(2)(c) for failing to observe the guidelines prescribed under section 87(zg).
4. Intermediaries will attract liability under section 79(3)(b) for failing to expeditiously remove or disable access to material without vitiating the evidence that is used to commit an unlawful act.
5. Intermediaries will also attract liability under section 69(4) for failing to comply with section 69(3).

The Draft Information Technology [Intermediaries Guidelines (Amendment) Rules, 2018

Under Rule 2, two definitions clauses have been added, i.e. the definitions of “Appropriate Government” and “Critical Information Infrastructure”, for which the definitions under sections 2(1)(e) and the Explanation in section 70(1) of the Act respectively.

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

In Rule 3(2) the words “terms and conditions” have been substituted with “privacy policy”. **However, “privacy policy” as such has not been defined in the parent Act, nor the Rules.**

In Rule 3(2) clauses (j) and (k) have been added.

Clause (j) places a duty on the intermediary to inform users not to transmit information that threatens public health or safety in the form of tobacco products, Electronic Nicotine Delivery Systems (ENDS), alcohol and other intoxicants except in in the manner and extent as may be approved under the Drugs and Cosmetics Act, 1940 and the Rules made thereunder.

Due to the wide definition of intermediary which includes telecommunication service providers, internet service providers and other platforms such as Facebook, Gmail, Youtube, WhatsApp, Amazon and Filpkart, private messages between two persons would fall foul of this Rule. Such a broad provision will not pass the test of proportionality laid down in *Puttaswamy*.

Clause (k) places a duty on the intermediary to inform users not to transmit information that threatens critical information infrastructure.

Rule 3(4) has been substituted with a new provision by which intermediaries shall inform users at least once a month that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate access and usage rights of the user and remove the non-compliant information.

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

This provision does not put in place a system which provides the user a right to be heard.

Rule 3(5) lays down that the intermediary shall comply with lawful orders within 72 hours of communication to provide such information or assistance as asked for by any government agency or;

- security of the State or cyber security;
- or investigation or detection or
- prosecution or prevention of offence(s);
- protective or cyber security and matters connected with or incidental thereto.

The provision prescribes that the lawful order must be made in writing or through electronic means and state the purpose clearly. However, it should also be mentioned that the order, when

made through electronic means, must also contain a digital signature as defined in section 2(p) and prescribed under section 3 of the parent Act.

Considering the impact of the Rule, it is essential that only a court order qualify as a “lawful order” in this context.

The provision also mentions that the intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised. However, with the broad definition of intermediary under section 2(w) of the parent Act, even online journalistic portals fall within the ambit of “intermediary”.

This becomes problematic as the Press Council of India’s *Norms of*

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

Journalistic Conduct stipulate that the confidentiality of the source is to be respected. The only circumstance where the source may be revealed is when “*the source is voluntarily disclosed in proceedings before the Council by the journalist who considers it necessary to repel effectively a charge against him/her*”. **In this regard, this rule may be used to coerce such portals to reveal their sources, which may subject such sources to the risk of physical harm if not endless litigation.**

Similarly, traceability here is a vaguely defined term and in order to do so, intermediaries may have to break encryption or even worse, create backdoors to encryption from the very beginning. This has grave implications for freedom of speech and secure communication.

Rule 3(7) makes it mandatory for intermediaries with fifty lakh or more users in India, or is in the list of notified intermediaries to be a registered company under the Companies Acts of either 1956 or 2013. The intermediary shall have a permanent registered office in India, and shall appoint a nodal person available 24x7 to coordinate with law enforcement agencies.

At the outset, the mandatory provision that the intermediary shall be a registered company is discriminatory and will hamper the growth and development of smaller entities who may be operating as partnership firms.

This Rule also does not take into account websites such as Wikipedia and Github which are knowledge sharing platforms and fall within the definition of intermediary as laid down in section 2(w) of the Act. Neither website has a physical presence in India. This may subject these websites to unnecessary litigation or even be banned under the Rules so framed. Further, neither of these websites have specific registration or subscription processes.

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

Rule 3(8) mandates that on the basis of a court order or a notice from the appropriate government or its agency under section 79(3)(b), the intermediary shall remove the specified objectionable material relating to Article 19(2) of the Constitution of India within 24 hours without vitiating the evidence.

Further the intermediary shall retain the information and associated records for a period of one hundred and eighty days, or for such period of time as may be required by the court or by government agencies.

However, the requirement of retaining the information and associated records for a period of one hundred and eighty days is double of what was mandated under the Rules of 2011. If retention is required for investigation purposes, copies of the requisite information can be obtained within a shorter period of time by the law enforcement agencies.

Rule 3(9) stipulates that “The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

This Rule goes beyond the scope of the role of an intermediary as laid down in the parent Act as an intermediary is not a content creator and cannot have essentially editorial functions. Pre-censorship would be an editorial function and not envisaged for an intermediary.

Under section 79(2)(b)(iii) of the parent Act, the intermediary is not liable if the intermediary does

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

not select or modify the information contained in the transmission. However, draft Rule 3(9) mandates that the intermediary shall play a proactive role in identifying and removing or disabling public access to unlawful information or content.

This would then extinguish the immunity offered by section 79(2)(b)(iii) of the parent Act. Further, the failure to comply with this guideline will extinguish the immunity offered by section 79(2)(c) of the parent Act. This creates a situation where the intermediary will lose an immunity offered under law whether complying with the guidelines or not.

The use of automated tools for what is essentially censorship has the following problems:

- 1) There are no accepted standards for the functionality of such AI tools, which raises serious questions on its deployment on the large scale as suggested in the Rule.
- 2) Such automated tools cannot distinguish between reporting that is critical of the government or reporting in the mainstream media, and fake news, material that is intended to arouse hatred or cause violence.
- 3) The only way such automated tools would work is by only allowing a dumbed down version of news and views.
- 4) The cost of even such automated tools is well beyond the power of most intermediaries and therefore heavily weighed in favour of the large global monopolies.

This Rule by mandating the use of “technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

removing or disabling public access to unlawful information or content” does not provide for the application of mind.

In effect this provision empowers the intermediary to play the role of a censor without the application of mind nor an adequate mechanism for appeal. This Rule is arbitrary and will violate Article 14 of the Constitution which operates as a guarantee against arbitrariness.

The Hon’ble Supreme Court in *Shreya Singhal vs Union of India* on March 24, 2015 when reading down section 79(3)(b) and the Information Technology (Intermediaries Guidelines) Rules,

2011 made it clear that the intermediary’s liability in relation to orders whether from a court or from the appropriate government or its agencies, is limited to a specific request to block or remove such offensive material to the extent that it is struck by Article 19(2). In this regard, this provision violates the principle of *delegata potestas non potest delegari* (no delegated powers can be further delegated) as it delegates the powers of the State agencies to identify unlawful content and take appropriate action to the intermediaries.

It further gives such intermediaries quasi judicial powers by forcing them to take private decisions on what content is legally permissible. In the context of online news portals, the Press Council of India guidelines can regulate the content.

However, giving such editorial jurisdiction to internet service providers, telecommunication service providers and other such intermediaries greater power and obligations than is desired, both by content creators as well as the intermediary.

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

The right to freedom of speech and expression as contained in Article 19(1)(a) of the Constitution can only be restrained by Article 19(2) provided that such restraint passes the test of Article 14. **This Rule empowers the intermediary beyond the scope of the parent Act.**

The Supreme Court has held in numerous cases, notably in *The Secretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal*, AIR 1995 SC 1236, that

“The freedom of speech and expression includes the right to acquire information and to disseminate it. Freedom of speech and expression is necessary, for self expression which is an important means of free conscience and self fulfillment... The right to communicate includes right to communicate through any media that is available whether print or electronic or audio-visual. .. This freedom includes the freedom to communicate or circulate one's opinion without interference to as large a population in the country as well as abroad as is possible to reach. This fundamental right can be limited only by reasonable restrictions under a law made for the purposes mentioned in Article 19(2) of the Constitution. ” In the context of television, the Supreme Court stated “The broadcasting media should be under the control of the public as distinct from Government. This is the command implicit in Article 19(1)(a). It should be operated by a public statutory corporation whose composition must be such as to ensure its

impartiality in political, economic and social matters and on all other public issues... Airwaves being public property, it is the duty of the State to see that airwaves are so utilised as to advance the free speech right of the citizens which is served by ensuring plurality and diversity of views, opinions and ideas. This is imperative in every democracy where freedom of speech is assured.”

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh



Free Software Movement of India

www.fsmi.in

Under such circumstances, Rule 3(9) should not be written into law.

Regards

Y. Kiran Chandra
General Secretary
Free Software Movement of India

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally,
Hyderabad, Andhra Pradesh

Blank

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

**SUBMISSION REGARDING THE INFORMATION TECHNOLOGIES
INTERMEDIARIES GUIDELINES (AMENDMENT) RULES 2018, AS PER PUBLIC
NOTICE ISSUED BY THE MINISTRY OF ELECTRONIC & INFORMATION
TECHNOLOGY OF THE GOVERNMENT OF INDIA**

*Dr. Joan Barata Mir
Intermediary Liability Fellow
Center for Internet and Society
Stanford Law School (USA)*

The present submission has the object of providing comments and recommendations regarding a very specific provision included in the document mentioned in the title, that is the specific proposed duty for intermediaries to:

“deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

This provision is included in the provisions under paragraph 3, on *“Due diligence to be observed by intermediary”*.

This submission will be based on the most relevant international standards currently in place with regards to the role of private intermediaries vis-à-vis content moderation, particularly when automated tools are used (and imposed by competent authorities).

In his Report to the General Assembly of 11 May 2016¹, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated that content regulation in the digital world (included those provisions that may affect the role and responsibility of intermediaries), must avoid taking steps that *“unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal”*. The Report also stresses the fact that the development and use of technical measures, products and services by private entities must be regulated by the States with the aim of advancing freedom of expression. Such regulation should also *“provide the private sector, civil society, the technical community and academia meaningful opportunities for input and participation.”* Last but not least, the Report also emphasizes the need to avoid the imposition of pressures from States to private actors that may lead to restrictions on the right to freedom of expression.

In the Report to the General Assembly of 6 April 2018², the Special Rapporteur includes a few references and recommendations related to the use of automated mechanisms with regards to content moderation. It is particularly outlined that *“(a)utomated content moderation, a function of the massive scale and scope of user-generated content, poses distinct risks of content actions that are inconsistent with human rights law”* and therefore it is particularly important to consider *“the significant limitations of automation, such as difficulties with addressing context, widespread variation of language cues and meaning and*

¹ Available online at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement>

² Available online at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

linguistic and cultural particularities". It is also important to mention that the Report also reiterates the already well established international legal principle that "States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship."

In the most recent Report to the General Assembly, focusing on the intersection between artificial intelligence (AI) and human rights, the Special Rapporteur acknowledges the role and presence of AI in the digital communications environment, also highlighting its potential problematic nature. In particular, the Report underscores that "States (...) are pressing for efficient, speedy automated moderation across a range of separate challenges, (including) child sexual abuse and terrorist content" and warns about the fact that "(e)fforts to automate content moderation may come at a cost to human rights". In line with previous Reports (as it has already been shown), the Special Rapporteur insists on the fact that:

"Artificial intelligence-driven content moderation has several limitations, including the challenge of assessing context and taking into account widespread variation of language cues, meaning and linguistic and cultural particularities. Because artificial intelligence applications are often grounded in datasets that incorporate discriminatory assumptions,¹⁷ and under circumstances in which the cost of over-moderation is low, there is a high risk that such systems will default to the removal of online content or suspension of accounts that are not problematic and that content will be removed in accordance with biased or discriminatory concepts."

A very important warning in this sense also refers to the fact that:

"Artificial intelligence makes it difficult to scrutinize the logic behind content actions. Even when algorithmic content moderation is complemented by human review — an arrangement that large social media platforms argue is increasingly infeasible on the scale at which they operate — a tendency to defer to machine-made decisions (on the assumptions of objectivity noted above) impedes interrogation of content moderation outcomes, especially when the system's technical design occludes that kind of transparency."

Two important recommendations derived from the Report are: 1) "Artificial intelligence - related regulation should also be developed through extensive public consultation involving engagement with civil society, human rights groups and representatives of marginalized or underrepresented end users", and 2) "Individual users must have access to remedies for the adverse human rights impacts of artificial intelligence systems. Companies should put in place systems of human review and remedy to respond to the complaints of all users and appeals levied at artificial intelligence-driven systems in a timely manner."

Beyond international standards it also needs to be outlined that there are well-founded reports that systematically highlight the problems associated with the use of automated tools when moderating content online. Such problems relate to two main areas: their negative impact on freedom of expression and non-discrimination rights, and their lack of effectiveness with regards to properly tackling undesired and/or illegal content. See for example the study made

by Natasha Duarte, Emma Llanso and Anna Loup at the Center for Democracy & Technology “Mixed messages? The limits of automated social media content analysis”³.

On the basis of the abovementioned parameters we comment and recommend the following:

a) Considering the impact on human rights (particularly the right to freedom of expression) and the problems related to adequacy and effectiveness (particularly when applied to content moderation) the law shall not mandate the use of automated tools or similar mechanisms for proactively identifying and removing or disabling public access to unlawful information or content. The provision included in the draft is also problematic vis-à-vis international standards inasmuch as establishes a general content monitoring obligation for platforms.

b) It is recommended that the law includes safeguards with regards to the voluntary use of automated tools by intermediaries when enforcing their own terms of service and community guidelines, in line with international standards. Such safeguards may include proper human review and remedy mechanisms.

c) Tackling unlawful legal content must be consistent with international standards. In particular, provisions must be clearly established by law, pursue a legitimate aim and avoid any excessive or disproportionate restriction on the fundamental right to freedom of expression. Take down mechanisms must incorporate adequate review mechanisms for intermediaries and content providers, as well as avoid liability regimes that may lead to over removal of legitimate speech.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

³ Available online at: <https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/>

Mozilla Headquarters

331 E Evelyn Avenue
Mountain View, CA 94041
United States of America
650.903.0800

MIT/79/071

To
Mr. Ravi Shankar Prasad
Minister of Electronics and Information Technology
Government of India

31st January 2019

To the Hon'ble Minister Prasad,

Thank you for the opportunity to provide comment on the draft Information Technology (Intermediary Guidelines) Rules 2018, that are proposed to replace the rules notified in 2011.

Mozilla is a global community working together to build a better internet. As a mission-driven technology company, we are dedicated to promoting openness, innovation, and opportunity online. We are the creators of Firefox, an open source browser and the family of Firefox products, including Firefox Focus and Firefox Lite, as well as Pocket, used by hundreds of millions of individual internet users globally.

As we've highlighted before, illegal content is symptomatic of an unhealthy internet ecosystem. To that end, Mozilla recently adopted an addendum to our Manifesto, in which we affirmed our commitment to an internet that promotes civil discourse, human dignity, and individual expression. Our products, policies, and processes embody these principles. Ultimately, illegal content on the web – and substandard policy and industry responses to it – undermine the overall health of the internet and as such, are a core concern for Mozilla. We have been at the forefront of these conversations globally (most recently, in Europe), pushing for approaches that manage the harms of illegal content online within a rights-protective framework.

We support the consideration of measures to hold social media platforms to higher standards of responsibility. However, **in our filing below, we explain why the current draft rules are not fit-for-purpose and will have a series of unintended consequences on the health of the internet as a whole.** For the sake of the internet's future and Indian users, we urge you to abandon these proposed rules and begin afresh with public consultations on the appropriate way to counter harmful speech online.

Continued open and wide ranging consultation on this complex issue will be necessary if India is to have a future-proof framework for tackling illegal

content in India. **Over the coming weeks and months, we will remain focused on shaping more sustainable solutions to these concerns, and to build out a vision for what a better framework for the "duty of diligence" could look like.** We look forward to providing these inputs and hope that they will be helpful as you continue your important work. For any questions on the present filing, please do not hesitate to contact Mozilla's Policy Advisor Amba Kak at amba@mozilla.com.

Summary of concerns and recommendations

Our concerns with the current draft may be grouped into three broad categories:

- I. Dilution of intermediary liability protections and content filtering obligations
- II. Enhanced government surveillance
- III. Operational requirements

I. Dilution of intermediary liability protections and content filtering obligations

Proactive takedown obligation creates a zero-tolerance approach to harmful content which will inevitably lead to over-censorship and chill free expression.

- This new regime significantly rolls back the intermediary liability protections enshrined in Section 79 of the Information Technology Act, and affirmed by the *Shreya Singhal* judgment of the Indian Supreme Court. The Court had put forth both practical and principled objections to requiring private companies to decide the legality of content on internet-scale. The verdict clarified that platforms would only be expected to remove content when they are directed to do so by a court order. The draft rules turn this logic on its head, and introduce a mandate for companies to proactively take down "unlawful content" using automated means.
- The rules provide no definition of "unlawful" beyond relating it to broad categories like "public order", and "decency and morality". Faced with the threat of direct liability for content, these rules not only encourage but essentially compel companies to bypass due process and make rapid, non-transparent, and unaccountable decisions

about what content gets removed. Eventually, it is users who will be deterred from expressing themselves online.

- On any online platform where users can communicate without prior restraint, there will be a risk that some users abuse that privilege. It is this freedom to communicate without ex ante restraints has been integral to the creativity, collaboration, access to knowledge and innovation that has made the internet successful. Moreover, the goal of completely purging illegal content online is also at odds with the technical architecture of platforms. When operating at enormous scale, it is technically infeasible to expect that risk to be entirely nullified.

Automated and machine-learning solutions should not be encouraged as a silver bullet to fight against illegal speech on the internet.

- The draft rules include a mandate to deploy automated tools to filter content. As we have [argued in Europe](#), automated content filters are a crude control instrument, and are of limited use when assessing the legality of content where *context* is essential.
- In opting to encourage automated tools, the government is putting primacy on the speed and quantity, rather than the quality, of content removals. These are blunt and inappropriate metrics of success when critical fundamental rights are at stake. Filtering tools are only effective with respect to a small subset of illegal content like child pornography where the standard is well defined and universally recognized, and the corresponding harm to free expression is minimal.
- When deployed in the context of the broad and subjective grounds provided in these draft rules, the additional context is critical (for e.g. a culturally specific reference; or if the content was excerpted for the purpose of commentary; or if intended for a specific and limited audience). False positives, or inaccurate labelling of content as illegal by algorithms could mean the suppression of legal content. This directly harms the freedom of speech guaranteed to Indian citizens, is likely to cause a chilling effect on users and eventually, diminishes the vibrancy of the public sphere.

One-size-fits-all obligations for (a) *all types of intermediaries* and (b) *all types of illegal content* are arbitrary and disproportionate.

- (a) *All types of intermediaries*
 - The term "intermediaries" is defined to go far beyond just social media companies. From internet service providers, to browsers, to operating systems, it is hard to imagine any internet company that wouldn't fall within its scope. While these rules have been justified as a way to tackle "instances of misuse of social media", the broad definition goes far beyond the specific companies they refer to. As written, these rules apply indiscriminately to all intermediaries regardless of the role we play in the ecosystem. While the intention might be for selective enforcement, the legal risk applies to all.
 - For small, medium-sized, and start-up online services, these elaborate content control obligations will be disproportionately burdensome to implement. Liability protections have allowed entrepreneurs to host platforms without fear that their innovations would be crushed by a failure to police every action of their users. Imposing the obligations proposed in these new rules would place a tremendous and in many cases fatal burden on many online intermediaries, especially new companies. A startup's first move should not be to build filtering infrastructure and hire an army of lawyers.
- (b) *All types of illegal content*
 - Illegal content is of various kinds, ranging from child pornography to hate speech to copyright to defamation. The draft rules, however, ignore crucial differences and put a uniform requirement of automated proactive removal of all types of "unlawful" content.
 - Each kind of illegal content has widely differing impact on fundamental rights and should not receive the same legal and technical treatment. For example, while sexual abuse content inevitably has a grave impact on victims and might require urgent takedown, a potential violation of copyright instead

calls for a balanced investigation of the claims and counter-claims, and necessitates a less hurried approach. On the other hand, with alleged hate speech or misinformation, there may be much more serious implications on freedom of speech depending on the political and social impact of the content in question. A single legal standard is a blunt approach to address these important differences.

II. Enhanced government surveillance

A proactive filtering mandate would require all online intermediaries to embed monitoring infrastructure and carry out continuous surveillance of user activity.

- The mandate to proactively filter unlawful content, in effect, requires companies to embed monitoring infrastructure in order to continuously surveil the activities of users. Note that the definition of intermediaries would include entities ranging from internet service providers to browsers and operating systems, all of which are uniquely placed to gather a range of sensitive personal data from users.
- Rather than ensuring privacy and data protection safeguards, the draft rules encourage continuous surveillance. This kind of bulk and unrestricted monitoring flies in the face of the Supreme Courts diktat in *Puttaswamy v Union of India*, which puts in place a requirement that any limitations on the fundamental right to privacy must be narrowly tailored and proportionate.

Requiring encrypted services to store additional sensitive information for the sole purpose of government surveillance weakens overall security and contradicts the principles of data minimisation, endorsed in MEITY's draft data protection bill.

- Under the draft rules, law enforcement agencies can demand that companies trace the originator of any information. Many popular services today deploy end-to-end encryption and do not store source information to enhance the security of their systems and the privacy they guarantee users. This would essentially be a mandate to collect

and store additional metadata about senders and receivers of content with the sole purpose being potential government surveillance requests.

- For users, the guarantees of both end-to-end encryption with minimal collection of metadata is an assurance of privacy and security in the products. Compelling companies to modify their infrastructure based on government requests undermines this trust and denies them the ability to provide secure products and services to their customers.
- This mandate also contradicts the principles of data minimization and privacy by design, endorsed in MEITY's draft data protection bill, which require that entities only store the personal data that they need to deliver the service.

III. Operational requirements

Operational obligations on global businesses (especially SMEs) are onerous and likely to spur market exit and deter market entry.

- The proposed rules, amongst other requirements, put a blunt requirement on any service with more than 5 million users in India to incorporate in the country and set up a permanent office. This is a significant operational obligation being imposed on hundreds of services, with no justification for this standard, nor any time period for compliance.
- If the justification is better compliance with government orders, then we submit that mandatory incorporation in India is a disproportionate means to achieve this end. For companies looking to have global presence, India is a large market that cannot be ignored. The stakes are already large enough, and combined with an effective regulator, these fears of non-enforcement are unfounded. Moreover, the choice of where to incorporate has multiple business consequences. Especially for small and medium sized entities, forcibly requiring incorporation and setting up an office in India could mean additional financial burden and operational inconvenience that may cause retreat from the Indian market altogether.
- This raises fears of several smaller international companies closing themselves off to Indian users, while also deterring potential market

expansion of new players into India. Less diversity of services means less choices for users, less competition between services and eventually harms the vibrancy of the Indian digital ecosystem.

- Any move to require companies to incorporate in India, especially with such a minimal market presence, would not only set a dangerous example for other countries, but also other countries would likely reciprocate in kind, requiring Indian companies to incorporate in their jurisdictional borders, which would represent a heavy burden on Indian industry and limit the efficacy of the Digital India and Made in India initiatives.
- Finally, developers of free to download software cannot easily control their distribution. This is especially true for open source software, which anyone can copy and compile. Software developers could thus find themselves falling under the requirements (and sanctions) of these rules absent any volition or action on their part.

Conclusion

As the creator of an open source browser, we are an online intermediary supported by a large number of Indian users and volunteers. If implemented in their current form, these rules would require us to embed an automated infrastructure for surveillance and censorship into our networks. This not only would contravene our core commitments to privacy and freedom of speech online, but also give us the impossible task of having to decide the legality of content at internet-scale.

We support the consideration of measures to hold social media platforms to higher standards of responsibility, and acknowledge that building rights-protective frameworks for tackling illegal content on the internet is a challenging task. On our part, we remain focused on building out a vision for what a better framework for the “duty of diligence” could look like. The current draft of the rules put forward by the Ministry, however, are not fit for purpose. For the sake of the internet's future and Indian users, we urge you to abandon these proposed rules and begin afresh with public consultations on the appropriate way to counter harmful speech online.

MIT/79/072

Mr. Pankaj Kumar
Additional Secretary
Ministry of Electronics & Information Technology (MeitY)
Government of India

31st January, 2019

Subject: Recommendation on Intermediary Guidelines (Amendment) Rules, 2018

Ref.: Public Consultation on Draft Intermediary Guidelines 2018 published on MeitY website

Sir,

With reference to the draft Intermediary Guidelines (Amendment) Rules, 2018 published for public consultation we'd like to submit that some of the proposed provisions may need to be reassessed given the nature of intermediaries being of various types and therefore and a one size -fits all approach may not necessarily be appropriate in bundling all types of intermediaries in the same category.

Under the current information technology regulations, an "intermediary" would be a platform that facilitates movement of content/ information or provision of a service. It has been observed that the definition of an intermediary is quite broad and includes most technology platforms available in India.

The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 ("Amendment") aim to amend the current regulations to place certain *additional compliances and liabilities on intermediaries*. We have elaborated on the changes and the significance of them on high growth internet companies and in lieu of the same recommendations that we propose to make:

No.	Current Position of Law	Proposed Amendment	Recommendations
1.	<p>Proposed Rule 3 (4): Requirement to inform users regarding failure to comply with intermediary terms</p> <p>The intermediary is required to inform its users that failure to comply with the rules would result in the immediate termination of the services to the user and the offending content will be removed.</p> <p>Currently, we add these terms to our customer/driver/rider T&Cs.</p>	<p>The intermediary has to now inform users <u>at least once a month</u>.</p>	<p>Monthly notifications would affect user experience significantly and could also have cost impact. We recommend making a representation that this should be a purely contract-based obligation between the intermediaries and users. An FAQ or similar option for transparency purposes, however, the frequent notification requirement should be removed.</p> <p>The users agree to the aforesaid terms of the User Agreement as well as the Privacy Policy at the time of signing up and also at the time of making a booking,</p>

No.	Current Position of Law	Proposed Amendment	Recommendations
			including but not limited to the aforesaid requirement. Therefore, the proposal of an intermediary informing its customers once every month of non-compliance with rules and regulations etc. will be of little consequence. We recommend to one fits all formula can't be applied in this case, as it will be onerous especially for the intermediaries with a large customer base to comply with the proposed amendments. The once a month requirement could also result in the user being spammed with such emails from different intermediaries, which will be sent repeatedly. The suggestion is that if at all it is required to comply with the same; it should be done once a year, only for inactive users (who have not transacted for over a year), for the intermediaries with a customer base that exceeds threshold of over 10 lakh users.
2.	<p>Proposed Rule 3 (5): Take-down Compliance & Cooperation with the Government</p> <p>Under the current position of law, an intermediary must, within 36 hours of a complaint, take down the offending content/ information and preserve the same for 90 days. This provision was read down in a 2015 Supreme Court decision – only a court order or a government authority can issue a takedown notice for an intermediary to act on.</p>	<p>The Amendment incorporates the requirement of a court or government order for taking down content/ information. The government order can be based on a set of broad purposes, including “security of the state” and “public order”.</p> <p>The offending content/information must be removed within 24 hours. The intermediary must maintain a record of the unlawful activity in question for 180 days. Other significant changes to this rule are as follows:</p>	<p>There should be an exception w.r.t the time frame of reverting on case to case basis depending upon the age of the data asked for. For data that is up to 180 days old, depending on the size and complexity of data demanded, it may be prudent to keep the time frame of 72 hours to one week from date of receipt of the notice, However, for data that is more than 180 days old, the time frame should be at least 15 days, extendable by another 15</p>

No.	Current Position of Law	Proposed Amendment	Recommendations
	<p>If served with an order, the intermediary must provide information/ assistance to the government or its agencies that are authorized investigate.</p> <p>The purpose of seeking the information must be provided and the order must be in writing.</p>	<ul style="list-style-type: none"> - the intermediary should respond within 72 hours; - purpose for seeking information has been broadened to include anything incidental to or connected with the purposes under the existing law, including “security of the state”; - intermediary should be able to trace the originator of the information/ content, if requested by the government. 	<p>days in certain circumstances be allowed.</p> <p>The ability to trace the “originator” of information must aim to place responsibility on social media, messaging and content hosting platforms.</p> <p>We recommend that the regulations clarify the applicability of this only for intermediaries who create and host their own content, and not apply to intermediaries that host third-party created/owned content. Furthermore, while the intermediary can provide information relating to the originator of the information/ content, it should not be allowed to access the intermediary’s systems.</p>
3.	<p>Proposed Rule 3 (7): Registration and Permanent Establishment of Intermediaries and Appointment of Nodal Officer:</p> <p>No provision currently exists for this.</p>	<p>Under the Amendment, an intermediary that (i) has more than 50 lakh users, or (ii) is notified as an intermediary by the government, must:</p> <ul style="list-style-type: none"> - <u>be a registered company under the companies’ laws;</u> - have a permanent registered and physical address in India; and - have a nodal officer and alternative senior for coordination with law enforcement 	<p>Protection of user data from a personal and national security standpoint is of utmost importance. Accordingly, while these changes are welcome and will have a positive impact, it may be more beneficial to make the proposed changes more stringent and ensure that any sizeable or relevant intermediary entity (Indian and foreign) providing goods/services through a digital platform in India is made subject to this provision and is required to have a permanent establishment in India.</p> <p>To re-iterate, from a security standpoint it is also very important that the users of the goods/services being</p>

No.	Current Position of Law	Proposed Amendment	Recommendations
			<p>offered by the intermediary entity (Indian and foreign) can easily identify the entity to initiate action against in case of a breach and/or non-compliance. This requirement would help address the current enforcement issues and ensure that all intermediaries do not evade other regulations that would be applicable; for instance, taxes paid on goods and services, foreign direct investment, companies laws' compliances, labour rules, consumer regulations, and personal data protection laws.</p> <p>It is recommended that the below- mentioned clarifications/amendments to the rules should be considered:</p> <ul style="list-style-type: none"> - that the intermediary entity registered in India should provide the services directly to its users, to ensure that the entity in India can be approached for any breaches and non-compliances; - that the user base threshold for an intermediary that falls under this provision be reduced to 10 lakhs; and - the term "users" should include any and all persons from whom data is collected and/or are registered on the platform (either as a service provider or a service recipient).

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2016
 (Published by MeitY)

No.	Current Position of Law	Proposed Amendment	Recommendations
4.	<p>Proposed Rule 3 (9): Monitoring of content/information: No provision currently exists for this.</p>	<p>Intermediaries are required deploy “technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying or removing or disabling access to unlawful information or content.”</p>	<p>We recommend some clarifying language in the Amendment:</p> <ul style="list-style-type: none"> - this must apply only to intermediaries hosting content from users (i.e. not licensing directly from content creators); - an exemption from liability for any non- content based platforms that are pure aggregators for services; and - that certain types of content can be filtered under this provision, such as explicit, hateful or harmful content that can have social or political repercussions.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
 (Published by MeitY)

MIT/79/073



AWS Recommendations on the Proposed Amendments of the Information Technology [Intermediary Guidelines (Amendment) Rules], 2018

Context: On December 24, 2018, the Ministry of Electronics and Information Technology (“MeitY”) released a set of proposed amendments to the rules governing intermediary liability under Section 79 of the Information Technology Act, 2000 (“IT Act”). Simultaneously, MeitY invited public comments on the proposed amendments.

We submit our comments to the proposed amendments of the Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 (“Draft Rules”) in the form of this note.

Applicability of the proposed amendments under the Draft Rules should be restricted to social media companies

We understand that the Government’s decision to introduce stricter intermediary obligations under the Draft Rules is triggered by the increasing instances of misinformation and fake news over social media platforms.¹ This is evident from the opening paragraphs of MeitY’s call for public comments on the Draft Rules, which highlight the Government’s resolve to “*make the social media platforms accountable under the law.*”² Thus, it is clear that the primary purpose of the Draft Rules is to regulate and monitor illegal content on social media platforms *exclusively*. However, the language of the Draft Rules is not aligned with this purpose, since the Draft Rules target *all* classes of intermediaries, including intermediaries that do not function as social media platforms. This problem can only be solved by regulating the *specific class* of intermediaries involved in the transmission of messages through social media platforms. The proliferation of misinformation and fake news occurs over social media platforms, messaging services and other similar platforms where users can disseminate such information or content, and it is this class of intermediaries (“Content Sharing Platforms”) that must be regulated under the proposed amendments under the Draft Rules.

Currently the Draft Rules apply to *all* classes of intermediaries, since they import the broad definition of intermediaries from Section 2(1)(w) of the IT Act³, which covers a range of service providers and platforms that operate in different ways, such as telecom service providers, web-hosting service providers, search engines, online payment sites, etc. As a result of this problem-solution mismatch,

¹ Minister Ravi Shankar Prasad’s remarks, Calling attention on misuse of social media, Rajya Sabha TV, Rajya Sabha Session – 246, July 26, 2018, available at <https://www.youtube.com/watch?v=aU1m2O7We6E> (Last accessed on December 24, 2018).

² MeitY, Comments / suggestions invited on Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018, available at <http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9Cinformation-technology-intermediary-guidelines> (Last accessed on January 8, 2019).

³ Section 2(1)(w) of the IT Act provides that an intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

intermediaries that have absolutely no connection with content sharing, fake news and the spread of misinformation (“Other Intermediaries”) will also be unintentionally regulated. They will also have to bear the inapplicable provisions and the heavy cost of complying with the proposed amendments under the Draft Rules along with Content Sharing Platforms.

Introducing the proposed amendments in their current form will also weaken the intermediary safe harbour for Other Intermediaries, since their safe harbour protection under Section 79 of the IT Act will be contingent on their compliance with the strict requirements of the Draft Rules. This will unnecessarily jeopardise growth and innovation by the Other Intermediaries, such as cloud service providers and telecom service providers in India, even though such intermediaries are not the intended targets of the proposed amendments. It will also affect the safe harbours which are crucial for the successful operation of intermediaries, as observed by the Indian Supreme Court in the *Shreya Singhal* judgment.⁴

In this regard, we make the following submissions:

- (i) *The proposed amendments should be integrated under a separate set of rules that apply only to Content Sharing Platforms:*

Given the negative consequences associated with the unnecessary targeting of all classes of intermediaries under the proposed amendments to the Draft Rules, the proposed amendments should be integrated under a separate legislation that applies *only* to Content Sharing Platforms. We note that in other jurisdictions, laws have been introduced to specifically deal with the dissemination of harmful content on Content Sharing Platforms. Germany has introduced an Act to Improve Enforcement of the Law in Social Networks (“Network Enforcement Act”), which places reporting and removal obligations on social networks. Social networks are defined under the Network Enforcement Act as “*telemmedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public*”, including “*platforms which are designed to enable individual communication or the dissemination of specific content*”. It specifically excludes other platforms, including “*platforms offering journalistic or editorial content, the responsibility for which lies with the service provider itself*”⁵. If the intention is to regulate social media platforms, a similar legislation can be introduced in India to fulfil the purposes identified by the Government. This will avoid unnecessary targeting of Other Intermediaries and will also safeguard against dilution of the safe harbour protection under the IT Act. Most importantly, it will ensure that the focus remains on the root cause of the problem at hand, i.e., fake news and the misuse of Content Sharing Platforms.

- (ii) *Alternatively, the Draft Rules must specify that certain specific amendments apply only to Content Sharing Platforms:*

⁴ *Shreya Singhal v Union of India* (2015) 5 SCC 1.

⁵ Section 1, Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), available at: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (Last accessed on January 25, 2018).

In the event that it is not possible to integrate the proposed amendments under a separate legislation, the Draft Rules must be modified to identify a separate class of intermediaries, namely Content Sharing Platforms, which are subject to the additional compliance requirements with respect certain specific obligations, which should only apply to Content Sharing Platforms. We have listed these specific obligations in detail below.

This is because, and as explained above, the primary purpose of the proposed amendments is to “make social media platforms accountable under the law”, and it would not be necessary to apply all of the amendments to intermediaries having a lower degree of control over the user’s content, and otherwise not acting directly as platforms which can be used to share harmful and illegal content with the public.⁶

Cloud service providers are a separate class of intermediaries and should not be subject to such compliance requirements

- Certain provisions of the proposed amendments cannot, in any event, be made to apply to cloud service providers (“CSPs”) ⁷ as CSPs cannot implement the content monitoring and control requirements under the Draft Rules⁸. CSP infrastructure may be utilized by individual customers for their personal use and by body corporates and businesses for commercial purposes. Unlike Content Sharing Platforms, which can exercise significant control over the data that is shared on their platforms⁹, CSPs do not have access or visibility into their customers’ data or nature of data that is stored or processed on their infrastructure^{10,11}. In fact, when using cloud services, customers have complete ownership and control over their content hosted on the cloud. CSPs are primarily responsible for maintaining the security of the infrastructure, while the customers are responsible for security of their own content stored / processed in the cloud. Customers can

⁶ MeitY, Comments / suggestions invited on Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018, available at <http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9Cinformation-technology-intermediary-guidelines> (Last accessed on January 8, 2019).

⁷ Cloud Infrastructure Services Providers in Europe, CISPE suggested amendments regarding the scope of the Proposed Regulation on terrorist content online, available at https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/CISPE_Position_Illegal_Terrorist_Content_Regulation_20181126.pdf (Last accessed on January 8, 2019).

⁸ Cloud Infrastructure Services Providers in Europe, CISPE suggested amendments regarding the scope of the Proposed Regulation on terrorist content online, available at https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/CISPE_Position_Illegal_Terrorist_Content_Regulation_20181126.pdf (Last accessed on January 8, 2019).

⁹ Cloud Infrastructure Services Providers in Europe, CISPE suggested amendments regarding the scope of the Proposed Regulation on terrorist content online, available at https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/CISPE_Position_Illegal_Terrorist_Content_Regulation_20181126.pdf (Last accessed on January 8, 2019).

¹⁰ UNESCO, Fostering freedom online: the role of Internet intermediaries, available at <https://unesdoc.unesco.org/ark:/48223/pf0000231162> (Last accessed on January 8, 2019). See also, Cloud Infrastructure Services Providers in Europe, CISPE suggested amendments regarding the scope of the Proposed Regulation on terrorist content online, available at https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/CISPE_Position_Illegal_Terrorist_Content_Regulation_20181126.pdf (Last accessed on January 8, 2019).

¹¹ Amazon, Comments on the draft Personal Data Protection Bill, Page 13.

use controls like encryption to maintain confidential and integrity of their content. In addition, CSPs have no way of identifying and controlling particular kinds of data and are incapable of differentiating one “piece of data” from another¹².

- As customers have complete ownership and control over the content hosted on the infrastructure provided by the CSP, placing responsibility on the CSP for such content can lead to the responsibility of the content owner being diluted, including in contravention of data protection regimes around the world—most notably the General Data Protection Regulation promulgated by the EU, but with effect globally—which do not permit CSPs to act like owners of their customer’s data. In fact, if CSPs were required to remove or disable access to specific content on a particular website that is supported by their infrastructure, they would be forced to take down the entire website, since that is the only manner in which CSPs can control content.¹³ It is therefore unreasonable to expect CSPs to implement the content monitoring and control monitoring requirements under the Draft Rules. Such requirements will also pose serious threats to the fundamental rights of free speech and expression, since the takedown of certain kinds of unlawful content by CSPs may result in the inadvertent removal or blocking of legal content as well, potentially crippling the other (lawful) operations of the customer.¹⁴ As private parties, CSPs should not be expected to undermine their customers’ lawful use of their services.
- Considering how data and content may be hosted and transmitted over a CSP’s network, it may not be possible to provide the information or assistance requisitioned by Government agencies, including tracing out of originator information as per Rule 3(5) of the Draft Rules or deploying automated tools or mechanisms to proactively remove unlawful content as per Rule 3(9) of the Draft Rules. The CSP’s role is only to provide hosting capability by way of cloud infrastructure to the customers, allowing them the freedom to deploy the CSP’s services in the manner required for their business functions. However, we note that the requirements in the Draft Rules with respect to (a) Rule 3(2) on publication of certain language in their privacy policy and (b) Rule 3(8) on disabling content access and maintaining evidence on the basis of a court order are intended to apply more broadly to all intermediaries and CSPs may be subject to the same standards as Content Sharing Platforms in this case.

In this regard we would like to submit the following suggestions/ changes to the Draft Rules:

- *Untenability of Rule 3(5):*

The Supreme Court of India, in *People's Union of Civil Liberties v. Union of India* (“PUCL Judgment”), held that certain procedural safeguards must be followed to protect the constitutional right to privacy while carrying out interception. These procedural safeguards were

¹² Digital Europe, Position Paper on the proposed Regulation on ‘Preventing the Dissemination of Terrorist Content Online’, available at http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=2781&language=en-US&PortalId=0&TabId=353 (Last accessed on January 8, 2019).

¹³ Cloud Infrastructure Services Providers in Europe, CISPE suggested amendments regarding the scope of the Proposed Regulation on terrorist content online, available at https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/CISPE_Position_Illegal_Terrorist_Content_Regulation_20181126.pdf (Last accessed on January 8, 2019).

¹⁴ Centre for Internet and Society, Intermediary Liability and Freedom of Expression, available at <https://cis-india.org/internet-governance/blog/intermediary/view> (Last accessed on January 8, 2019)

subsequently embodied in the IT Act in Section 69 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 formed thereunder, with regard to the direction to carry out interception, monitoring and decryption. Given that the order specified in this sub-rule will amount to an order for interception, it must also comply with the requirements laid down in the PUCL Judgment. Further, the ambit of the term 'assistance' is broad. It cannot be any assistance as intermediaries are not in the business of law enforcement and it should be restricted to those specific cases authorized under the IT Act. Therefore, the scope of the information or assistance that is requested from intermediaries under this provision is broad and must be specified under the lawful order under Sections 67-C, 69, 69-A and 69-B of the IT Act.

As noted above, it may not be possible to provide the information or assistance requisitioned by Government agencies due to how content is hosted by a CSP, including tracing out of originator information. Therefore, we propose the following changes to Rule 3(5):

"When required by lawful order under Sections 69, 69-A, 69-B or 67-C of the Act, issued by a court of law or Appropriate Government in relation to matters concerning (i) security of the State; (ii) cyber security; (iii) investigation or detection or prosecution or prevention of offence(s), the intermediary shall, (a) without undue delay, following receipt of such lawful order, provide such information necessary for the purposes mentioned above if such information is stored or hosted by it in its computer systems and the intermediary has access and control over such information and (b) if required by such lawful order, provide such lawful assistance in relation to information, as required by laws within a reasonable timeframe, if such information is stored or hosted by it in its computer systems and the intermediary has access and control over such information. ~~as asked for by any to Government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto.~~

*Any such lawful order ~~request~~ shall be made in writing **or through electronic means** stating clearly the (i) nature of information sought by the lawful order and the (ii) purpose of seeking such information or any such assistance. ~~The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.~~"*

We suggest that the obligation in relation to tracing out the originator of the information must be removed from the Draft Rules or may be made specifically applicable only to Content Sharing Platforms.

- *Untenability of Rule 3(9):*

CSPs, being private parties, cannot be asked to pass judgment on the legality of any content. In the *Shreya Singhal* judgement¹⁵, S. 79(3)(b) was read down in such a way that the intermediary can only act once it receives 'actual knowledge' in the form of a court order or a notification by the Appropriate Government or its agency that strictly conforms to the subject matters laid down in Article 19(2). Proactive removal or blocking of access by the intermediary will therefore also be *ultra vires* the IT Act, which is the parent legislation for these Draft Rules. The Hon'ble Supreme

¹⁵ *Shreya Singhal v Union of India* (2015) 5 SCC 1.

Court has also acknowledged how difficult it would be for intermediaries to judge the legitimacy of takedown requests, if they are to be made directly to the intermediary. Requiring CSPs to proactively make such judgments and remove or block public access to websites will place them in an even more difficult position. This position was reiterated in *MySpace Inc. v. Super Cassettes Industries Ltd.*¹⁶, where the Delhi High Court reached a similar conclusion with respect to intellectual property. Here, the Court stated that an intermediary being responsible for identifying infringing content, could have a chilling effect on free speech. The *MySpace* judgment also supports the idea that there should be no unwarranted private censorship of free speech. Based on our experience, it would be exceedingly difficult and likely commercially impossible to develop accurate and automated tools or mechanisms and controls to identify and remove/disable public access to unlawful information or content hosted by a CSP. Further, as a threshold matter, at present, it is not even possible to automate the determination of the legality of information or content. Therefore, this requirement is untenable for CSPs. We also submit that "appropriate mechanisms" and "appropriate controls" are vague terms, and no indication has been given regarding how to determine what such appropriate mechanisms and controls are. This makes it very difficult for intermediaries to put any such measures in place. This is a vague standard which will result in uncertainties which drastically increase the liability on the intermediaries and reduce the commercial value of their services, thereby making the business model of intermediaries unviable due to both financial liabilities and liabilities on key officers and directors under various laws.

Thus, CSPs face technical, commercial, and legal barriers to enable mechanisms to take down specific content and cannot be considered in the same manner as Content Sharing Platforms for these purposes. As CSPs do not have access and control over such information, they will be unable to comply with these requirements, which can affect a very large user base of Indian customers (including businesses) that makes use of the services of such CSPs.

Therefore, we suggest deleting Rule 3(9). Alternatively, this provision must be made applicable only to Content Sharing Platforms.

- *Proposal with respect to Rule 3(8):*

Considering how information and content may be hosted, transmitted, shared etc. over an intermediary network, and the steps that will need to be taken by the intermediary to remove or disable public access to it, it may not be possible to complete the removal / blocking process within 24 hours. Originally, the time provided is 36 hours, which is more conducive to the effective implementation of this provision.

There may also be cases where the actionable content is not completely within the intermediary's control. The original provision accounted for such a circumstance and allowed the intermediary to work with the user or owner of such information to disable it. Additionally, intermediaries should be automatically conscripted to preserve data for protracted periods, but rather as required under the circumstances. Therefore, we recommend re-instating the same as follows:

¹⁶ *MySpace Inc. v. Super Cassettes Industries. Ltd.*, 2016 SCC Online Del 6382

"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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, within thirty six hours and where applicable, work with user or owner of such information to disable such information as far as possible immediately, but in no case later than ~~twenty-four hours~~ in accordance with sub-rule (6) of Rule 3. Further the intermediary shall, in accordance with the requirements of such order, preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised."

- *Inapplicability of Rule 3(7) of the Draft Rules to CSPs:*

We note that the factors discussed here indicate that this sub-rule is intended to apply to Content Sharing Platforms with large user bases. Therefore, this provision should not be made applicable to Other Intermediaries. We also note that the requirements provided under Rule 3(7) do not seem to have accounted for the models by which global companies operate, where customers have the option to sign up with Indian entities or offshore entities exercising their contracting choices. Such contracting choices are often guided by customer preference in relation to centralized billing, management, commercial needs, etc. It is also possible that the offshore entities may be carrying out different functions vis-a-vis other entities of the same group company for the same user located in India. In such cases, where both the local and offshore entity would qualify as intermediaries separately, amended Rule 3(7) would unnecessarily require the group to separately incorporate an Indian entity for the offshore entity as well. It is impractical to suggest that offshore entities must also set up a company in India to enjoy the safe harbor under section 79. It is also important to acknowledge that the definition of "user" as provided in the Intermediary Guidelines is broad and would apply to anyone interacting with the intermediary's computer resource. This will prove to be extremely problematic for most intermediaries. Specifically, for CSPs this is onerous since the data hosted by customers on the CSP's infrastructure may be accessed by a vast number of people on whom the CSP has no control over or obligation towards. CSP also do not have knowledge of customer's clients who access such data. In such a case, many CSPs who functionally only serve their own customers will be brought under the ambit of this sub-rule and be forced to undertake these additional compliances, which places unnecessary financial and regulatory boundaries on CSPs who wish to do business in India.

Further, we note that the current clause gives the Government powers to notify different classes of intermediaries under the ambit of Rule 3(7). However, it does not mention the criteria that will be mentioned for its determination. The criteria for this also must be adequately captured in Rule 3(7).

Therefore, we propose that the Rule 3(7) be made applicable only to Content Sharing Platforms.

- *Inapplicability of Rule 3(4) to CSPs:*

The present definition of user, as noted previously, will include all persons who interact with a CSP's computer resources by way of accessing content hosted by the CSP's customer. CSPs do not have the capability to track, identify, and notify these users on a monthly basis (or any other singular or recurring basis) regarding their obligations under the Intermediary Guidelines. Therefore, this obligation must only be with respect to the registered customers of a CSP. Further, an intermediary's right to immediately terminate the access or usage rights of their customers to the computer resource of the intermediary and remove noncompliant information in these circumstances will be a part of the user agreement / privacy policy that the customer consents to, which is a valid and enforceable contract. Given that there is a valid contract under the Indian contract law, there is no need for a specific requirement to send monthly reminders to the customers.

It is also our submission that monthly reminders do not serve any practical purpose, particularly in case of CSPs, which do not provide a platform for users with the purpose of communication as in the case of Content Sharing Platforms. Sending monthly reminders is a cumbersome and impractical measure for intermediaries to adopt over and above the consent taken from them under these contracts. Moreover, users are entirely likely to simply ignore or automatically discard (e.g., through email filters) such reminders, as nuisance or SPAM. We therefore recommend deletion of the monthly reminder.

Therefore, it is submitted that among Draft Rules, the applicability with respect to CSPs must be as follows:

Rule	Proposed Clause under the Draft Rules	Applicability
3(2)(j)	(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;	All intermediaries
3(4) ¹⁷	The intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of	Original text must be retained

¹⁷ Originally, sub-rule 5 of Rule 3.

	the users to the computer resource of Intermediary and remove noncompliant information.	
3(5) ¹⁸	<p>When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or any such assistance as asked for by any to gGovernment aAgency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. who are lawfully authorised for investigative, protective, cyber security activity. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.</p>	Applicable to all intermediaries, except the obligation to enable tracing out of originator on its platform, which may be only apply to Content Sharing Platforms. Rule must be modified as described above.
3(7)	<p>The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:</p> <ul style="list-style-type: none"> (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their 	This must be deleted or be made applicable only to Content Sharing Platforms

¹⁸ Originally, sub-rule 7 of Rule 3.

	orders/requisitions made in accordance with provisions of law or rules.	
3(8) ¹⁹	<p>The intermediary, on whose computer system the information is stored or hosted or published, 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 Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. 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 as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least one hundred and eighty ninety days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.</p>	All intermediaries. Rule must be modified as described above.
3(9)	The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.	This must be deleted or be made applicable only to Content Sharing Platforms

¹⁹ Originally, sub-rule 4 of Rule 3.

MIT/79/074

S. N O.	RULE 3 OF DRAFT RULES (Due diligence to be observed by the intermediary)	SAMVAD COMMENTS	PROPOSED CHANGE
1.	<p>Sub-rule (5):</p> <p><i>“When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”</i></p>	<ul style="list-style-type: none"> Intermediaries are obligated to provide information or assistance on the basis of a lawful order, but what constitutes a “lawful order” is not defined in the Draft Rules. For example, it is unclear whether a departmental enquiry/request would also amount to a “lawful order”. In order to address this, it is recommended that a statutory basis be provided for such order. The scope of the obligation is too broad for government agencies to seek information. We suggest that this should be limited to scenarios when the security of the State or cyber security is in question and not otherwise. The term “<i>protective or cyber security and matters connected with or incidental thereto</i>” appears to have been inserted in error as an earlier reference to cyber-security has already been made. Furthermore, the term ‘<i>matters connected with or incidental thereto</i>’ is vague and capable of exploitation through interpretation. Detailed/confidential information about persons interacting on the intermediary platform can be obtained without a need to maintain secrecy of such information. So, there should be some checks 	<p><i>“When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s). Any such request can be made in writing or through electronic means from the designated government agency having authority to make such order stating clearly the purpose of seeking such information or any such assistance and the statutory basis for such order.”</i></p>

		<p>and balances to further use of the information so obtained. For example, racial profiling, targeted messages from departments, political propaganda, etc. The Draft Rules should not encourage any abuse of power by State and should protect the privacy of the Indian citizens as per the Constitution of India.</p> <ul style="list-style-type: none"> • <i>“The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”</i> This provision will affect intermediaries who have enabled privacy in their communications such as WhatsApp’s end-to-end encryption, resulting in compromising privacy for all users of the platform. 	
<p>2.</p>	<p>Sub-rule (7):</p> <p><i>“The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall: (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions</i></p>	<ul style="list-style-type: none"> • Clarity on the nature of intermediaries who would be notified for the purpose is unclear. Perhaps, parameters for being so notified can be elucidated. For example, whether the registration is voluntary or mandatory can be elucidated. Similarly, whether this list is meant to identify all intermediaries operating in Indian jurisdiction or only significant ones is unclear, especially since the list is in addition to the intermediaries who already meet the threshold requirement. • The need to be incorporated under the Companies Act or have a local presence by 	<p><i>“The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.”</i></p>

	<p><i>made in accordance with provisions of law or rules.”</i></p>	<p>registering a company in India is antithetical to the concept of “global presence” of most social media startups and established players. This requirement could also pose consequential tax and local compliance burdens on entities who may be offshore and could dis-incentivize such entities from opening up their platform to Indian audience.</p> <ul style="list-style-type: none"> • Alternately, it may be preferable to place permanent office and registration requirements on intermediaries passing a higher threshold. Up to that threshold, the presence of a nodal person should be sufficient. • Also, the criteria of having local presence on the basis of number of subscribers / users is impractical, since popularity of social media sites vary from time to time, and tracking status and compliance may pose a practical challenge. • The Draft Rules must clarify the role of the Nodal Officer and the scope of obligation to be discharged by him. Perhaps, one can also specify qualification requirements in this regard to ensure effective implementation as opposed to having a mere paper compliance in place. 	
<p>3.</p>	<p>Sub-rule (8):</p> <p><i>“The intermediary upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its</i></p>	<ul style="list-style-type: none"> • The Supreme Court in <u>Shreya Singhal v. Union of India</u> (decided on March 24, 2015) has laid down the parameters for deciding an “unlawful act” and has been limited to reasonable restrictions provided 	<p><i>“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 Act shall remove or disable</i></p>

<p><i>agency under section 79(3)(b) of Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorized.”</i></p>	<p>in Article 19(2). This should be reflected through an amendment to the Act and not through Draft Rules.</p> <ul style="list-style-type: none"> • Also, compliance with moral standards cannot be a requirement of law. Morality standards vary for different persons. Acts such as defamation, blasphemy, etc. can be categorized as unlawful acts for this purpose. • The timeline of twenty four hours provided for compliance may not always be possible to achieve. The intermediary should have a means of appealing an order for removal within twenty four hours if it is not technically possible for the intermediary to do so within the 24-hour timeline prescribed. 	<p><i>access to such unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3, provided that, where the intermediary is unable to comply with such removal within twenty-four hours, the intermediary may respond to such order or notification with specific reasons for such inability and seek additional time, which may not be unreasonably withheld by the appropriate Government or its agency. Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorized.”</i></p>
<p>4. Sub-rule (9):</p> <p><i>“The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to</i></p>	<ul style="list-style-type: none"> • Section 79(2)(b)(iii) of the Information Technology Act, 2000 mentions the grounds on the basis of which liability of an intermediary can be limited. Sub-rule (9) directs an intermediary to “proactively” identify any unlawful information and/or content. The 	<p><i>Suggested Removal</i></p>

<p><i>unlawful information or content.”</i></p>	<p>Draft Rules assumes that the intermediary has the ability to access information being published on the platform as well as the option to “select” the kind of information that can be posted on the platform. Such an assumption conflicts with the role of an intermediary and hence needs to be reconsidered.</p> <ul style="list-style-type: none"> • Furthermore, accessing information / messages being shared takes away privacy and hence, is not conducive. For example, certain intermediaries like WhatsApp have a large customer-base because of the security protocols like end-to-end encryption. WhatsApp will have to break the end-to-end encryption code if it is obligated to access the information and segregate the content and origin of the content. This may compromise privacy for all users of the platform. • Lastly, in the absence of any new technology which will automatically identify and remove unlawful content and/or information or disable public access as and when required, intermediary will have to necessarily intervene and monitor what has been shared on its portal. This violates the grounds mentioned in Section 79(2)(b)(iii) of the Information Technology Act, 2000 for limiting an intermediary’s liability and right to privacy under Article 21 of Constitution of India. Hence, the same must be reconsidered. 	
---	--	--

ADDITIONAL RECOMMENDATIONS			
	RECOMMENDED ACTION	REASONING	PROPOSED CHANGE
5.	<p>Rule 3(11) of the Draft Rules / Rule 3(10) of the Information Technology (Intermediaries Guidelines) Rules, 2011:</p> <p><i>“The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:</i></p> <p><i>Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.”</i></p>	<p>This provision is vague and capable of exploitation as a number of online intermediaries may now allow the installation of applications or patches that alter or enhance the functionality of personal computers, phones, servers, networks and any kind of computer resource. A provision of this nature places all intermediaries at risk even if they want to introduce innovative new technologies or products. The provision could be applicable to situations where the intermediary does so without notice or sufficient information to the owner of such computer resource.</p>	<p><i>“The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force without the prior knowledge and informed consent of the owner of said computer resource:</i></p> <p><i>Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.”</i></p>
6.	<p>Process for Contesting Government Order</p>	<p>There should be a quasi-judicial process allowing either the intermediary or the user whose content or privacy is being affected to contest the order of the Government agency.</p>	
7.	<p>Timeline for completion of inquiry</p>	<p>There is no fixed time period set for completing an inquiry and submitting a final report on the complaints raised by end-users.</p>	

BOARD OF DIRECTORS

Thomas J. Donohue
U.S. Chamber of Commerce

Prakash H. Mehta
Akin Gump

Carlos Gutierrez
Albright Stonebridge Group

James Taiclet, Jr.
American Tower Corporation

Samir Behl
Amway

Amb. Mark Lippert
Boeing

Kiran Mazumdar-Shaw
BioCon

Michael Hayden
The Chertoff Group

Pramit Jhaveri
Citibank

Matthew Friedrich
Cognizant

Ralph Voltmer
Covington & Burling LLP

James Muhs
FedEx

Maurice "Hank" Greenberg
Starr Companies

Linden P. Blue
General Atomics

J. Michael McGuire
Grant Thornton LLP

Dinesh Paliwal
Harman

Christopher A. Padilla
IBM

Andreas Fibig
International Flavors & Fragrances

Sanjay Govil
Infinite Computer Solutions

Salil Parekh
Infosys

Rajiv Lall
IDFC Bank

William Thomas
KPMG International

Richard H. Edwards
Lockheed Martin

Dr. Pawan Kumar Goenka
Mahindra

Edward Knight
NASDAQ

Vijay Advani
Nuveen

Stephen J. Hadley
RiceHadleyGates LLC

Tulsi Tanti
Suzlon

Banmali Agrawala
Tata Sons Ltd.

Amos Hochstein
Tellurian

Nando Cesarone
UPS

Sudhanshu Vats
Viacom18 Media

Judith McKenna
Walmart

Siva Sivaram
Western Digital Corporation

Rana Kapoor
Yes Bank

Amb. Nirupama Rao

January 31, 2019

Shri Pankaj Kumar
Additional Secretary
Cyber Law and eSecurity Group
Ministry of Electronics & Information Technology

Re: USIBC Recommendations to Promote the Digital Economy through Balanced Intermediary Liability Regulations

Dear Shri Kumar,

U.S. Chamber of Commerce's U.S.-India Business Council (USIBC) writes to offer our comments to the Ministry of Electronics & Information Technology (MeitY) on its Draft of Intermediary Guidelines of 2018 (Draft Guidelines).

As you may know, USIBC is an integral part of the U.S. Chamber of Commerce, the world's largest business federation representing more than 3 million businesses of all sizes, sectors, and regions, as well as local U.S. state and local chambers, and numerous industry association members. USIBC is the largest of our 25 country- and regional-specific business councils, and we represents nearly 300 companies based in India, the United States and Europe. Our digital economy members are central to India's digital transformation and strongly support the *Digital India* initiative.

Industry shares the goal of responsibly addressing the challenge of illegal and harmful content, and looks forward to ensuring that all actors work hand-in-hand for the security of Indian citizens. We welcome in particular the intention to improve the cooperation between private companies, law enforcement and other competent authorities. The focus of these comments is to raise concerns largely with compliance challenges associated with unrealistic expectations the Draft Guidelines create. Specifically, we would raise the following points:

We would like to call attention to the Indian Supreme Court's ruling in the *Shreya Singhal* case, which declared Section 66A of the IT Act unconstitutional due to ambiguous language such as "grossly offensive," "menacing," "false," and "causing annoyance, inconvenience, danger." The Court indicated further restrictions must fall within the contours outlined in Article 19(2) of the Constitution of India and include principles of natural justice and elements of due process of law. Thus, we encourage MeitY to carefully review the draft language to ensure that it meets the legal test of this ruling to ensure that any new rules do not run counter to Indian jurisprudence, which could result in legal uncertainty, confusion, and instability within the digital ecosystem.

Section 3 (4) – While we agree it is in the intermediary's interest to inform its users that in the case of non-compliance with rules and regulations the intermediary has the right to terminate the user's access and remove noncompliant information, requiring that this be done "at least once a month" is not an advisable practice to put into guidelines. Such a requirement is likely to have little of its intended impact, as users are likely to view the notifications as routine and become desensitized to their purpose. We would recommend the Draft Guidelines suggest users be informed at least once in a 12-month period.

Section 3 (5) – It is important that intermediaries are responsive to lawful orders in a timely manner. However, the insertion of “within 72 hours of communication” may be unreasonable in certain situations. We would recommend the Draft Guidelines direct responsiveness to lawful orders in an expeditious manner and perhaps indicate in response to copyright violations and emergency situations within 72 hours. Further, USIBC recommends the addition of “Stop the Clock” provisions that list criteria such as seeking clarifications, technical infeasibility, etc., under which the time limit would cease to apply to allow for due process in enforcing such requests. In other cases, including copyright violations, where commercial-scale or other harms are likely to accrue within 72 hours, a more timely response is appropriate. In addition, USIBC notes that absolute traceability and attribution is not technically feasible in all instances. Finally, in order to protect privacy and prevent cybersecurity breaches, some products utilize encryption features that preclude or severely limit the ability of intermediaries to track and trace content.

Section 3 (7) – This added provision creates an unnecessary, burdensome localization requirement that is not justified. We strongly recommend it be struck because it will result in some internet services no longer being offered in India and it has discriminatory impact on small and medium-sized enterprises.

Section 3(8) – The need to comply with a court order is clear. However, the new provisions extend to notification by the “appropriate Government or its agency.” This is too broad as drafted, as situations will arise where notification by the Government or its agency may be appropriately questioned on both a legal and due process basis. Requests from the Government to remove content that is a clear violation of the law, such as pirated content, is not debatable; however, in other contexts a Government order to take down objectionable content may invoke legal and procedural challenges. Keeping in mind the India’s Supreme Court *Shreya Singhal case*, we recommend the Draft Guidelines provide greater nuance regarding the extent to which notifications beyond court orders must result in an intermediary removing content or disabling access in 24 hours.

We also question, in general, the feasibility of imposing a hard 24-hour requirement for compliance with notifications. Perhaps the Draft Guidelines should state that removal of content or disabling of access should normally occur within 36 hours, unless there are complicating factors. “Stop the Clock” provisions should apply in these instances as well. Finally, the requirement to keep records and information for 180 days raises policy implications associated with privacy-related limits on the storage of unnecessary data. The Draft Guidelines should retain the current 90-day requirement, unless directed by a court order. This balances the need to retain information while minimizing the burden to maintain data for extended periods of time.

Section 3(9) – USIBC underscores that while automated detection tools can help identify content that violates policies, it is not effective in all instances, and for small or start-up products and services, may not be economically or technically practical. The updated rules, therefore, should incentivize but not mandate the use of automation and provide guidelines for its usage and limitations.

The U.S.-India Business Council appreciates the opportunity to provide our views on the Draft Guidelines and looks forward to our continued engagement with the Ministry.

Sincerely,



Nisha Biswal
President, U.S.-India Business Council
U.S. Chamber of Commerce

Introduction

Internet Intermediaries commonly refers to a wide, diverse and rapidly evolving range of service providers that facilitate interaction on the internet between one another. Some connect user to the internet, enable processing of data and host web services, others gather information, assist searches, facilitate the sale of goods and services, or enable other commercial transactions. Importantly, they may carry out several functions in parallel apart from being intermediary. Internet intermediaries also moderate and rank content, mainly through algorithmic processing, and they may perform other functions that resemble those of publisher. As a result, different regulatory framework can apply, respectively, to their intermediary roles and to their other functions.

Intermediaries are entities that provide services enabling the access of online content to end user. The *Information and Technology Act, 2000* defines the term Internet Intermediaries as,

“with respect to any particular electronic records, any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber café”.

According to the definition it can be understood that any person providing any service with respect to electronic message including receiving, storing, transmitting it would qualify as an intermediary.

CPF's Suggestions

CPF proposed the following suggestions on the proposed amendments to the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018.

1. Rule 3(4) – We believe monthly notification to users by intermediaries may create a decline in the interest of the users, a phenomenon that has been reported by a study conducted by *The Guardian*¹. A better approach would be to send annual or by-annual notifications strictly about the amendments and how it may affect the user.

2. Rule 3(5) – Rather than a time limit of 72 Hours of communication, we propose that the time limit of intimation by virtue of the lawful order should be distributed into categories based on the seriousness of the issue. Such a bifurcation will allow swift action in criminal or emergency cases. Taking an example of cases of terrorism, murder or any other such case in which the delivery of information cannot be delayed by an hour and which may even lead to loss of life, the intermediaries may take advantage of this 72 hour time cap and delay the communication or delivery of information. Hence, we suggests that this 72 hours point should be either removed and such decision should be left on the discretion of the court depending upon the case or there should be bifurcation of time limit depending upon the seriousness of the case.

3. Rule 3(7) –

- (i) The incorporation of Intermediaries may not be done under Companies Act, 1956 or Companies Act, 2013 in every case, there may be companies who are already incorporated outside India. Therefore this rule may harm our economy as these companies will not be able to provide their services in India.
- (ii) Appointing a nodal officer and alternate senior designated functionary on a 24/7 availability in India may not always be logistically feasible for the intermediary.

¹“Click to agree with what? No one reads terms of service, studies confirm”, *The Guardian*, Link-
<https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>



4. Rule 3(9) – On this part there are 3 points that need to be taken into consideration.

- (i) The *deployment of technology based automated tools or appropriate mechanism, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content*, it may be possible by only few intermediaries, who have the capability to meet this requirement. Mostly intermediaries may lack the technical capability for screening the content due to non-availability of technology or higher cost of the same².
- (ii) Looking at the instances where intermediaries have been using the user's data for their own benefit without taking the proper consent, this rule may give them a legal right to perform such activities more openly, thereby affecting the data privacy of users.
- (iii) Additionally, the rule also goes against previous judgements given by Supreme Court of India and different High Courts, In the case of Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors Delhi High Court held that "Merely because intermediary has been obliged under the IT Rules to remove the infringing content on receipt of complaint cannot be read as vesting in the intermediary suo motu powers to detect and refuse hosting of infringing contents". In another case of Shreya Singhal vs Union of India Supreme Court of India held that "intermediaries must not be required to screen content or assess the legality of such content".

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
(Published by MeitY)

²"Problems with filters in the European Commission's Platform Proposal", Daphne Keller, The Centre for Internet and Society, Link- <http://cyberlaw.stanford.edu/blog/2017/10/problems-filters-european-commissions-platforms-proposal> ;





COAI Position on Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018”

At the outset, we thank you and sincerely appreciate the opportunity provided to us to present our inputs on the Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018” (“Draft Amendment”) which seeks to amend the Information Technology (Intermediary Guidelines) Rules, 2011 (“Intermediary Guidelines”) under the Information Technology Act, 2000 (“IT Act”)

We take this opportunity to introduce us as COAI which was constituted in 1995 as a registered society. COAI has emerged as the official voice of the digital communications industry that interacts directly with ministries, policy makers, regulators, financial institutions and technical bodies. Our membership comprises of *inter alia* telecom service providers, internet service providers, search engines, e-commerce companies, and also social media platforms who are classified as “intermediaries” under the Information Technology Act. Our members are key constituents of the digital ecosystem and are committed to working with the government to realise the vision of a Digital India.

It is critical that the exercise of amending the Guidelines which govern the responsibilities of Intermediaries for user-generated content should be in line with international norms. In this regard the regulations need to strike a careful balance between the rights and obligations of users and intermediaries, promoting and upholding Internet freedom while putting in place appropriate safeguards for the privacy and security of users. It is also important to ensure that there is enough protection built to prevent online dissemination of illegal and harmful content. Additionally, it is also important that the proposed guidelines are consistent with the existing laws, rules and regulations including the License conditions of the Telecom Service Providers and not in conflict with any of the same. Any requirement that is added should be reasonable and without added burden which is onerous in nature.

We believe that the Draft Amendment would run contrary to the Supreme Court ruling in Shreya Singhal Vs Union of India where the Supreme Court had significantly read down the statutory provisions and held that ‘knowledge’ under Section 79(3) of the IT Act would only mean knowledge by the intermediary pursuant to an order of a court of law. The Supreme Court of India has recently also upheld the fundamental right to privacy of individuals in the case of KS Puttaswamy v. Union of India, as a critical and essential component of the right to life and liberty under Article 21 of the Constitution of India. While upholding this right, the Supreme Court stated that any limitation on the right to privacy should satisfy the triple test of legality, necessity and proportionality.

The Draft Amendment proposes changes that could be detrimental to citizens, democracy and free speech. The amendments pose several critical impediments to the right to privacy of individuals as they fail to satisfy the three-tier test that has been laid down for this purpose. While all sub-rules under Rule 3 of the Intermediary Guidelines deal with the obligations that an intermediary must fulfil in order to claim safe harbour from prosecution, it is important for the language to be adequately clear and the obligations spelt out clearly. The lack of clarity in relation to the obligations under the Intermediary Guidelines could lead to inadvertent non-compliance resulting in arbitrary prosecution. Further, the lack of clarity shall also result in onerous obligations that are likely to potentially drive several intermediaries out of business in India and preclude the possibility of new intermediaries developing in the future.

In this context, we would like to offer our inputs on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018.

The draft rules use various terms such as 'any government agency', 'lawfully authorized government agency', 'appropriate government agency', 'government agencies who are legally authorized', in various provisions, which is creating confusion and ambiguity and is likely to lead to implementation challenges as well as monitoring challenges. It is suggested that the terminology be uniform, clear and unambiguous. We suggest that the term legally authorized and duly designated Government agencies may be used and, either the authorised agency be named, or it be made clear as to what would be the process and criteria for designating such government agencies.

1. Rule 3(2)

The existing Rule 3(2) of the Intermediary Guidelines prescribes that intermediaries must inform their users not to host, display, upload, modify, publish, transmit, update or share certain type of content – failing which [under Rule 3(4)] such content could be removed and the user's access to respective resources and content could be terminated. The Draft Rules add two additional types of content that cannot be shared: (i) content that threatens public health or safety (promotion of cigarettes or any other tobacco products or consumption of intoxicants including alcohol and Electronic Nicotine Delivery Systems); (ii) content that threatens critical information infrastructure.

COAI Response:

We would like to submit that these two clauses of the Draft Rules have been drafted very broadly and should be removed for the reasons detailed below:

- i. **Ambiguity** - The Draft Amendment does not specify as to what would be 'threatening' to public health or safety and critical information infrastructure, or what would tantamount to 'promoting' intoxicants and thus fail to identify the particular kind of content that is meant to be restricted from publication. For example, would online content depicting a person holding a glass of liquor or smoking would be considered as "threatening" to public health or safety as

prescribed in the Draft Amendment. We submit that the restricted content be described clearly which will allow the intermediaries to communicate to the users in clear and unambiguous terms.

- ii. **Constitutionality** – The terms such as ‘threaten’ and ‘promotion’ suffer from the same kind of vagueness that Hon’ble Supreme Court cautioned against in the case of Shreya Singhal by striking down Section 66A of the IT Act and holding that they were likely to have a chilling effect on freedom of speech by intermediaries. The Hon’ble Supreme Court took note that vague restrictions are not only against the spirit of providing a safe harbour for intermediaries but also challenging to implement and enforce.
- iii. **Conflict with other Regulations:** We submit that depending on the issue and product/services involved, there would also be separate regulatory authorities, for example for food product, Foods Standards and Safety Authority (FSSA) is the sectoral regulator, who has already published independent guidelines regarding the health and safety of products coming under their domain. Another example is the Cable regulation Act, which states that no advertisement is permitted to be aired by the channels, if the same is prohibited by another body like ASCI. It is therefore submitted that, there are enough checks and balances already in place and the proposed regulation to that effect if not only in excess, but also may run in conflict with other sectoral regulations. Alternatively, it should be clearly established and stated in the Regulations of which Regulation will take precedence or all such ambiguities should be considered and removed.

2. Rule 3(4)

The existing provision prescribes that intermediaries shall inform their users that their non-compliance with rules, regulations, user agreement and terms and conditions could lead to the termination of their access or usage rights to the computer resource. The Draft Rules mandate intermediaries to inform their users regarding the above at least once every month.

COAI Response:

This provision places an unreasonable and disproportionate burden on intermediaries without any corresponding public benefit and should therefore be removed. Further, this amendment is not required as this provision is already incorporated in the terms and conditions of use of all websites, and mandating changes to the interface of all intermediaries across several jurisdictions for this purpose will be unduly onerous without serving any corresponding purpose. Further, this could lead to notice fatigue on the part of users and fail to have the intended impact i.e. to increase the awareness of this provision.

3. Rule 3(5)

The existing Rule 3(5) of the Intermediary Guidelines requires intermediaries to provide information or assistance when required by lawful order. The Draft Rules amend this rule significantly by changing the timelines and by mandating that any government agency can seek such data.

The Draft Rules also mandate intermediary to proactively trace the originator of the content as may be required by legally authorized government agencies in order to claim exemption from intermediary liability.

COAI Response:

We would like to submit that these two clauses of the Draft Rules should be removed or modified accordingly, for the reasons detailed below:

- i. **Time limit** - The Draft Rules mandate a time limit of 72 hours within which intermediaries are required to provide the information or assistance which is arbitrary; timing can vary as it depends on the nature, volume, scale, duration, historicity and type of information being sought. This duration is also unduly onerous as it does not allow the intermediaries the time to collate, review the legitimacy of the information request and respond appropriately. While the obligation on the intermediary comes with a strict time limit that has no specific justification, there is no corresponding obligation on the government agency as regards the specificity of the information or assistance being sought.

Stop the Clock Provisions: 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.

- ii. To comply with the draft law intermediaries would need to put in place organisational measures that today may not be generally built-in due to various reasons. COAI suggests that the legality of the removal order should be open to and be determined through judicial review. More time should be provided to respond to the removal order itself. This is essential to give sufficient time to the hosting service provider to undertake the technical review to ascertain that the order is complete, can be carried out correctly, and possibly appeal the decision.
- iii. **Inadequate procedural safeguards** – This provision lacks any procedural safeguards (both in terms of defining the scope of “information and assistance”, as well as specifying which government agencies and specific

officers who can issue these requests, and for what purpose) and hence it is extremely prone to misuse.

Vagueness - The use of the term “or” before “assistance concerning security of state” etc. seems to imply that assistance can be sought by government agencies for any purpose, in addition to the security of state, cyber security, and related reasons. This indicates that there is no purpose limitation on the kind of assistance that may be sought. The term “any agency” also implies no limitations on who may seek such assistance.

- iv. **Provision for information requests already exists** - Information requests to help with criminal investigations are already addressed under existing criminal law and are applicable to intermediaries. There is no need for a separate process which contains fewer safeguards. In this regard, it is also important that the proposed guidelines are consistent with the existing telecom regulations of Department of Telecommunication (DoT), the security obligations under the Licence conditions and more importantly consistent with the existing telecom regulations of Department of Telecommunication (DoT), in this area.
- v. **Mode of communication of data requests** - The Draft Amendment includes requests made by electronic means. This provision should clearly specify the procedures that can be used by legally authorized and duly designated government agencies to communicate such orders for information or assistance in order to have a clear and transparent process. In this context, it is vital to note that the Manila Principles on Intermediary Liability specifically state that requests for restrictions of content must be clear, unambiguous and follow due process.
- vi. **Inconsistency:** The first part of new Rule 5 calls for intermediaries to respond to requests from ‘any government agency’ whereas earlier rules read “government agencies which are lawfully authorised for investigative, protective, cyber security activity.” Thus, this new rule expands the scope of which agencies can seek such information. This should be narrowed down to only the agencies lawfully authorised to do so. The last part of new Rule 5, however, restricts agencies to those which are legally authorised to do so. This creates an inconsistency and differential standards for requests for information.
- vii. **Tracing obligation poses multiple challenges** - The Draft Amendment also imposes an obligation on the intermediaries to enable tracing of originators of information, as required by government agencies.
 - a. **Technical Challenges** – We submit that this requirement would not be applicable to Telecom Companies as the same may not be practically possible to implement as in case of information that flows through a

series of intermediaries, each intermediary would only be able to assist to the extent of the origin of the information at their end. Alternatively, it is suggested that where the applicability is not possible, the carve outs should be provided.

- b. **Undermines security and privacy of communications** - This is deeply problematic from a privacy perspective and would be difficult to operationalise given that the intermediary does not control or monitor content. This obligation also undermines the use of encryption technology, which ensures that content is not accessible to the intermediary or third parties. Thus, placing the obligation of tracing on an intermediary creates a restrictive regime which seeks to dictate the underlying technology governing the intermediary's business, in addition to incentivising the development of technology that undermines globally recognised best practice for preserving the privacy and security of communications, in particular the deployment of robust encryption tools.
- c. **Lacking in procedural safeguards** - There are no procedural safeguards limiting the scope of the tracing request to ensure that the provision is not misused. In this context, it is important to note that the recent Supreme Court judgement on the Aadhaar Act, 2016, has ensured that unfettered access to citizen's data is not permitted even if data is sought for national security purposes. The Supreme Court has delineated a clear and a high standard of needing due process safeguards when it comes to accessing an individual's data even if it is for national security purposes. Thus, on similar grounds, the tracing requirement contemplated in the Draft Rule would not stand judicial scrutiny.
- d. **Technological changes** - From the perspective of the user, this constitutes a violation of their right to freedom of speech and expression, as well as their right to privacy, while from the perspective of the intermediary, this may impinge on their freedom of business and commerce as it may require the introduction of procedures to comply with these requirements that would potentially change several underlying technologies and business practices.

In this context, it is worth noting that several intermediary platforms are already working closely with the government in order to come up with the best ways to combine the interests of law enforcement with the business and technology operations of said intermediaries, we urge the government to follow international best practices in this regard. To proceed with the legally problematic approach outlined in the draft law could have restrictive impacts on such online platforms without giving rise to a corresponding public benefit.

4. Rule 3(7)

This provision of the Draft Rules prescribes that intermediaries with more than fifty lakh users in India or those notified by the Central Government must meet certain conditions, such as local incorporation, maintaining a permanent registered office in India, and appointing persons of contact in India for 24x7 coordination with law enforcement agencies.

COAI Response:

The principle of “Same Service, Same Rules” relating to the Over-The-Top (OTT) services, needs to be applied so as to address the licensing, regulatory and security asymmetries between the two sets of services. COAI is of the firm view that bringing parity between the licensed telecom players and the OTT players offering any services that are permissible to the former, is essential, not only for fair business but also for addressing various national security concerns in terms of access to data/records and ensuring security, safety and privacy of the consumer data.

In this regard COAI supports the measures described under rule 3(7) which would ensure that online intermediaries which compete directly with licensed telecom service providers are subject to an equivalent level of regulation, and do not obtain a competitive advantage through the existence of regulatory safe harbours for online intermediaries.

The proposal that intermediaries over a certain size should meet certain conditions, such as local incorporation, maintaining a permanent registered office and appointing a local contact person are proportionate and necessary to ensure a level-regulatory playing field between competing service providers. As such we would lodge no specific objection to the inclusion of these measures in the draft Rules.

5. Rule 3(8)

Under this rule, the Draft Rules create an obligation on intermediaries to take down content upon a court order or being notified by the appropriate Government or its agency within 24 hours, where the content pertains to the restrictions under Article 19(2) of the Constitution. The Rules also extend the period of time that the information must be stored for, and even authorises government agencies to extend it further.

COAI Response:

Our concerns on this are highlighted below:

- i. **No procedural safeguard** – There are no procedural safeguards built into content takedown notices by appropriate government. This rule contains a process for the removal or disabling of content but does not incorporate any

safeguards while creating this new process as it neither specifies who can pass the orders, nor does it require reasons to be recorded for such orders.

- ii. **Time Limit** – The Draft Amendment provides for an unreasonable time limit of 24 hours to implement orders of removing or disabling access to content. This time limit does not provide any opportunity to intermediary to review the order and ascertain whether it is legitimate or to identify the specific content which needs to be removed or disabled. Sufficient time should be given to the intermediary to: undertake the technical activities ensuring the order's completeness; make sure it can be carried out correctly; and avail of the possibility to appeal the decision. The required response time should be proportionate to the level of risk and exposure to illegal/harmful content of the platform. Hence, it is requested that existing sub-rule 4 of the 2011 intermediary rules be retained, which has specified the time limit as 36 hours.
- iii. **Storage of data** – When requiring service providers to preserve content for an undefined period lawmakers risk imposing new data retention requirements on telecom service providers. This would increase legal uncertainty and confront companies with new financial, logistical and technical challenges. There should be a time limit prescribed and it should be clarified that the storage is required for a maximum period (example - 180 days or 240 days) and longer periods should only be provided that there is a direction from the Court of Law or a lawfully authorized Government agency.
- iv. **Checks and balances to avoid misuse of the regulations and cost Sharing:** It is necessary that the regulations are not misused to enable individuals / Corporates to obtain court orders which benefits their commercial activity and ensure compliance through ISP's. It is important that there should be equal penal provision on the individuals/ corporates / authorities who may misuse or take advantage of this regulation.

6. Rule 3(9)

Rule 3(9) of the Draft Rules mandates that intermediaries undertake proactive identification, monitoring and filtering of content through automated tools, as a pre-requisite for an intermediary to be able to claim exemption from liability.

COAI Response:

We recommend removing this for the reasons detailed below:

- i. **Violation of Fundamental Right to Privacy** - This creates a legal incentive for intermediaries to engage in overbearing censoring of content in order to retain legal immunity, thereby potentially censoring lawful content and violating the privacy of users.

- ii. **Contrary to Supreme Court Ruling** - The obligation of the intermediary to adjudicate content as unlawful, has been read down by the SC's decision in *Shreya Singhal v. Union of India*. This obligation is being re-introduced in the Draft Amendment, which goes against the Supreme Court mandate. The Supreme Court of India categorically read down any obligation of intermediaries to assess the lawfulness of content and restricted its responsibility to taking down content when requested to do so by court order or authorized government agency along the lines of the 'notice and take down' model applied via international best practice.
- iii. **Censorship role assigned to intermediaries** - By making intermediaries the monitoring bodies, the rule also places the responsibility for assessing the legality of speech and expression of users in the hands of private entities that are neither the Court nor authorized government agencies, contrary to what is envisaged by the IT Act, Supreme Court judgment in the *Shreya Singhal* matter, and the Manila Principles. We are concerned that this obligation amounts to the privatisation of law enforcement, and places upon intermediary's obligations which go well beyond their role as commercial entities. This will also lead to subjectivity and uneven implementation across intermediaries. As telecom operators, the telecom license conditions also state that '*once specific instances of such infringement are reported to the Licensee by the enforcement agencies/Licensor, the Licensee shall take necessary measures to prevent carriage of such messages in its network immediately.*'
- iv. **Blocking orders can be issued without any safeguards** - Section 69A of the IT Act and the rules notified thereunder already provide for a procedure of issuing blocking orders with specific processes and safeguards. The Draft Amendment seeks to introduce a parallel process for the same under Section 79 of the IT Act without providing for any safeguards.
- v. **Onerous** - Deployment of automated tools or appropriate mechanisms to monitor content is also extremely onerous as a precondition to getting safe harbour as it involves creating new technology or deploying additional resources with very little clarity on what would be the threshold of content monitoring that would meet the relevant criteria.
- vi. **Violation of international standards and Manila Principles** - The global best practices in intermediary guidelines are usually structured along the lines of the Manila Principles, which states that Intermediaries should be shielded from liability for third-party content stored and uploaded at the request of a user. This is the fundamental principle based on which any intermediary liability regime should be structured. Making intermediaries liable to monitor content would put India's legal regime out of step with global best practices.

- vii. **Contradiction:** The proposed amendment is in contradiction of the very definition of intermediaries under the IT Act, as intermediaries are only making available a communication link over which the information of the users is transmitted or temporarily stored/hosted.

In conclusion, we would like to submit that if the Draft Amendment were to come into effect in the present form, it would put India's legal regime significantly out of step with global best practices. Further, requiring intermediaries to deploy mechanisms to identify, filter, and remove access to unlawful content adds to the chilling effect to free speech and expression as the intermediaries may apply these measures too aggressively in the interest of legal compliance.

As COAI, we support the introduction of proportionate rules which incentivise operators of digital platforms to take more responsibility for the dissemination of illegal and harmful material on their sites. In the context of the draft rules, we believe that a sensible balance can be struck which does not penalise digital platforms for acting in a more responsible way.

Crucially any such measures need to be narrowly targeted at the Internet layer where the harm actually takes place: i.e. online platforms which allow for the upload of user generated content and the broad dissemination of illegal and harmful material. Such measures should expressly not apply to service providers involved in technical/passive activities ('mere conduits') who do not store or provide end users with the ability to access or share content with a wide audience on the public Internet. Thus providers of electronic communications services, caching services, enterprise cloud hosting services, content delivery networks and Internet registries should not be within scope.

We would urge that an opportunity of personal hearing be provided when our members can visit your good offices and explain our position with evidences and international best practices.

We look forward to your favourable consideration of our submissions made herein above.

Please note that one of our members, Reliance Jio has divergent views on this issue and may respond separately.

**COMMENTS ON THE INFORMATION TECHNOLOGY INTERMEDIARIES GUIDELINES (AMENDMENT)
RULES 2018**

BY XIAOMI GROUP

MIT/79/078

Rule	Issue/Concerns	Xiaomi's Suggestions
Rule 3 (4)	<p>The intent of the proposed change seems to be to make the users aware, on a periodic basis, of the intermediary's right to terminate access or usage rights and remove non-compliant information. However, it is not clear as to what 'user' category it covers. In case of business-to-business intermediaries, this obligation becomes pointless and very onerous.</p> <p>A conspicuous notification at the time of registration and a permanent provision in the rules and regulations, user agreement or privacy policy along with an obligation to inform users in the event of any changes to the rules and regulations, user agreement and privacy policy should suffice the intent.</p>	<p>The Intermediary shall inform its users at the time of registration and at least once every month shall incorporate a provision in either the rules and regulations, user agreement or privacy policy of its computer resource for not less than ten (10) consecutive days in every calendar year, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of Intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information. In addition, and without prejudice to the foregoing, the Intermediary shall notify its users in the event of any changes to the rules and regulations, user agreement or privacy policy of its computer resource.</p>
Rule 3 (5)	<p>It is not clear as to what constitutes a "lawful order". The right to seek information should be limited to the 'orders' issued by court of law or the authorities and agencies authorized and notified under Sections 69, 69A or 69B of the Act.</p> <p>The usage of the phrase "as asked for by any government agency or assistance concerning..." suggests that the information may be asked for by persons other than the appropriate government agencies, that is <i>ultra vires</i> the Act. Rule 3(5) should be limited to seeking information for any assistance in terms of interception, monitoring, decryption, blocking for public access and collecting traffic data as required by the court of law or appropriate government are covered under Sections 69, 69A or 69B of the Act.</p> <p>Also the requirement of making any such requests in writing should be mandatory and not on an optional basis. This is also in line with the requirement under Sections 69 and 69A of the Act which mandate "...reasons to be recorded in writing, by order..."</p>	<p>When required by an order issued by a court of law lawful order, or on being notified by the appropriate Government or its agency under Sections 69, 69A or 69B of the Act, the Intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by the court of law or any appropriate government or its agency or for assistance concerning security of the State or cybersecurity; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can shall be made in writing or through electronic means stating clearly the purpose of seeking such information in the prescribed format or any such assistance.</p> <p>The Intermediary shall, on a best efforts basis, enable tracing out of such originator of information on its platform as may be required by an order of a court of law or by government agencies who are legally authorised under Section 69 or Section 69B of the Act. Where an intermediary, despite its best efforts, is unable to trace the originator, it shall provide</p>

	<p>A format should be prescribed to enable intermediaries to provide the required information in a definite and a time bound manner.</p> <p>We understand that the obligation to ensure traceability under Rule (5) is further to the requirements of Section 69. While Section 69 requires certain procedures and safeguards to be prescribed, subject to which orders on interception, monitoring and decryption are to be carried out, the provision under Rule 3(5) lacks any such safeguards or procedures. Due to its vagueness and the absence of the safeguards on individual's privacy, the traceability requirement under Rule 3(5) is likely to be violative of the fundamental right to privacy as recognized and set out by the Honourable Supreme Court in <i>Justice K.S. Puttaswamy & Anr. v. Union of India & Ors.</i>¹</p> <p>Further, every intermediary may not always be successful in tracing the originator, especially when a user masks his/her identity or if the user has deleted the data before the issuance of orders of the court or government and such data is irretrievable. The obligation, therefore, should be limited to taking all steps or using best efforts and in case intermediaries are unable to trace the originator despite undertaking best efforts, the reasons can be provided in writing and that should be taken as fulfilment of this obligation.</p>	<p>reasons in writing that shall be deemed to fulfil its obligations under this Rule.</p>
<p>Rule 3 (7)</p>	<p>The phrase “fifty lakh users in India” is very ambiguous. It is not clear as to what this user category covers – whether it is daily active users or registered users but are dormant. It is also not clear if fifty lakh users in India is a cumulative number of the users generated within a certain period of time (such as one calendar year, etc.) or during the entire operating time of an intermediary.</p> <p>The government should notify the list of intermediaries who must compulsorily comply with the requirements set out under (i), (ii) and (iii) of Rule 7.</p>	<p>(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:</p> <p>(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;</p> <p>(ii) have a permanent registered office in India with physical address; and</p> <p>(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.</p>

¹ WRIT PETITION (CIVIL) NO 494 OF 2012

<p>Rule 3 (8)</p>	<p>The power to issue directions to remove or disable access to any information through any computer resource is granted under Section 69A of the IT Act, 2000. Section 79(3)(b) merely annuls the safe harbour for Intermediaries in the event of such Intermediary's failure to remove or disable access to the unlawful content.</p> <p>The reference to sub rule (6) of Rule 3 is unclear as the same does not prescribe any timelines. The timeline itself should be increased to 72 hours to accommodate cases where the unlawful content is stored outside India.</p> <p>In case of user generated content, it may not be possible to retrieve such information if the user chooses to delete the same. The requirement of preserving such information and associated records should, therefore, be limited to cases where the same are retrievable.</p>	<p>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) 69A of Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four seventy-two hours in accordance with sub-rule (6) of Rule 3.</p> <p>Further, where retrievable and notified by a court order, or by the appropriate Government or its agency under section 79(3)(b) 67C of Act, the Intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required.</p>
<p>Rule 3 (9)</p>	<p>The rule in the present form is violative of the right to free speech enshrined under Article 19 of the Constitution of India and as upheld by the Honourable Supreme Court in the matter of <i>Shreya Singhal v. Union of India</i>² as well as the fundamental right to privacy as recognized and set out by the Honourable Supreme Court in <i>Justice K.S. Puttaswamy & Anr. v. Union of India & Ors.</i>³</p> <p>The obligation to pro-actively, and on an anticipatory basis, take down unlawful content requires intermediaries to apply their own mind in judging the lawfulness of the content and thereafter self-censor the content. Both these requirements are contradictory to the Honourable Supreme Court's directions in <i>Shreya Singhal v. Union of India</i>⁴.</p> <p>The requirement under Rule 3(9) is also contradictory to Section 79 of the Act, which provides a safe harbour to Intermediaries provided Intermediaries do not "<i>select or modify the information contained in the</i></p>	<p>The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content</p>

² AIR 2015 SC 1523

³ *Supra* note 1

⁴ *Supra* note 2

	<p><i>transmission</i>". Requiring Intermediaries to exercise their own judgement, when Intermediaries are, by their very definition, neutral platforms is against both the letter and spirit of Section 79.</p> <p>The determination of what content or information should be taken down should be made by a court or government agency of competent jurisdiction, as provided for under the amended Rule 3(8).</p> <p>Further, the obligation to mandatorily deploy technology based automated tools may not be commercially and/or technically feasible for small and medium scale intermediaries. This requirement could therefore become an impediment to the establishment and development of intermediary based e-commerce entities.</p>	
--	---	--

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

ANNEXURE

AMCHAM SUBMISSION ON THE DRAFT AMENDMENT TO THE INTERMEDIARY GUIDELINES

- Intermediaries as entities that provide services in the form of online content to end users host a lot of security and privacy issues. The draft amendment of these rules which was issued by Ministry of Electronics and Information technology (MeitY) may result in eroding the safe harbour protection available to intermediaries. Intermediaries in the form of Internet Services providers (ISPs), Search engines, Web Hosts and Website Providers are some players that come under the gamut of affected players. While the end user is free to post or generate content which may be illegal or may infringe someone else's copyright or obscene content, the liability of this content may come to the intermediaries who host or transmit this content.
- The new intermediary guidelines mandate these intermediaries to put forward a set of rules to the user. The set of terms of such regulations have a broad list of categories of content which should not be posted by the user. In these days of fake news and misconstrued arguments, it is important to bring Safe harbour guidelines and not burden the intermediaries.
- ISPs/TSPs should be exempt from the definition of Intermediaries under the act. As they are mere carriers or providing access to internet or connect destinations. No content is generated by the TSPs/ISPs who are already bound by the terms and conditions of their respective license agreements in this regard. Providing same time frame for all categories of intermediaries is unjustified given the varying nature of intermediaries – some of these platform providers have no control on the traffic even if its encrypted.
- While lawfully, free expression online is a human right, the right includes freedom to hold opinions without interference and to seek, receive and impart information which gives more choice, power and opportunity. Online platforms' ability to innovate and operate responsibly.
- The vague legal standards and uncertainty may hamper investments and innovation in the country as it brings uncertainty in the business environment and increases compliance cost for big and small players alike. This also creates barriers to competition and brings an uneven playing field.
- Carefully designed legal frameworks regarding liability for illegal third-party content makes innovation and responsible operation possible for online platforms. These laws make sure that as long as an online platform meets certain conditions, it is not liable for the third-party information, data or communications link which is generated by its users.
- With more than 80% of internet traffic encrypted, the ISPs as a carrier and owner of bandwidth cannot deliver a technological solution to detect, trace or report offenses related to the security of the state. We would further recommend that they advocate against the replacement of "terms and conditions" with "privacy policies." Privacy policies are generally intended to provide users notice about data collection and use practices. User agreements or other terms and

conditions are more appropriate vehicles for providing users notices about what they may or not be able to post on a given platform. Given the trend to have reader friendly privacy policies, this rule that mandates content unrelated to privacy would introduce confusion and complexity.

- The proposal also introduces the need of ‘Traceability’ which violates the provision of end-to-end encryption through some service providers and while the state would want to trace the source of messages which are inducing violence or fake news, it endangers the promise of end-to-end encryption by larger platforms. The free flow of information is essential to creativity and innovation and leads to economic growth for companies and countries alike.
- There is a need for clear rules for today which promise flexibility for tomorrow. When platforms follow their removal obligations under the law, they should be certain that they will not be held liable for the third party hosted content. It must also be noted that because technological change can render language obsolete, safe harbours should not be limited to enumerate lists of services or technologies or conditions, but should be allowed to operate on certain broad universally accepted principles.
- While it is important for platform to take down content through a notice-and-take down approach, it is important that there should not be rigid timelines for content removal which imposed short turnaround times. This inhibits companies from carefully considering the merits of each supposed infraction.
- The lack of procedural safeguards brings uncertainty on the circumstances under which intrusive and potentially privacy endangering requests can be made, and who can make such requests. Adding to the concern, extremely strict and short-term limits for direct compliance leads intermediaries with no time to address unlawful requests. Recent amendments in the Aadhaar Act also rule out that unfettered access to citizen data would not be permitted and it is important for the country to not undergo such legal changes that prove to be unstable.
- In the regulation to require intermediaries to implement proactive measures, it has become difficult for intermediaries to work sustainably. If failing to filter a particular piece of content which could endanger a service and its legal whether through fines or engineering changes, then platforms can’t take a fair approach to content removals and will have to take a ‘better safe than sorry approach’ which in this case mean ‘take down first, ask questions later’.
- Self-regulation in terms of conducting due diligence and removing the content will also have concerns. ISPs under their telecom license issued under the Indian Telegraph Act, 1885 need to ensure privacy of its customer with no deep packet inspection. Given such mandates it is not possible to expect ISPs to check their customer traffic in the name of conducting due diligence. This is also at variance with section 79 of the IT Act 2000 which extends safe harbor. Even with DPI ISPs will not be able to look within IP packets payloads due to encryption of social media transmission. Therefore, even if this amendment/rule overrides previous privacy acts, ISP may not be able to implement it.
- ‘One Size Fits all’ standard or principle of review and reviewing content is not appropriate. Online content sharing platforms that actually host the content must be distinguished from other

services that may not have direct access to content, electronics communication services, and enterprise B2B services. Here, instead of the enterprise cloud provider, the business entity providing the end service to its users or customers is in a more appropriate position to handle removal and user information requests along with conducting proactive monitoring.

- **Removal of Provision:** 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, etc.
- **Graded Content Takedown Time Limits:** 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. Some ISPs are not capable of complying due to predominant use of encryption in social media transmission and should be granted exception.
- **The extended retention period introduces significant burden on intermediaries from increased costs to storing, protecting, and administering the retained data.**
- **Stop the Clock Provisions:** 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.

Introduction

The Internet is a key enabler of rights and socioeconomic progress, and online intermediaries play an important role in letting people access the Internet and take advantage of all the opportunities it offers. Social media platforms provide the perfect condition for the creation of cascades of information of all kinds. The power of these platforms has been leveraged to create social movements like Black Lives Matter and the MeToo and TimesUp campaigns.

However, this power has also been exploited to sow discord and manipulate elections. India has been reeling from the consequences of misinformation floating on social media and messaging platforms. Rumours, especially related to possession of beef and child kidnapping have led to the deaths of several innocent people.

In the wake of increased spread of misinformation on social media, the Ministry of Electronics and Information Technology (MeitY) has issued a draft amendment to the Information Technology (Intermediaries Guidelines) Rules, 2011. The most contentious provisions of the new draft Rules, [*The Information Technology \[Intermediaries Guidelines \(Amendment\) Rules\] 2018*](#), are Rules 3(5) and 3(9) that require intermediaries to:

- enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised; and
- deploy technology based automated tools to proactively identify and remove or disable public access to unlawful information or content.

SFLC.in conducted a series of discussions on misinformation and the proposed Draft Intermediary Guidelines across India in January 2019 including New Delhi (Jan 11), Bengaluru (Jan 15), Mumbai (Jan 16) and again in New Delhi (Jan 18). Another discussion is scheduled to take place in Kochi (Jan 30).

This Blue Paper contains the comments, remarks and inputs made during the above-mentioned discussions by the participants. It is being released in the the current state in order to facilitate readers in drafting comments to be submitted to the Ministry of Electronics and Information Technology by 31 January 2019. This document does not reflect the views of SFLC.in.

New Delhi – 11 January 2019

Agenda

“Killing the Messenger: A Roundtable Discussion on the Draft Intermediaries Guidelines (Amendment) Rules, 2018”

Session 1: Background and Context Setting

1. The Current Rules: What is Section 79 of the IT Act, 2000 and how do the current Intermediaries Guidelines Rules, 2011 affect the multi-stakeholder community?
2. Points of distinction between the current rules (2011) and the draft rules (2018).
3. The effect of the the Shreya Singhal judgment on Intermediaries Guidelines. Do the draft rules comply with conditions laid down in Shreya Singhal?
4. Draft rules and their repercussions on the right to privacy as enunciated by the Puttaswamy judgment.

Session 2: Impact and Way Forward

1. Content filtering and the impact of the draft rules on the multi-stakeholder community.
2. A backdoor to encryption. Is it justified for due diligence?
3. The permanent establishment requirement for large intermediaries. Localisation all over again?
4. The Personal Data Protection Bill, 2018 and draft rules. Regulatory over-burden on intermediaries?
5. Global standards of Intermediary Guidelines. What are some best practices?

Note: This discussion was held under the Chatham House Rule. The following is a list of participants:

1. Amrita Choudhury, CCAOI
2. Anulekha Nandi, Digital Empowerment Foundation
3. Beges Malu, ShareChat
4. Rahul Sharma, IAPP
5. Rishab Bailey, NIPFP
6. Snehashish Ghosh, Facebook

7. Rajan Mathews, COAI
8. Vinayak Krishnan, PRS Legislative
9. Sudhir Singh, ISPIRT
10. Naman Aggarwal, Access Now
11. Yesha Paul, CCG – NLUD
12. Roshni Sinha, PRS Legislative

Session 1: Background and Context Setting

1. **Vagueness:** Terms like “promotion” in Rule 3(2)(j) and “blasphemous” in Rule 3(2)(b) are vague and need to be defined. In the Shreya Singhal judgement the court declared that Section 66A suffered from the vice of vagueness and had struck it down. Expressing concern over Rule 3(2)(j) the participants stated it could lead to excessive censorship of posts on social media as there is no clarity whether promotion means advertisement or is applicable in general.

2. Operational difficulties:

- There are difficulties from the operational perspective and due to over-regulation. At present there are a number of Acts and Regulations that TSPs need to comply with. For example although the licensing conditions already define ownership, terms like “belong to another person” under Rule 3(2)(a) make it difficult to make a quick decision and act.
- At present, the requirement for all intermediaries is the same. The fact that different categories of intermediaries serve different purposes has been ignored. Intermediaries could potentially be classified according to sectors and sectoral regulators and there should be specific rules applicable to them.
- The recent webinar with MeitY suggested that the Ministry is ready to look at different purposes of intermediaries for the purpose of classification with a focus on B2B.

3. Implications of automated filtering on safe harbour protection:

- Rule 3(9) requires intermediaries to deploy automated filtering. This provision would imply that intermediaries have to modify content which might take away their safe harbour protection.

- In this context, the participants referred to a case of European Court of Human Rights in which it was held¹ that the news portal could not benefit from safe harbour protection as it exercised editorial control.
- In Myspace Inc. vs. Super Cassettes Industries Ltd² it was held that the intermediary is not responsible for preventive filtering and must do so only under certain conditions.
- In light of the proposed automated filtering under the Rules, it is important to define intermediaries such that the action expected from them is in conformity with the Supreme Court judgements.
- Expressing operational concerns, the participants agreed that starts up may not have the wherewithal and financial ability to filter content.

4. Tracing without breaking encryption:

- In the Puttaswamy case³, the court stated that citizens have a fundamental right to privacy.
- As Rule 3(5) requires intermediaries to enable tracing the originator of messages, the participants discussed if this could curtail the right to privacy as it is not clear if the originator can be traced without breaking encryption.
- Further clarification from the government is required to understand what traceability means.

5. **Ambiguity under Rule 3(5):** It requires that the intermediaries shall within 72 hours of communication provide information or assistance as asked for by “any government agency”. The participants agreed that agency and the officer responsible for issuing orders must be specified.

6. **Ambiguity under Rule 3(7):** Rule 3(7) requires that an intermediary that has more than fifty lakh users in India shall adhere to the specified conditions. It must be clarified what this number means and how it has been arrived at. Importantly, such Rules must apply uniformly and the size or number of users of intermediary should not be a criteria to differentiate among intermediaries.

7. **Unlawful activity:** The role of intermediary to prevent unlawful activity needs to be further examined.

1 Delfi Judgment (Delfi AS v. Estonia, 16 June 2015)

2 236 (2017) DLT 478

3 2018 (9) SCJ 224

Session 2

1. Notice and Consent fatigue:

- Under Rule 3(4), the intermediaries are required to inform users at least once every month about the terms of access or usage which can result in notice and consent fatigue. This has been discussed in the Srikrishna report⁴. Sending such messages once every month to the user can result in user fatigue.
- Genuine messages such as information regarding changes in terms of service of a service provider may get lost in the barrage of monthly messages.
- Use of simplified language, vernacular language, monthly notifications, pop-up messages / showing links on applications that do not maintain user email address could be resorted to for resolving this issue. Pop-ups do not provide a good user experience.
- As the terms of service and privacy policy are usually in a language that is difficult to understand, most users may not be able to read and understand their contents. The focus, therefore, should be on using a language which can be understood easily. Further, importance should be given to informed consent.

2. Local presence:

- The draft Rules require a local presence of the intermediaries under certain conditions.
- Local presence and other regulations are a resource barrier for many startups as compared to the environment that prevailed when Facebook and Google started.
- At the same time, there is a legitimate concern regarding enforcement of jurisdiction against companies that do not have physical presence here. Many companies have not responded to notices from Indian authorities to their Indian offices, with the claim that they are mere advertising arms / marketing entities and have no relation to the parent company.
- Some participants felt that such companies must adhere to the laws in India if they want to do business in India. Under Companies Act, 2013 a foreign company is any company that is not

4 A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N Srikrishna, Available at: meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

incorporated in India, but does business in India, including business done via electronic mode. Such companies, therefore, have to adhere to the laws in India.

- Some entities may be in violation of the above. Evasion of cost of compliance and ease of incorporation abroad could be the reasons for not setting up offices here.
- According to an attendee, Indian companies are pushing for changes under the draft Rules as they want a level playing field for both Indian companies and foreign companies, regardless of size.
- Some participants felt that requirements mandating companies to follow different laws in different jurisdictions may lead to balkanisation of the internet.
- The incorporation requirement in the proposed Rules seems to categorize intermediaries arbitrarily and there is no legal basis for this. Clarity is needed on this front. It might be open to challenge under Article 14 of the Constitution.
- The participants explored more options such as the requirements in Vietnam. Vietnam has mandated that the companies set up a representative office with a grievance redressal officer within Vietnam's jurisdiction. This is not the same as requiring a company to be set up in the country.

3. Impact of regulation on innovation and startups:

- Participants felt that bigger companies are complying with laws across multiple jurisdictions but smaller companies will find it challenging. As most startups are started by techies who are not well versed with the laws, they will find the compliance requirements discouraging.
- As seen from past experience, in Europe the barriers are higher compared to those in Silicon Valley. These differences have had a high impact on innovation. One of the participants mentioned that in the Data Science Conference in Amsterdam, it was emphasized that the requirement of local presence under GDPR makes it difficult to share data and acts as a barrier to innovation.
- A possible solution for this could be what the European Commission is doing by defining a framework wherein if a certain threshold is crossed, then the platforms will self-identify as significant data fiduciaries instead of letting a data protection authority determine who will be a significant data fiduciary. However, this could result in passing the burden to the platforms.
- Vague regulations can create a bigger problem in the form of cost overheads.

- Some participants opined that as markets are emerging and maturing, more regulations are inevitable. There is a basic principle that the economic opportunity should justify the cost of compliance. OTT platforms, unlike telecom operators, do not require licensing fee. The requirements are not so onerous that they deter companies from doing business and hamper startups. Consequently, the cost of regulation is not very high.
- Participants explored how different intermediaries could have different obligations. For example, out of the various categories of intermediaries, hosting service providers tends to have higher responsibility. Intermediaries modelled on B2C will have a larger impact than B2B. The Rules must distinguish between these.
- The cost benefit of implementation has to be worked out by the government. Making safe harbour conditional on mandating automated filtering of content is not implementable. What needs to be looked at is the ripple effect these laws can have on the IT sector across jurisdictions.
- Seeking support from the government for free and open source automated prior censorship tools is a slippery slope, but this can be explored. This solution could also go against innovation as it does not incentivise exploring different ideas.

4. Fake news:

- Participants discussed latency issues (how quick can intermediaries act), horizontal applicability of free speech rights, Election Commission's guidelines on fake and paid news (registering of social media handles, disclosure of people hired for social media).
- Participants pointed out that horizontal applicability has its own challenges as it involves adjudication of complex issues by platforms to decide what content is lawful and what is not. Moreover, AI cannot be used to monitor fake news as it has its inherent challenges.
- User awareness is extremely important to tackle fake news.
- Participants agreed that proportionality must be built into take down notices, censorship demands for information.

Agenda

“Countering Misinformation: Policies and Solutions”

Locations:

- 15 January 2019: Bengaluru
- 16 January 2019: Mumbai
- 18 January 2019: New Delhi
- 30 January 2019: Kochi (Upcoming)

Session 1: Contours of “Fake News” and its Impact on Society

1. Deconstructing Misinformation and “Fake News”: Defining terms and limits.
2. The proliferation of misinformation enabled by the Internet: The network effect and its realities.
3. The impact of this information disorder on society: Freedom of speech and national security.
4. From Donald Trump to Jair Bolsonaro: Elections in the era of digital campaigns.

Session 2: The Way Forward: Do we need more regulation?

1. Key challenges of content moderation in the digital sphere: The risk of over regulation.
 2. Harmonizing the right to privacy with access to law enforcement: Backdoor to encryption.
 3. Role of various institutions in combating misinformation (Government, Media and Tech Companies): Assessing accountability.
 4. Alternatives to government regulation: A stronger focus on digital literacy.
-

Bengaluru, 15 January 2019

For agenda, please refer to page 9.

The Roundtable was organised in partnership with the Indian Institute of Management Bangalore and the Independent and Public Spirited Media Foundation. It was moderated by Biju Nair, Executive Director, SFLC.in and Priyanka Chaudhuri, Counsel at SFLC.in, The following is a non-exhaustive list of participants to the Roundtable.

1. Rajeev Gowda, Member of Parliament
2. Sanjay Sahay, IPS
3. Malavika Prasad, Legal Researcher
4. Akriti Bopanna, CIS
5. Rahul Matthan, Fellow, Technology and Policy Research at the Takshashila Institution and Partner, Trilegal
6. Kanchan Kaur, Dean, Indian Institute of Journalism and New Media
7. Timothy Franklyn, Partner, Tatva Legal
8. Sridhar Pabbisetty, Public Policy Analyst
9. Siddharth Narrain, Independent Lawyer
10. Nayantara Ranganathan, Internet Democracy Project
11. Ram, Free Software Movement of Karnataka
12. Shreyas Satish, Founder, OwnPath
13. Sneha Banerjee, Independent and Public Spirited Media Foundation
14. Anna Isaac, Journalist, The News Minute

Session 1: Contours of “Fake News” and its Impact on Society

- The definition of ‘fake news’ is vague and ambiguous and has to be deconstructed. There is no real agreement as to what the expression means. It is being used in an elastic manner and is being brandished as an all purpose slogan to describe everything from errors to deliberate falsehoods. We have seen world leaders weaponizing this term and using it against news organizations and journalists whose coverage they find disagreeable.

- Traditional media had a particular reputation and integrity, but with the advent of social media platforms, everyone can be 'journalist'. People are willing to share information to increase their popularity. The speed and ease with which the information travels is unparalleled.
- Mainstream media is partly to be blamed for contributing to the fake news ecosystem.
- The spread of misinformation is linked to human beings making decisions. Any kind of speech should not be censored as individuals should be able to make a choice (whether they want to read a particular news item or not).
- Print and broadcast media have certain editorial processes they follow. It's unclear whether news websites in the online space follow the same standards and processes.
- The architecture of social media is built to control how an individual engages with the content they experience. That is not the control that print or broadcast media wields on its reader or viewer.
- All over the world, fake news is also peddled by political parties. We need to think about what it means when misinformation is emerging from people who have control over law enforcement.
- Our information diet is coming from algorithms on social media platforms. There is a real problem of filter bubbles on these platforms. If you follow a particular website that spreads fake news, it is very likely that the response of fact checkers to that will not reach your timeline. Therefore, it is important to think about algorithmic transparency and algorithm accountability.

Session 2: The Way Forward: Do we need more regulation?

- It was asked whether regulation or moderation was needed at all and further stated that moderation perhaps was only warranted in cases where there was actual danger to life and liberty. Credibility is the only currency in the world of journalism.
- Regarding deployment of artificial intelligence, industry experts dealing with AI on a regular basis claimed that AI was nowhere near to ready for the task of solving human and political problems; AI inheriting the bias of its creator was also discussed.
- A co-regulation solution wherein the government and private players could collectively decide whether some news was fake or not was proposed. Some attendees suggested self-regulation.
- A decentralized blockchain type of voting system by people which would automatically put up credible news was suggested.

- A licensing regime to authenticate genuine websites was discussed for newspapers but the question of who would be the regulator remained undecided. The possibility of the government being made the regulator was discussed by rejected vehemently by the participants.
- News of the sort that causes ‘harm’ is a crime and should be prosecuted, although the definition of harm must be clear. Prosecuting individuals for spreading news that is not good for collective morality is problematic. As long as it does not cause harm, it should not be a problem.
- In spite of giving lip service, India has never really put out real open data for independent researchers to critique govt actions and what could be done better.
- University of Cambridge came out with an immersive role-playing game called ‘Bad News’⁵ wherein the user goes through the life-cycle of a troll. The game is helpful in understanding the components of Fake News.
- On content moderation, it was said that if Germany can require Facebook to go through each and every video that is uploaded, then India can do the same for bigger intermediaries. Bigger companies have enough resources to do something like this.
- The problem lies in our education system. Apart from digital literacy, we need to teach critical thinking skills to young people. We, as a country should encourage a culture of questioning.
- Fact checking should become an essential part of good journalism. A journalist / reporter should not push out stories without fact checking them. Social media platforms should tie up with fact checkers. The ‘forwarded’ feature of WhatsApp is a good initiative. Initiatives like Ekta Coalition are useful.
- Other solutions that were mentioned by attendees were giving incentives to startups that do fact checking, giving tax breaks to small organizations that bring truth back as an important value in the digital realm. Banning things does not work, proper incentive structure should be provided.
- Decentralization of technology is important: There is already a decentralized search engine called “SearX”.
- There was a suggestion to implement a digital point system like Steam It in India.
- The general consensus relating to the Draft Intermediary Guidelines, 2018, was that the Guidelines were unnecessarily restrictive and cast a huge burden on intermediaries to forcibly “deploy technology based automated tools or appropriate mechanisms, with appropriate

5 Available at <https://getbadnews.com/>

controls, for proactively identifying and removing or disabling public access to unlawful information or content.”

- The Rules mandate due diligence responsibility on intermediaries, which would mean pre-screening the content. Sub rule 9 creates a positive obligation to remove content by use of the words “shall” and “proactive monitoring”, which implies that even without an order, the intermediary should remove content.
- A question was asked specifically pertaining to Rule 3(5) was that whether it’s possible to trace the originator of information on a platform which deployed end-to-end encryption such as WhatsApp. The answer by the technologists was in the affirmative. They stated that while it was matter of public knowledge that WhatsApp deletes messages from its servers as soon as they were delivered, it is unknown whether or not WhatsApp stores metadata of these messages and if so, for what period of time. Metadata could lead to the point of origin of a message.
- It was unanimously agreed that intermediary guidelines should provide for different types of intermediaries; roughly: large intermediaries, medium intermediaries and small intermediaries. A criteria based on function, revenue and number of users etc. should be applied. A one size fits all approach is problematic.
- There are two ways to think about regulation. For example, if we consider the problem of air pollution, Government can either regulate the polluter or it can mandate everyone buys air purifiers. In the new IL rules, they are mandating everyone read the terms and conditions while they should really be regulating the tech giants who are building this flawed distorted infrastructure. If we allow the government to set the terms of the debate by critiquing just these Rules, then the government will push more privatization of burdensome regulation. We should be re-framing the terms of the debate and ask the government to do its job instead of putting the onus on citizens.

Mumbai – 16 January 2019

For agenda, please refer to page 9.

The Roundtable was organised in partnership with MouthShut.com. It was moderated by Prasanth Sugathan, Legal Director, SFLC.in and Priyanka Chaudhuri, Counsel at SFLC.in, The following is a non-exhaustive list of participants to the Roundtable.

1. Geeta Seshu, Independent Journalist, Advisory Board Member, SFLC.in
2. Faisal Farooqui, Founder and CEO, MouthShut.com, Board Member, SFLC.in
3. Vickram Crishna, Engineer working at the intersection of technology and education, Advisory Board Member, SFLC.in
4. Sachin Kalbarg, Executive Editor, Hindustan Times
5. Jency Jacob, Managing editor, BOOM Fact Check
6. Smita Vanniyar, Point of View
- 7, Rega Jha, ex- Editor-in-Chief, BuzzFeed India
8. Bhusan Jatania, Senior Associate, IDFC Institute
9. Vijay Srirangan, Director General, Bombay Chamber of Commerce and Industry
10. Vidyut Gore, Technologist and Social Media Influencer

Session 1: Contours of “Fake News” and its Impact on Society

- To dissect the term fake news, we need to understand the intent of the individual who put out the wrong piece of information. There is a difference between someone who deliberately fabricates a story and a journalist who makes an honest mistake. Journalists in their enthusiasm to break a news story first, sometimes do not check the veracity of the story before publishing it. As long as the intent and impact is not criminal, there should be no prosecution. The question also arises whether we should punish someone that puts out something that is factually incorrect, even if it was with malaise.
- There is no way to establish a proper definition of ‘harm’ that includes all the components. It is a slow time bound process, decided on the basis of jurisprudence and case law just like the definition of ‘defamation’ took years to develop.

- Tech platforms make it very easy for fake news to spread. Platforms like Facebook are not passive intermediaries; they are active. They actively propagate certain kinds of content. Such intermediaries do not just have responsibility but also liability.
- There is a general mistrust in institutions that have formed over the last couple of years. People do not trust their doctors, politicians, law enforcement, and media. There is a lot of misinformation especially in the health sector.
- It is important to regulate paid news and funding of TV channels to fight the problem of fake news.
- There is no absolute right to free speech. The Internet is a medium that is relatively anonymous and users hide behind the mask of anonymity to do whatever they want. That link of anonymity should be decisively cut by the intermediaries. There should be a real person linked to every account on social media.
- Disagreeing with the above-mentioned point, a participant mentioned that there are human rights defenders, journalists and activists who do not want to reveal their identity for safety reasons. Disallowing anonymity would lead us towards China's social credit system.
- When we talk about anonymity, it is a slippery slope. Right to anonymity like other rights is a privilege and can be revoked if its misused. Anonymity v. Security is a dangerous path to go down specially when we are talking about a law proposed by the government. The right to anonymity is already being cited as a threat to national security.
- Every media organisation has a different policy regarding social media. Until the editor of a particular beat has approved the news in question, the social media team should not publish it. Two level or three level filtering should be carried out before publishing a piece of news.
- WhatsApp maybe facilitating lynchings but it cannot be the cause of it. It is a social problem that cannot be solved at the technology level. India's social structure is complex with issues like caste, religion, social and economic hierarchy.
- The Election Commission has failed in dealing with the problem of fake news. Enforcement of the model code of conduct that requires forty eight hours silence on social media before an election is difficult to enforce since there is no clear definition of a "party supporter" . Also, the Election Commission has a fundamental lack of understanding on how social media works and the said rule is a shot in the dark.

- The situation in India is different from USA where newspapers take a stance for or against the Government. The problem is paid news in India. Candidates use disproportionate amount of money and power to be able to put across one point of view. We are not talking about one or two candidates. We are talking about a larger ideological thrust. Tackling that is not easy.

Session 2: The Way Forward: Do we need more regulation?

- The law can act like a minesweeper. There have been several instances when the law did not just prosecute the accused, but innocent people as well. We have to look at regulation in a larger context and ask: who is regulating, what is it they are regulating, how is the regulation being implemented? Regulation should be such that it aids in the growth of a free Internet. The current regulation is restrictive.
- The United States is trying to control data to the exclusion of other countries. MLAT is broken, therefore the draft Rules are important to hold people accountable. The only way to control fake news is to hold individuals accountable by due process of law. Methods of investigation in the online world are different from the offline world. In the online world, implementing traceability is essential for the purpose of giving access to law enforcement agencies. There should be a real person linked to every account on social media.
- The new Rules require intermediaries to curate content which is against the Supreme Court's reasoning in *Shreya Singhal v. Union of India*. Intermediaries should be mere conduits without any adjudicatory function.
- Automated filters will lead to increase in content take down. There are two problems with AI: it is easy to get around it, and design problems - it contains existing biases of the person who developed it and these biases get amplified. AI can be a tool but it cannot be a decision maker. Language has many social and cultural contexts which is hard to understand by AI. It is showing signs of failure already.
- 'Blasphemous', 'offensive', 'grossly harmful' are not words defined in law. These are borrowed from Section 66A of the Information Technology Act which was struck down by the Supreme Court.
- A legitimate concern is balancing curbing misinformation with excessive surveillance. If traceability is enforced, there should be enough checks and balances so that it is not misused. Judicial oversight must be ensured. There should be a provision in law to challenge the

surveillance order after the investigation is complete. Special courts must be assigned to look into this and surveillance should be time bound.

- If there is more regulation by the State, then there should be more regulation of the State via checks and balances.
 - When we talk about regulation in terms of monitoring and control, it will not work. We have to put suggestive fears and social penalties. We need to build a cultural ecosystem that promotes a certain kind of behaviour.
 - Regulation need not be a punitive measure. There can be a creative aspect to it as well: making digital literacy compulsory in schools. The education sector needs to be revamped. Nurturing critical thinking skills is extremely important. It is also an important aspect of building an information society.
 - Trust in the mainstream media has to be rebuilt. There cannot be a one size fits all solution to misinformation. A more graded response to different kinds of misinformation is needed.
-

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

New Delhi – 18 January 2019

For agenda, please refer to page 9.

Panellists in Session 1:

- *Abhinandan Sekhri* – Co-founder and CEO of NewsLaundry;
- *Rupa Jha* – Head of Indian Languages services at BBC World Service;
- *Prasanto K Roy* – Technology / Public Policy, Media and Communications Professional; and
- *Malavika Balasubramanian* – Journalist with the Quint.

Panellists in Session 2:

- *Karnika Kohli* – Audience editor at Scroll.in;
- *Siddhartha Jain* – Assistant Commissioner of Police, Cyber Cell, Crime Branch, Delhi Police;
- *Shehla Rashid Shora* – Student leader and activist from Jawahar Lal Nehru University;
- *Berges Y. Malu* – Public Policy & Corporate Affairs Head at ShareChat;
- *Ghanshyam Tiwari* – National spokesperson of the Samajwadi Party and Founder of Learner.in; and
- *Shashank Mohan* – Volunteer Counsel at SFLC.in.

Both panels were moderated by *Mishi Choudhary* – Managing Partner at Mishi Choudhary & Associates, and Legal Director at Software Freedom Law Center, NY.

Abhinandan Sekhri - *Co-founder and CEO of NewsLaundry*

- Defined fake news as demonstrably false claims. Spin is not the same as fake news.
- To say that fake news affects elections is far fetched. There is absence of empirical data to support this.
- Fake news can be combated once we are able to define it. Differentiating between platforms is a way to tackle fake news.
- He explained that commerce is the biggest impact for anything and therefore an evolving and disrupted revenue model for news has to be created.

- As a substitute for digital advertising model he underscored the need to differentiate between advertising for news and other content. Subscriber driven model on digital platforms can be a solution. Subscription results in subscribers paying a premium for real news and it helps everyone else. Unlike television where advertisement rates are determined by the number of viewers and the content does not matter, digital platforms are different as they offer a space for evolving new revenue models.
- Solutions offered by MNCs in different countries will vary depending upon the sensitivities of the people.
- There are already systems in place for dealing with fake news from established media houses. For example, the Indian Penal Code provides for criminal defamation. Though the judicial machinery is slow the government must be kept out of this.

Malavika Balasubramanian - *Journalist with the Quint*

- Malvika emphasised that fake news is defined as misinformation, disinformation and mal-information.
- In India, we primarily deal with disinformation (news spread with the intention to harm) and misinformation (fake news spread with no intention of harming but the idea to do good). An example of misinformation – fake news about contaminated polio vaccine was disseminated in good faith but slowed down the polio vaccine campaign.
- While misinformation can be countered, checking the spread of disinformation is very difficult as there is a spin to it; a vested harmful propaganda.
- Fact checking is a basic foundation of journalism. It is a way to stop the information from going viral. This can be done by stopping the fake news from breaking.
- After checking the facts, the next aim is to put the fact checked stories back on the platforms they emanated from and make it as viral as the fake news. It has to be packaged in manner similar to fake news with catchy / click-baiting headlines.
- Quint has a WhatsApp broadcast channel for fact checking and a WhatsApp business number on which suspicious forwards can be sent. A list of suspects is also maintained.
- Rupa added that fact check by Ekta News Coalition published by BBC Hindi is doing the same for Hindi news. In her experience, people are eager to know the truth as people on both sides (those that make fake news and its consumers) are politically active.

Prasanto K Roy - *Technology / Public Policy, Media and Communications Professional*

- According to him, fake news is reality blown out of context.
- Given the nature of the internet is such that it enables the news to spread with extreme velocity, to tackle the menace of fake news it is essential to focus on the spread of information through online platforms.
- He explained the structure of the internet user base. As we go further down the socioeconomic pyramid, people depend on videos only for information. As compared to text, videos are easier to manipulate and are extremely potent sources of fake news. The fake news busters can't do anything about it as fact checking right now is limited to text at present. This will become an important issue in the future.
- Inability to find the source is the prime contributor to fake news. Mostly, it is the political parties, especially those in power and those in opposition that are the sources of such news. He gave example of how efforts have been made to counter this. Amnesty International established labs to verify fake news.
- He also referred to Rajesh Jain's analysis that 40% of undecided voters can be swung with repeated stories that have a certain pattern.
- Though platforms are not the source of fake news they have a responsibility to tackle fake news as online fake news can be replicated with ease and spread with lightening speed faster than we have seen ever before. For example WhatsApp came up with a forward tag and limited the number of people that a message can be forwarded to in one go in order to slow down the velocity of the spread by making people re-think.
- He explained that there is a traffic sustainability to fake news busting. The entire life cycle of fake news which includes – the fake news, denial, its impact and corrective action - attracts millions of views.
- Disrupting the encrypted business model of a platform or forcing the platform to identify anonymous posts is not the right way. At present digital forensics does not have the wherewithal to tackle the source of fake news and all that is needed is scaling up of the effort and resources.

Rupa Jha - *Head of Indian Languages services at BBC World Service*

- Rupa emphasised that the impact of fake news on elections is the most important concern today.

- Fake news sows biases, impacts the social structure, affects wise decision making and democratic discourse. It has been used as a weapon in the hands of autocratic leaders and is a big threat to our democracy.
- Citing the BBC research on fake news, she explained that nationalism is a reason for the spread of fake news. People don't intend to incite violence. Further, they forward the news as they trust the person who forwarded the news to them and are not concerned about the source.
- Traditional media such as the television still remains a big platform for consumption of news in India.
- Media houses are now focusing on busting fake news rather than reporting it. It is not just the big media houses but even the small media houses that are doing a lot to counter fake news.
- Talking about the source of fake news in India, she said that the spread of fake news from the right wing is very fast as the right wing network is very organised as compared to the left leaning wing. There is a concerted effort to mislead politics in India towards Hindu glory and jingoism.
- The government must encourage and empower independent journalism which is the basic requirement of a democratic setup. According to her, WhatsApp and Facebook are platforms that are popular for the spread of regional media. If we can start dealing with these two, we will be dealing with a lot of problems.

Shehla Rashid Shora - *Student leader and activist from JawaharLal Nehru University*

- She shared her personal experiences on how she became a target of disinformation campaigns which included calling her a member of separatist organisations, and siphoning funds meant for rape victims.
- People spread false information due to their confirmation bias. Fake news is not isolated but part of a concerted propaganda.
- Going live on social media to share the true version of the news did not help as sources of fake news had significant following and verified handles. This is compounded by unverified accounts with huge followers and bots that re-tweet the falsehood.
- Regarding law enforcement, she described her apprehensions including the possibility of cases being filed against her as most of the sources were backed by the political party in power.

- She suggested nurturing a ‘Culture of Scepticism’, wherein we should ensure credibility of news content and its source before sharing. Besides, political parties should come together in dealing with this issue.

Ghanshyam Tiwari - *National spokesperson of the Samajwadi Party and Founder of Learner.in*

- Every individual is responsible to bust any piece of information that seems incorrect.
- India should respond to fake news based on its own central values of diversity of communities and federal governments. Our response should not be that of a technocratic or autocratic, but of a mature civilization.
- He shared a BBC article which mentions that higher level of distrust towards mainstream media has pushed people to alternative, social media news sources. He suggested that mainstream media entities should engage more with people and create reliable content.
- Companies have been given a long leash by the government as they get away even after incidents of lynching. With high level of general illiteracy and abject disregard to digital literacy, busting fake news is not the government’s priority. . Alternatively, the role of key stakeholders at the grass-root level is of higher significance. ‘Save The Internet Campaign’ is a good example. On countering communal incidents fuelled by fake news, he suggested increasing inter-community interaction and sensitisation.
- He was critical of the procedure-oriented approach of law enforcement agencies which are not able to respond on time.

Berges Y. Malu - *Public Policy & Corporate Affairs Head at ShareChat*

- Most content claimed as fake news is innocuous sarcasm and the proper way forward should be user education rather than fact-checking services. He raised concern about the influx of Chinese platforms in India which actively perpetrate fake news, including political content.
- On the role of platforms in addressing misinformation, ShareChat has tied up with a fact-checking agency. Tools are being implemented to bar re-uploading of content that might incite violence or falsehood.
- He supported the viewpoint that foreign intermediaries must appoint local representatives in India as there have been cases where foreign apps have been known to share fake news and

illegal content. These entities take a long time to respond to take down requests from the government. Concerns that these Rules would encourage censorship are unfounded.

Siddhartha Jain - *Assistant Commissioner of Police, Cyber Cell, Crime Branch, Delhi Police*

- Common police complaints on the social media front include fake accounts, sharing obscene content, online frauds under the guise of government services and using crypto-currencies to hide black money, among others. Such crimes run into crores of rupees.
- Initiatives taken by the Delhi Police include creation of Twitter and Facebook handles, but more effective at ground level was making constables members of RWA WhatsApp groups which help in nipping fake news in the bud. Similar decentralized corrective measures should be introduced.
- Challenges faced by law enforcement in dealing with fake news are non-filing of formal written complaints by personally visiting police stations and non-cooperation of complainant in sharing information. The role of prosecutor and judge is also critical.
- The police on receiving information on a cognizable offence where threat to life is involved does register an FIR. Otherwise an FIR is registered if a complaint is referred to local magistrate.
- Instead of more regulation, better regulated should be used. Finding originator is one of the major requirements that the present draft Rules aim to address. The tech-companies are not proactive in cooperating with the police on taking down the content or locating the originators.

Karnika Kohli - *Audience editor at Scroll.in*

- Fake news is not sarcastic: where incidents of a meat being beef or not became fatal for few. There shouldn't be any regulation that comes from the government or tech-platforms. Change should come from the society itself with media and digital literacy being the way forward.
- On incidents of fake news in regional / vernacular media, she shared that vernacular media sources are witnessing higher viewership compared to others. She shared the example of Navbharat Times progressing towards highest online subscribers. However, fact-checking is limited to English media only.
- There is a lack of incentives to fact-checkers in advertisement based business models of online media groups.

Shashank Mohan - *Volunteer Counsel at SFLC.in*

- He brought up recent legal developments, particularly the Draft Intermediary Guidelines (Amendment) Rules, 2018. Changes introduced include automated taking down of content and traceability features to locate originators.
- The press release issued with the draft Rules states that ‘instance of misinformation on social media by criminals and anti-national elements, obscene content, terrorism, spread of disharmony, incitement of violence, fake news, lynching incidents’ among others to be the reason behind the draft Rules.
- In *Shreya Singhal v. Union of India*, it was held that in only two instances intermediaries may be asked to take down content – by an order by an authorized official or by a court order.
- The draft Rules are reminiscent of grounds mentioned in Sec 66A held unconstitutional in the *Shreya Singhal* case.
- Fake news is undoubtedly a problem, but breaking encryption in the garb of traceability might violate the fundamental Right to Privacy. Tracing the originator without decrypting the message is possible in the case of WhatsApp.
- He then directed the audience towards certain international developments such as the EU Directive on Copyright in the Digital Single Market which mentions automated content filtering and the Australian law⁶ that provides access to law enforcement agencies in decrypting information stored with private tech-companies.

⁶ Telecommunication and Other Legislation Amendment (Assistance and Access) Act, 2018

End Note

We thank all the participants in our discussions for participating and sharing their inputs, MouthShut.com Pvt. Ltd. for partnering with us for the discussion in Mumbai on 16 January 2019, Indian Institute of Management Bangalore and the Independent and Public Spirited Media Foundation for partnering with us for the discussion in Bengaluru on 15 January 2019.

The inputs received from the events conducted in different cities can be used by all readers of this document to form and submit their own comments and counter comments to the Ministry of Electronics and Information Technology (MeitY). As of the time of publication of this document, the deadline for submission of comments is on 31 January 2019 for comments, and 14 February 2019 for counter comments. Further information regarding the submission of comments and counter comments is [available here](#).

We hope that this document proves useful for creating and submitting comments, conducting discussions on the issue, and in enacting an informed policy on the issue at hand.

© SFLC.in

License: CC BY-NC-SA 4.0

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

January 31, 2019

Shri Ajay Prakash Sawhney,
Secretary, Ministry of Electronics and Information Technology,
Government of India,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003
secretary@meity.gov.in

MIT/79/081

Sub: Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

We write to you to express our concern on certain provisions of the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (“the Draft Rules”), recently issued by Ministry of Electronics and Information Technology (“MeitY”). These Draft Rules seek to amend existing Intermediaries Guidelines Rules, 2011 and emanate from Section 79 of Information Technology Act, 2000 which provides safe-harbour protection to intermediaries from liability due to third party content.

Following are some critical issues with the Draft Rules:

1. Disproportionate use of Government Regulation

The Draft Rules, despite being targeted primarily on social media platforms and messaging applications, would apply equally to all intermediaries including TSPs, ISPs, Cyber Cafes etc. This is a disproportionate use of government regulation.

2. Vague Terms Resulting in ‘Chilling Effect’

One of the grounds for the Supreme Court striking down Section 66A of the IT Act, 2000 in *Shreya Singhal* was the vagueness of the terms used in the provision, like - offensive, menacing and dangerous - as these disproportionately invaded the right of free speech. However, words with a similar level of vagueness, such as ‘grossly harmful, harassing and hateful’ still exist in the Draft Rules.

3. Privacy and Breaking Encryption

The Draft Rules require intermediaries to include a traceability feature to assist law enforcement agencies. Such a traceability requirement could lead to breaking of encryption on apps such as WhatsApp and Signal, and this will be a major threat to the privacy rights of citizens as enshrined in the Puttaswamy judgement of the Supreme Court. Addition of a requirement of traceability in a subordinate legislation is also beyond the rule making power of the Government.

4. Pre-Censorship and Automated Content Filtering

The Draft Rules require intermediaries to deploy automated tools for proactively filtering unlawful content on their platforms. This would result in a pre-censorship regime, violating the right to free speech and expression, where AI technology would crawl through social media to filter and remove content which it deems ‘unlawful’.

We request you to protect the principles of open and accessible internet, safe harbour granted to intermediaries and the fundamental rights of privacy and free speech of the internet users in India. While being cognizant of national security interests, we appeal for a less-invasive and proportional means of regulation of the internet.

Sincerely,

Signatories

COMMENTS OF THE INFORMATION TECHNOLOGY [INTERMEDIARIES GUIDELINES (AMENDMENT) RULES], 2018

The safe harbour provision under Section 79 of the Information Technology Act, 2000 (hereinafter the "Act") has had a crucial impact on the growth of digital economy in India. Intermediaries have benefitted immensely from the assurance that they will not be liable for content originating from their users, provided that they exercise due diligence and remove the content upon receiving actual knowledge of unlawful content.

Section 79 has thus been a key factor that has led to the proliferation of intermediaries in India, with India becoming one of the most important markets for multinational companies such as Facebook, Google, Amazon, Walmart etc. The importance of this provision was further highlighted by the Supreme Court in *Shreya Singhal v Union of India*, (2015) 5 SCC 1, wherein the Court further strengthened the protection available to intermediaries.

Our comments are as follows:

I. Comments on removal of Rule 3(4) and the proposed Rule 3(8)	2
I.A. KEY FEATURES OF THE PROPOSED CLAUSE	2
I.B. COMMENTS ON THE PROPOSED CLAUSE	3
I.C. SUGGESTION BY IRA LAW	4
II. Comments on proposed Rule 3(5)	5
II.A. KEY FEATURES OF THE PROPOSED RULE	5
II.B. COMMENTS ON THE PROPOSED RULE	5
II.C. SUGGESTIONS BY IRA LAW	6
III. Comments on proposed Rule 3(7)	7
III.A. KEY FEATURES OF THE PROPOSED RULE	7
III.B. COMMENTS ON THE PROPOSED RULE	7
III.C. SUGGESTIONS BY IRA LAW	9
IV. Comments on proposed Rule 3(9)	10
IV.A. KEY FEATURES OF THE PROPOSED RULE	10
IV.B. COMMENTS ON THE PROPOSED RULE	10
IV.C. SUGGESTIONS BY IRA LAW	14

I. Comments on removal of Rule 3(4) and the proposed Rule 3(8) of the Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

~~(4) The intermediary, on whose computer system the information is stored or hosted, 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 as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,~~

*(8) 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 Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ **one hundred and eighty days** for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.*

I.A. KEY FEATURES OF THE PROPOSED CLAUSE

1. The new proposed Rule 3(8) which effectively replaces Rule 3(4) has introduced the following changes:
 - (i) **Actual knowledge:** Actual knowledge statutorily requires communication of the unlawful act to the intermediary either through a court order or by the appropriate Government or its agency. This has been done to conform with the mandate of *Shreya Singhal*.
 - (ii) **Impugned information:** The impugned information under the erstwhile sub rule 4 was '*information that is in contravention of sub-rule (2)*'. This however has been replaced by '*access to unlawful acts relating to Article 19(2) such as*
 - (a) in the interests of the sovereignty and integrity of India;
 - (b) the security of the State;
 - (c) friendly relations with foreign States;
 - (d) public order;
 - (e) decency or morality;
 - (f) contempt of court;
 - (g) defamation; or
 - (h) incitement to an offence.
 - (iii) **Timeline to comply:** Upon receipt of actual knowledge, the intermediary is required to remove access within 24 hours as opposed to 36 hours as granted under the earlier rule.

- (iv) **Preservation of evidence:** All evidence must now be preserved by the intermediary for 180 days as opposed to 90 days as required under the earlier rule.

I.B. COMMENTS ON THE PROPOSED CLAUSE

1. The Supreme Court in *Shreya Singhal v Union of India*¹ (hereinafter *Shreya Singhal*) read down Rule 3(4) to mean that the intermediary would have to remove the impugned material only upon "...receiving actual knowledge from a court order or on being notified by the appropriate Government or its agency that unlawful acts relatable to Article 19(2)...". In other words, the Supreme Court held that an intermediary is not required to remove the impugned material unless the affected person had obtained a court order or the intermediary was notified by the appropriate Government/ its agency. The reasoning employed by the Supreme Court was that intermediaries are not in a position to determine whether the material they have been notified to remove, falls under Rule 3(2). The determination should therefore be done by a court or the government/ its agency and an appropriate order/ notification could be issued to the intermediary accordingly. However, *Shreya Singhal* also mandated that the actual knowledge so communicated should determine and indicate that the unlawful acts are relatable to Article 19(2) of the Constitution of India.
2. A division bench of the Delhi High Court interpreted *Shreya Singhal* in *Myspace Inc. v. Super Cassettes Industries Ltd.*² (hereinafter '*Myspace*') and applied it to an intellectual property dispute while discussing the scope Section 79 and 81 of the Act read with Section 51 of the Indian Copyright Act, 1957. In this case, the intermediary, namely Myspace Inc. was accused of hosting user generated content which infringed the copyright held by the Plaintiff. The Bench held that "...In the case of copyright laws it is sufficient that MySpace receives specific knowledge of the infringing works in the format provided for in its website from the content owner without the necessity of a court order...".
3. Myspace had two important findings concerning intermediary liability in the case of copyright laws:
 - (i) The unlawful acts need not necessarily be relatable to Article 19(2).
 - (ii) A court order is not necessary. The right holder may communicate specific knowledge (clearly identified) of the infringing works to the intermediary in the format provided by the latter, for the content to be removed.
4. The expression "in accordance with sub-rule (6) of Rule 3" does not appear to have any relevance to this provision since Rule 3(6) pertains to Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.
5. The removal of erstwhile Rule 3(4) and the insertion of new proposed Rule 3(8) poses the following issues from an intellectual property perspective:

¹ (2015) 5 SCC 1.

² 2016 SCC OnLine Del 6382.

- (i) The violation of intellectual property rights such as trademarks and copyright does not constitute 'unlawful acts relating to Article 19(2)'. Instances of infringement of IP rights by third parties using an intermediary's platform must be reported to the intermediary. This would be in line with Section 52(1)(b) and (c) of the Copyright Act, 1957 and judicial precedents such as *MySpace* and *Kent RO vs. Amit Kotak*.³
- (ii) This amendment will render holders of such rights helpless insofar as they will no longer be able to approach intermediaries for removal of infringing content. This was also recognized by the Delhi High Court in *MySpace*.
- (iii) While Rule 3(2) specifically mandates a policy requiring users to not to violate third party intellectual property rights, this Rule is rendered nugatory and toothless by virtue of removal of erstwhile Rule 3(4). The new proposed Rule 3(8) does not consider or refer to Rule 3(2).
- (iv) Even if an intermediary is supplied with a court order calling upon it to remove access, it may not be in a position to determine whether the access is in fact to unlawful acts relating to Article 19(2). The Supreme Court's concern in *Shreya Singhal* was that an intermediary is not qualified or empowered to conduct such exercises. The proposed amendment, however, will require intermediaries to exercise their own discretion and interpret court orders to determine if they are relating to Article 19(2). Therefore, the onus ought to be on the Courts to ensure that the restraint on speech is balanced and is relating to Article 19(2) of the Constitution.
- (v) The threshold of Article 19(2) must be considered in the context of rights available under specific statutes such as those under Trademarks Act, 1999 and Copyright Act, 1957. Therefore, a balance must be achieved as has been done through Section 52(1)(b) and 52(1)(c) read with Rules 75 and 76 of the Copyright Rules, 2013.
- (vi) The 24-hour deadline, from the notification of the court order, to remove or disable access is too short a deadline. Court orders may be in vernacular languages and require translation. The timeline should be changed to "as expeditiously as possible" rather than an inflexible time limit.

I.C. SUGGESTION BY IRA LAW

The Ministry may consider amending the sub-clause in the following manner:

(8) 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 Act shall remove or disable access to that unlawful **content** acts relating to Article 19(2) such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, **as the case may be** on its computer resource without vitiating the evidence in any manner, as far **expeditiously** as possible

³ (2017) 240 DLT 3.

immediately, but in no case later than twenty four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.

II. Comments on proposed Rule 3(5) of The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.

II.A. KEY FEATURES OF THE PROPOSED RULE

- 1. Mandatory nature of the rule:** The term "shall" in proposed Rule 3(5) makes it mandatory for an intermediary to respond to a request for information or assistance made in the prescribed manner by a government agency within the prescribed timeline.
- 2. Information or assistance that an intermediary can be required to provide:** The rule requires an intermediary to provide any information or assistance, as required by lawful order, concerning:
 - a) security of the state or
 - b) cyber security; or
 - c) investigation/ detection/ prosecution/ prevention of offences;
 - d) protective or cyber security and matters connected with or incidental thereto;
 - e) tracing of originator of information on the intermediary's platform.
- 3. Persons entitled to make a request an intermediary for such information:** Any government agency can make such a request based on a lawful order.

II.B. COMMENTS ON THE PROPOSED RULE

- 1. Both the rule presently in force and the proposed rule refer to 'lawful order', which is a subjective term:**

While on the one hand, the Supreme Court has cautioned against requiring an intermediary to judge the legitimacy of takedown requests, this rule refers to the term 'lawful order' which may be subjective. The intermediary should not be burdened with the adjudication of whether an order is "lawful" or not. Instead, the term used ought to be an "order by a government agency authorized to issue such order under a law for the time being in force".

In any event, given the nature and wide ambit of information that an intermediary can be requested to produce under this rule, to balance the interests of individuals with those of the state, we suggest that the requests be pre-screened by a court.

2. The phrase 'protective or cyber security' is superfluous:

The proposed rule refers to 'cyber security' twice. The phrase 'cyber security' used a second time appears to be superfluous. Furthermore, the term 'protective' appears to be misplaced in the proposed rule.

3. The phrase 'matters connected with or incidental thereto' is too broad and vulnerable to abuse:

Government agencies are permitted to collect information and request assistance from an intermediary concerning security of the state or cybersecurity or investigation/ detection/ prosecution/ prevention of offences. Adding 'matters connected with or incidental thereto' significantly broadens the scope of information/ assistance and could be used to collect information/ request assistance for issues not intended to be covered by the rule. This phrase is not at all necessary especially since the term "cyber security" is defined widely under Section 2(nb) of the Act.

4. The addition of the word "electronic means" is a very wide term. This provision should clearly specify the modes of communication to be used for requesting such assistance or information by the government agencies. Practical experience has shown that oftentimes requests are sent by SMS or on personal messaging apps, which creates uncertainty regarding obligation and compliance.

5. While the provision initially uses the term "as asked for by any government agency", the latter part of the sub-rule uses "by government agencies who are legally authorised".

6. The phrase 'tracing of originator of information on the intermediary's platform' will unduly compromise privacy of users if implemented without the safeguards suggested above:

The proposed rule should balance the interests of individuals and the state. Judicial scrutiny is a tool that should be used to achieve this balance. Therefore, requests for information/ assistance under this rule should be made only pursuant to and in compliance with court orders.

Further, tools such as end-to-end-encryption are critical for protecting the privacy and security of individuals and the proposed rule cannot be interpreted or implemented in a manner such that it forces intermediaries to remove end-to-end-encryption all together.

II.C. SUGGESTIONS BY IRA LAW

1. The Ministry may consider amending the term "lawful order" to "order by a government agency authorized to issue such order under a law for the time being in force".

2. **The Ministry may consider removing the phrase “protective or cyber security and matters connected with or incidental thereto”.**
3. **The Ministry may consider the following language for the last sentence of the Proposed Rule 3(5): “The intermediary shall enable tracing out of such originator of information on its platform, as reasonably possible, as may be required by government agencies who are legally authorised.”**

III. Comments on proposed Rule 3(7) of The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

- (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;*
- (ii) have a permanent registered office in India with physical address; and*
- (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.*

III.A. KEY FEATURES OF THE PROPOSED RULE

1. **Applicability:** The rule will apply to all intermediaries who (i) have more than fifty lakh users in India or (ii) are in a list of intermediaries notified by the government of India.
2. **Mandatory nature of the rule:** The use of the term “shall” implies that this rule is likely to be considered a mandatory provision requiring the specified classes of intermediaries to comply with the conjunctive requirements stated in the proposed rule.
3. **Incorporation under the Companies Act, 1956 or Companies Act, 2013:** Intermediaries falling within the specified class as mentioned in the proposed rule must be incorporated in India under the applicable laws.
4. **Physical presence in India:** Intermediaries falling within the specified class as mentioned in the proposed rule must have a permanent, physical registered office in India.
5. **Point of contact in India:** Intermediaries falling within the specified class as mentioned in the proposed rule must appoint a nodal person of contact and alternate senior designated functionary to coordinate and ensure compliance with requests from Indian law enforcement agencies

III.B. COMMENTS ON THE PROPOSED RULE

1. The object behind the introduction of proposed rule appears to be “for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their

orders/requisitions made in accordance with provisions of law or rules.” The comments made to the proposed rule are therefore being made in this backdrop.

2. **Classification of intermediaries under the proposed rule is arbitrary and vague:** The proposed Rule 3(7) specifies two classes of intermediaries (“Specified Intermediaries”) to which the rule will be applicable. The classification of these intermediaries is, however, problematic for the reasons mentioned below:

- a. The first class of intermediaries are those who have more than fifty lakh users in India. At the outset, the classification of intermediaries with over fifty lakh users does not appear to have any evident rationale and therefore appears *prima facie* to be arbitrary. If the rationale is to ensure compliance by intermediaries which see extensive web traffic, the number of users specified in the proposed rule is extremely conservative and may not fulfil the purpose intended. To elucidate, in February 2018, it was estimated there would be 500 million i.e. 50 crore users accessing the internet in India by June 2018.⁴ Thus, given the large number of users of the internet from India and especially given the requirements that such intermediaries would be required to follow under the proposed rule, it would be advisable to increase the number of users of the intermediary.

It is also necessary to mention that if the classification of intermediaries remains to exist in its current form, it would be necessary to include a time period over which the number of the users of the intermediary is calculated for the purposes of the proposed rule.

- b. The second class of intermediaries are those in a notified list of intermediaries notified by the government of India. The proposed rule does not specify under what statute or authority the list of intermediaries will be notified and is therefore, vague. To ensure that no intermediary is taken by surprise, it is necessary that these details are mentioned in the proposed Rule 3(7) to ensure that an intermediary is aware of the basis on which it is required to comply with its requirements.

3. **Proposed Rule 3(7) creates an unreasonable burden on the Specified Intermediaries to be incorporated under Indian laws**

Proposed Rule 3(7) requires Specified Intermediaries to be incorporated under the Indian Companies Act, 1956 or Companies Act, 2013. Generally, the decision of an entity to incorporate is entirely voluntary. Some rare examples of rules or policy which mandate that an entity is incorporated under the Indian laws are the government’s Foreign Direct Investment Policy and the Startup India Scheme. However, even these policies afford such entity the option to register itself as a Limited Liability Partnership. Additionally, there are several other entities which are recognised under the law, such as proprietorships and partnerships.

In any event, the proposed Rule 3(7) fails to fundamentally recognise that a large number of intermediaries are not based in India and could prefer not to do business

⁴ Surabhi Agarwal, *Internet users in India expected to reach 500 million by June: IAMAI*, Economic Times, February 20, 2018, available at <https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms> (last accessed on January 23, 2019).

within the Indian jurisdiction if the legal requirements, including that of incorporation become cumbersome. Therefore, this requirement may act as a trade barrier as other countries may also impose similar conditions on Indian multinational corporations or negatively impact the bilateral trade treaties.

The object of this rule is to ensure that the Specified Intermediary complies with government authorities and is not a fly-by-night operator who avoids performing such an obligation. Given that at least one class of the Specified Intermediaries are assumed to have a certain amount of web traffic, this apprehension may be unwarranted, and the object will be achieved as long as the Specified Intermediary is an entity recognised under extant Indian laws.

4. Ensuring a physical presence in India will be extremely costly for smaller intermediaries and in any case is not required

The requirement for a Specified Intermediary to have a registered office address with a physical address in India is similarly cumbersome and could be viewed as a hurdle for several small intermediaries or foreign intermediaries to conduct business within India.

In an increasingly digital age, where even courts recognise that a virtual presence through a website is enough to characterise such an entity as carrying on business in India⁵ and service of summons through email⁶ and messengers such as Whatsapp⁷ are valid, mandating the Specified Intermediaries to have a permanent registered office and physical presence is archaic and pointless.

5. Appointment of a nodal person of contact and an alternate senior designated functionary for coordination with governmental authorities is unnecessary

While the object of requiring the Specified Intermediaries to name and appoint a person for coordination with law enforcement authorities and officers is valid, it is superfluous to require that such person be appointed and named in addition to the "Grievance Officer" who is also named under Rule 3(12) of the same proposed guidelines.

III.C. SUGGESTIONS BY IRA LAW

A. For the reasons stated hereinabove, it is suggested that if the provision is to be retained, the Specified Intermediaries be more specifically defined to (i) include a higher and more realistic number of users of such intermediaries in view of the increasing internet penetration and usage in India, and (ii) to provide details of the notification in which such intermediaries may be included.

⁵ *World Wrestling Federation vs. Reshma Collection & Ors.*, 2014 (60) PTC 452 [Del] [DB].

⁶ *Central Electricity Regulatory Commission vs. National Hydroelectric Power Corporation Ltd. & Ors.*, (2010) 10 SCC 280.

⁷ *Kross Television India Pvt Ltd & Anr vs. Vikhyat Chitra Production & Ors.*, Order dated March 23, 2017 (G.S. Patel, J.) in Notice Of Motion (L) No. 572 Of 2017 In Suit (L) No. 162 Of 2017 before the High Court of Judicature at Bombay.

B. The first two requirements of the proposed Rule 3(7) enumerated under clauses (i) and (ii) are deleted.

C. The requirement of the nodal person of contact and alternate senior designated functionary be deleted and the Grievance Officer envisaged under Rule 3(12) be additionally entrusted with the responsibility of coordination with governmental authorities.

IV. Comments on proposed Rule 3(9) of The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.

IV.A. KEY FEATURES OF THE PROPOSED RULE

- 1. Mandatory nature of the rule:** The use of the term "shall" implies that this rule is likely to be considered a mandatory provision requiring the intermediary to deploy such technology based automated tools or appropriate mechanisms.
- 2. Nature of the technological tool/ mechanism:** The technological tool must proactively identify and remove/ disable public access to the information/content.
- 3. Scope of content to be identified and removed:** The rule requires removal of all "unlawful" content, which would imply that the technological tool must identify and detect content which violates any law for the time being in force. While the number of laws which have an impact on legality of online content are many, this would illustratively include content which is defamatory, obscene, infringes copyright, trademarks, designs, patents etc..

IV.B. COMMENTS ON THE PROPOSED RULE

- 1. The proposed rule creates an obligation which is in violation of the Supreme Court's mandate in *Shreya Singhal*:**

The proposed Rule 3(9) puts the onus on intermediaries to deploy technological tools to proactively identify and remove information/ content which is "unlawful". The intermediary would, therefore, be required to develop tools which would identify and thereafter remove any offending information/content, and effectively adjudicate on whether the information/content is unlawful.

The Supreme Court in *Shreya Singhal* specifically cautioned against the perils of requiring an intermediary to judge the legitimacy of takedown requests. It is for this reason that the Supreme Court mandated that the takedown requests must be supported by a "court order", so that intermediaries are not required to perform an adjudicatory function.

Thus, the proposed Rule 3(9) would go against the letter and spirit of the Supreme Court's mandate in *Shreya Singhal*.

2. Currently available technological tools are inapposite for identifying and removing unlawful content

A. Content interpretation is subjective, contextual and therefore, complex:

The same content may be interpreted and understood differently depending on the individual. For instance, a joke may be offensive to the subject of the joke but acceptable and even entertaining to others. Similarly, while content may *prima facie* appear defamatory, it may be truthful or a fair comment and thus be permitted under the law. While unlicensed use of copyrighted content may *prima facie* appear unlawful, such use may be protected under the doctrine of fair dealing under the Copyright Act, 1957.

Similarly, content is often contextual, and the unlawful nature of content will often depend on the context in which it appears. This has been categorically recognized by the Supreme Court in *Aveek Sarkar v State of West Bengal*.⁸ The Court, in that case, held as under:

"We have to examine the question of obscenity in the context in which the photograph appears and the message it wants to convey. In Bobby Art International & Ors. v. Om Pal Singh Hoon (1996) 4 SCC 1, this Court while dealing with the question of obscenity in the context of film called Bandit Queen pointed out that the so-called objectionable scenes in the film have to be considered in the context of the message that the film was seeking to transmit in respect of social menace of torture and violence against a helpless female child which transformed her into a dreaded dacoit...."

We have to examine whether the photograph of Boris Becker with his fiancée Barbara Fultus, a dark-skinned lady standing close to each other bare bodied but covering the breast of his fiancée with his hands can be stated to be objectionable in the sense it violates Section 292 IPC. Breast of Barbara Fultus has been fully covered with the arm of Boris Becker, a photograph, of course, semi-nude, but taken by none other than the father of Barbara.

We should, therefore, appreciate the photograph and the article in the light of the message it wants to convey, that is to eradicate the evil of racism and apartheid in the society and to promote love and marriage between white skinned man and a black skinned woman. When viewed in that angle, we are not prepared to say that the picture or the article which was reproduced by Sports World and the Anandabazar Patrika be said to be objectionable so as to initiate proceedings under Section 292 IPC or under Section 4 of the Indecent Representation of Women (Prohibition) Act, 1986."

It is instructive that the court considered the fact that the photograph in question was clicked by the father of the subject. The above case illustrates that content has to be viewed in the context in order to determine its legality.

The subjectivity and contextuality of content interpretation pose serious restrictions on the ability of artificial intelligence to identify "unlawful content". Doctrines surrounding the legality of content are complex, require human

⁸ (2014) 4 SCC 257.

intervention and are best applied by trained judges. Currently available technological measures for content filtering cannot detect its context and the message it wants to convey in the manner in which human cognition permits.

B. Proposed Rule 3(9) fails to appreciate that accurate algorithms for detection of unlawful content do not exist

Even the most sophisticated technological tools available today such as content fingerprinting are imperfect, inaccurate and often show false positives⁹ (i.e. content which the technological tool finds to be unlawful but is in fact legal under the applicable law). The use of these blunt tools for content filtering and removal will have a serious chilling effect on free speech, a consequence that the Supreme Court in *Shreya Singhal* cautioned against.

Some of the existing tools use fingerprinting technology which compares the allegedly unlawful content with pre-existing content. For instance, to determine copyright infringement, content uploaded by a user can be compared with a database of copyrighted content and technologies, albeit inaccurate, still exist. However, in contrast, building detection algorithms for determining the legality of content with no comparators is extremely onerous and difficult.

3. Requiring intermediaries to proactively identify unlawful content will compromise data encryption

One of the cornerstones of modern digital communication is end-to-end data encryption which ensures that users can securely and privately communicate with each other, without their content being reviewed by the intermediary or any third party. If intermediaries are to proactively identify unlawful content, they will no longer be able to provide end to end encryption services to users, which would severely compromise the security and privacy of the user's data.

4. Proposed Rule 3(9) creates an obligation to not only proactively identify but also to remove the content

Proposed Rule 3(9) requires intermediaries to not only proactively identify but also to remove the content. The rule does not envisage any interaction or cooperation with the user or owner of the information and there would not be any opportunity for such user/ owner to provide any response or justification in support of the legality of the content. This is in sharp contrast to notice and takedown procedures, which often allow users an opportunity to contest a claim that the content is unlawful.

Even the Copyright Act, 1957, requires a copyright holder or its licensee to report instances of infringement after which the intermediary is required to take down the content and the copyright holder or its licensee is required to obtain a court order within 21 days. So, a parallel legislation such as the Copyright Act, also lays down a notice and take down regime. The legislative intent and judicial precedents are, therefore, in favour of a 'notice and take down regime' rather than a proactive monitoring one.

⁹ Engstrom and Feamster, *The Limits of Filtering: A Look at the functionality and Shortcomings of Content Detection Tools*, March 2017

Further, the proposed amendment changes the nature of the intermediaries by transforming them into censorship bodies rather than the government, which is contrary to the principles laid down by Supreme Court in "*Shreya Singhal*".

5. **Technological tools will be extremely costly for smaller intermediaries**

Google Inc., to monitor copyright infringement, introduced the Content ID programme on the YouTube platform which enabled right-holders to identify user-uploaded videos that are entirely or partially their content, and choose, in advance, what they want to happen when those videos are found. This was a voluntary effort by Google to develop and monitor copyright infringement for which it spent US\$ 100 million for developing its Content ID tool (till the year 2018)¹⁰.

However, smaller intermediaries are unlikely to have the bandwidth or resources to develop and deploy such tools. Therefore, making deployment of such tools mandatory for availing the safe harbour under Section 79 of the Act would render it practically impossible for smaller intermediaries to enter the market and would in fact reduce competition.

Further, search engines currently only crawl websites for the purposes of indexing; however, for deploying detection technologies, search engines may have to download the content for the purposes of identifying unlawful content which would exponentially increase the cost of indexing the content on the internet.

6. **Rule 3(9) will create an uncertain/ subjective standard for availing the safe harbour**

The proposed Rule 3(9) does not provide any standard as to sophistication of technological tools that would need to be deployed in order to be compliant with this rule. This is particularly problematic since the failure to deploy such tools could lead to the intermediary losing the safe harbour protection available under Section 79(1) of the Act. This would lead companies to expend inordinate resources in the deployment of these tools. This, in turn, would create a chilling effect on competition in this space since companies which don't have these resources will exit the market and will also pose a significant barrier to entry for new entrants.

7. **Different countries have very different definitions of unlawful content**

The difficulty in developing and deploying technological tools is further exacerbated by the fact that different countries have different definitions of unlawful content. This would thus require intermediaries to customize the tools for each jurisdiction and further add to the already prohibitive cost of developing these tools.

8. **The expression "appropriate controls" is vague**

The proposed Rule 3(9) uses the term "appropriate controls" which is a vague expression and it is not clear from the rule as to the nature and extent of the controls that is being referred to in the rule.

¹⁰ Cedric Manara, *Protecting what we love about the internet: our efforts to stop online piracy*, November 7, 2018, available at <https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/> (last accessed on January 23, 2019).

IV.C. SUGGESTIONS BY IRA LAW

- A. For the reasons elaborated hereinabove, the Ministry of Electronics and Information Technology may consider deletion of this sub-rule.**
- B. Alternatively, the Ministry may consider making the deployment of technological tools voluntary rather than mandatory by replacing the word “shall” with “may”.**

While this would encourage intermediaries to adopt technological tools when possible and as and when they are available, it will not make the availability of the safe harbour under Section 79 dependent on the deployment of these tools.

- C. The Ministry may also consider clarifying the scope of the term “appropriate controls” appearing in this rule.**

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
(Published by MeitY)

**RELIANCE JIO INFOCOMM LTD'S COMMENTS ON "INFORMATION
TECHNOLOGY [INTERMEDIARY GUIDELINES (AMENDMENT) RULES] 2018
DATED 24th DECEMBER 2018"**

General Comments:

1. At the outset, Reliance Jio Infocomm Limited (RJIL) welcomes the Government's initiative to introduce the amendment in the information technology [intermediary guidelines rules 2018 to bring in important players in the digital communication space under the ambit of the prevailing legal oversight.
2. Information Technology Act 2000 ("Act") elaborates on the exemption from liabilities of intermediaries in certain cases (Section 79); although they must observe due diligence while discharging their duties and also observe such other guidelines as prescribed by the Central Government.
3. Accordingly, the Information Technology (Intermediaries Guidelines) Rules, 2011 ("Rules") were notified in April 2011. However, the Rules lacked the required impetus to ensure that social media and mobile apps are not misused by users to threaten national security and user privacy.
4. Further, the Rules, left the intermediaries providing the digital service out of its ambit, so much so that the Rules did not even mandate such firms to assist/cooperate with law enforcement agencies in an effective manner. The proposed Information technology [Intermediary Guidelines (Amendment) Rules] 2018 ("Amendment") bolster the existing Rules to ensure right use of such platforms in digitally empowering the nation in a secure manner.
5. RJIL submits that with increase in penetration of high speed internet, social media platforms and mobile apps ("Platforms") have seen an unprecedented growth in last few years in India. While, this growth of platforms has helped expand digital footprint in the country but there has also been a rampant increase in misuse of these technologies for committing cybercrimes. Such misuse of the technology/platform is aggrieved by the seamless nature of internet. Users can open accounts in any name including fake name from any part of the world owing to insufficient background information check done by such Platforms.
6. There have been multiple cases in recent past in India where the social media and mobile chat apps have been misused for wide circulation of rumors or fake news to incite violence in society leading to death of innocent citizens; eg: mob lynching incidents reported in various parts of countries.



7. Upon being pushed by Government, such Platforms have taken limited steps like curbing the number of forwards and indicating that the incoming message is forward, however these steps are still not sufficient to prevent misuse of the technology.
8. Additionally, the fact that many of popular Platforms are owned by foreign entities and the servers of such foreign Platform operators are mostly located abroad, makes it further difficult for the Indian law enforcement agencies to get the required information/assistance in a time bound manner in case of violation of any provision under the IT Act and associated Rules.
9. We submit that the Platform companies must be instructed to implement appropriate additional remedial measures and be advised to implement security framework that will help to assist the law enforcement agencies in curtailing any misuse of such technology. Such measures should include:
 - a. Extend active assistance/cooperation to law enforcement agencies.
 - b. Tracing the origin of such fake news/rumors and assisting the law enforcement agencies to identify the same.
 - c. Technical solutions to identify harmful messages on their platforms and notify the same to law enforcement agencies.
 - d. Incorporation of large foreign Platform companies under Indian laws and appointment of nodal officer to coordinate with law enforcement agencies, to bring such companies under effective reach of Indian regulations.
10. **In view of the above, we believe that the proposed Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 take significant steps to amend and rectify the current prevalent misuse of the Platforms.**
11. As you are aware, any proposal mandating the Platform service providers to provide required information/assistance to law enforcement agencies is often protested on grounds of violation of freedom of speech and expression as provided in the Constitution. However, we submit that such protests are without any basis and the Government must ignore the same and address the emergent need to prevent reckless abuse of such technologies and Platforms.
12. RJIL firmly believes that there is a need to strike balance between freedom of speech & expression and the obligation to be responsible & accountable, so that the Platforms do not become conduit for unlawful activities like incite hatred, provoke terrorism, extremism, etc.



Key issue wise response:

I. Provide information/assistance to law enforcement agencies

1. Refer Clause 5 and Clause 8 of the Amendment
2. Intermediaries should be mandated to cooperate/assist law enforcement agencies in maintaining law and order in the country. Such information request can be with respect to security of nation, cyber security, investigation/detection/prosecution/prevention of an offence and maintaining law & order/peace in any part of country.
3. We support the proposal of mandating an intermediary to provide the required information/assistance to identified Government agencies in a time bound manner (72 hours in this case). In addition, we propose that that such request from the Government may be expedited and responded within 36 hours in specific cases depending on the criticality of the requested information and associated national threat/risk in question.

Explanation: Information request may be divided into critical and non-critical. If Government perceives the risk/threat to be grave for national security, it may request the intermediary to respond within 36 hours. For other concerns, it may continue with proposed time line of 72 hours.

4. Similarly, intermediaries should be mandated to remove or disable access to any unlawful content on its platform within a limited time (latest 24 hours in proposed amendment), on receiving actual intimation in form of court order or being notified by Government agencies.
5. Although we recommend that to avoid any possibility of abuse of proposed provision in Clause 5 of the Amendment, the information or assistance request should be done only by lawfully authorized or duly designated government agencies instead of current proposed "any government agency" (refer clause 5).

II. Track the originator of fake news/rumors

1. Refer clause 5 of the Amendment
2. Fake news and rumors often threaten the peace, harmony and social fabric of country. Hence it is imperative that originators of such misleading information be identified and held accountable.



3. At present, many OTT players employ end to end encryption of information under the guise of providing better security to their users. But such features, although perceivably beneficial to users, are detrimental to national interest and hence should not be allowed. It is imperative to have an optimum balance between the two.
4. We strongly recommend that the intermediary should enable tracing out of originator of such information on its platform, which will help Government agencies identify the originator of such misleading information and hold them accountable in order to maintain cyber security, required for national security and prevention of offence.
5. Upon information request by the law enforcement agencies, intermediaries should be mandated to provide the Traffic Data (as defined in the Act) of the originator.
6. Such obligations are already mandatory for Telecom Service Providers (TSP), which are also part of intermediaries as per IT Act 2000. Hence it is natural and advisable, for national interest, that similar obligations must be imposed on other intermediaries having a similar functional role of communication provider.

III. **Use of technology by Platform players to combat fake news**

1. Refer clause 9 of the Amendment
2. Any company/entity operating social media platforms in the country is an important stakeholder in the digital communication space in the country and therefore it cannot evade its responsibility, accountability and larger commitment to ensure that its platform is not misused on a large scale to spread fake news designed to instigate people to commit crime. If they do not take adequate and prompt action, then the law of abetment of offences should be applicable to them.
3. Platform operators should provide for technological solutions so that any news source that may be notified by the Government agencies as being violative of the proposed Rule 3 (2) can be filtered by technical solutions and any similar such news being circulated based on tag words notified by such Government agencies in the course of the above action is then proactively reported to such governmental agency for determining action. They should also seek to provide the facility of verifying fake news on the platform itself.

We suggest that the criterion for classification of the content and action for filtering or removal should not be left to the discretion of the Platform service provider and any proactive removal or disabling public access by intermediaries should not be permitted. This will ensure that such filtering of unlawful content will not affect the neutrality that intermediaries are required to ensure in transmission of information and also will not interfere with the freedom of expression of the user, especially when (i) such filtering and/or removal through automated processes may lead to idiomatic



or inadvertent filtering or takedown of content with entirely different connotation or context; and (ii) other filtering processes involve platform service providers reviewing, intruding or censoring communications and transmitted content. Hence we recommend that the Government should elaborate and establish the specific guidelines for classification of content posted by users on such Platforms as being violative of Rule 3 (2), the notification mechanism requiring platforms to filter such news, including review of proactive reporting by intermediaries of similar news containing tag words notified by such government agencies.

4. We suggest that this provision requiring automated tools should be applicable only for Platform service providers having a minimum threshold user base, which can be defined by the Government. This will ensure that growth of small or startup companies is not thwarted by burden of cost of developing such AI solutions.

IV. Extend the reach of law enforcement agencies

1. Refer clause 7 of the Amendment
2. We support the provision that any intermediary with more than 50 lakh users in India should be registered and incorporated under Companies Act 1956. This would ensure that the law enforcement agencies can implement the Indian laws effectively and can hold the foreign firm accountable in case of violation of any clause of the Act.
3. Many of the social platforms or e-commerce firms operate and service Indian users without having any significant presence in India owing to seamless nature of internet. There have been numerous cases in the past when the Indian law enforcement agencies have been rendered ineffective as the concerned firm is a foreign firm with almost no presence in India. Having a nodal officer for coordination with enforcement agencies will help in compliance with orders/requisitions made by such agencies.

IV. Have similar regulations related to national security for all communication providers

1. Today an internet user can communicate or broadcast his/her views to select recipients or all users in general using various mediums like social media, messages and chat services and web sites with option to upload inputs, beside the traditional voice calls. Hence Platforms and telecom services have functionally become substitutable, to a large extent, for communication purpose from user perspective.
2. It is important that regulations related to national interest and security are applicable uniformly across all such mediums and no discrimination should be made on account of ownership of infrastructure, network layer on which the medium is operating, etc.



3. TSPs have various obligations, under the license agreement with Department of Telecom, which ensures protection of national security, cooperation with law enforcement agencies and maintaining user privacy. Few prominent such regulations include following:
- Setting up Lawful Interception and Monitoring (LIM) systems
 - Restriction on sending user information abroad
 - Gives the Licensor the right to inspect the sites/network used for extending the service
 - Providing necessary facilities for continuous monitoring of the system, not employing any bulk encryption equipment; taking prior evaluation and approval of Licensor for any encryption equipment for specific requirements
 - Responsibility for ensuring the protection of privacy of communication and confidentiality of subscriber information.
4. But Platform service providers don't have similar obligations on them. They are currently exempted from ownership of any content on their platform if they are following reasonable security practices. Also in practice they are not mandated to maintain sufficient processes to ensure effective assistance/cooperation with law enforcement agencies.
5. As a result, often these Platforms are used by miscreants as channels for spreading fake news/rumors which can disturb peace and harmony or be threat to national security. Hence it is imperative that law enforcement agencies should have control over such mediums to ensure that originator of such information can be held accountable and national interest can be secured.
6. IT Act appropriately captures the gamut of players and mediums which enable a user to communicate information to the recipient in its definition of intermediary. The definition (as per IT Act) is reproduced below for quick reference:
- "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.*
7. Hence we recommend that to promote the intent and the spirit of the Act, similar regulations related to national security which are applicable on TSPs should be applicable for Platform service providers.
8. But at the same time, we recommend that the above provisions should be considered in adjunction with the license obligations for TSPs and it should be ensured that the TSPs should not be burdened to duplicate their efforts in fulfilling their obligations



under Unified License as well as IT Act and associated Rules, whether in keeping records or providing facilities to LIM authorities. This is required to ensure that there is not further increase in obligations for the already burdened TSP.

Other issues

1. We recommend that the proposed change in clause 4 of the Amendment be done away with as the provision creates an onerous burden on intermediaries without any corresponding public benefit. It may also lead to case of user fatigue.
2. The above referred clause is reproduced below for your reference:

“The Intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information”.

3. We recommend that the proposed provision of storing the required information in clause 9 may not be increased beyond the current 90 days to 180 days as it increases the burden on the intermediary without any corresponding benefit. Although we agree that such period may be extended as may be required by the court or by government agencies who are lawfully authorized to do so.





CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA (MEITY) ON THE DRAFT INFORMATION TECHNOLOGY [INTERMEDIARY GUIDELINES (AMENDMENT) RULES], 2018¹

INTRODUCTION

We appreciate the government's concern regarding the misuse of social media, the resultant harm, and the challenges that it has brought for the law enforcement Agencies (LEA)². We support the need to consider various efforts to make the Internet a safer space, and also to update the laws governing cyberspace in order to bring them in consonance with the technological advances, and global best practices, and to deal with illegal speech online.

However, the draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 (*Draft Rules*) if passed in the current form will not achieve their intended outcomes. The draft rules violate the fundamental rights to freedom of speech and expression, and privacy of Indian citizens as enshrined in the Constitution of India,³ to which this government has declared its commitment⁴.

¹ Authored by **Sarvjeet Singh** with assistance from **Yesha Tshering Paul** and inputs from **Shrutanjaya Bhardwaj**, **Smitha Krishna Prasad** and **Ujwala Uppaluri**.

² Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>, ¶ 4.

³ See Chinmayi Arun, *The 'Purdah' amendment: Proposed changes to the IT Act could draw a veil over the Indian internet*, SCROLL (Jan. 24, 2019), <https://scroll.in/article/910601/the-purdah-amendment-proposed-changes-to-the-it-act-could-draw-a-veil-over-the-indian-internet>.

The draft rules, if enacted will privatize censorship, which has thus far been a power of the state, discharged primarily by the executive arm and subject to review for compatibility with constitutional bounds by the judiciary. Privatizing this power has an adverse effect on our core fundamental rights. Moreover, the censorship of the degree envisaged by Rule 3(2) read with Rule 3(9) of the draft rules will effectively guarantee unchecked surveillance and will violate the fundamental right to privacy.

As per the press note released with the draft rules, the object of the proposed amendment appears to tackle the menace of fake news/ misinformation and the circulation of obscene content,⁵ and to make the social media platforms accountable under the law.⁶ However, the proposed rules apply to all intermediaries⁷ irrespective of their specific role or nature⁸.

“Intermediaries” according to the Information Technology Act, 2000 (IT Act) with respect to any particular electronic records is defined as:

*any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes.*⁹

The amended definition of “intermediaries” after the 2008 amendment of the IT Act was hailed by some for its clear definition and extensive scope, expanding the type of entities that can claim safe harbor protection.¹⁰ However, others have

⁴ Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>, ¶ 3.

⁵ Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>, ¶ 4.

⁶ Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>, ¶ 5.

⁷ The Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018, r. 2(k).

⁸ See Chinmayi Arun and Sarjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASES STUDIES 67 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

⁹ The Information Technology Act, 2000, s. 2(1)(w).

¹⁰ Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).

criticized it for failing to make allowances for functional differences between various intermediaries.¹¹

The scope of this clause is extremely wide and includes everything ranging from social media services and communication platforms to ride hailing applications and cyber cafes. Moreover, this is not an exhaustive list and may include services not mentioned in the section.

In case of the draft rules there is no nexus between the object of the amendments¹² and the actual regulations in case of most of the entities which fall under the definition of intermediaries. For these entities, the obligations under the proposed amendment seem “entirely misplaced and inapplicable”.¹³ It is necessary for MeitY to identify the relevant intermediaries, based on reasoned and valid categorization, which have a nexus to the concerns that are sought to be remedied, and draft appropriate regulations (if permissible)¹⁴ for such intermediaries.

PROBLEM OF EXCESSIVE DELEGATION

According to the doctrine of excessive delegation, delegation of essential legislative functions by a legislature to any other authority is unconstitutional.¹⁵ The power to make changes in policy is an essential function and cannot be delegated.

¹¹ Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

¹² Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>, ¶¶ 4-5.

¹³ Amba Kak, *Move fast and break things: Government's new rules on internet regulation could kill innovation and privacy*, TIMES OF INDIA (Jan. 4, 2019), <https://timesofindia.indiatimes.com/blogs/toi-edit-page/move-fast-and-break-things-governments-new-rules-on-internet-regulation-could-kill-innovation-and-privacy/>.

¹⁴ While the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 were promulgated on April 11, 2011, on a bare reading of Sections 79 and 87(2)(zg) of the Information Technology Act, 2000 it is not apparent that the Act provides the government authority to make such distinctions between intermediaries. Section 79(2)(c) of the Information Technology Act, 2000 does state that “the intermediary observes...[and] also observes such other guidelines as the Central Government may prescribe in this behalf.” However, a bare perusal of the act, it probably means that such guidelines (in addition to the due diligence requirement) apply to any and all intermediaries. Moreover, unlike cyber-cafe, it will be very problematic to define a set of intermediaries (without it being over or under inclusive).

¹⁵ See *In Re Delhi Laws Act*, (1951) S.C.J. 527; *Harakchand v. India*, (1970) 1 S.C.J. 479. See also STANDING COMMITTEE ON SUBORDINATE LEGISLATION, PRACTICE & PROCEDURE-ABSTRACT SERIES (Feb. 2005), available at https://rajyasabha.nic.in/rsnew/practice_procedure/book13.asp.

The legislature is the master of legislative policy and if the delegate is free to switch policy it will lead to usurpation of legislative power itself.¹⁶

The authority which is the delegate is not allowed to widen or reduce the scope of the Act, and cannot legislate in the garb of making rules.¹⁷ Moreover, delegated legislation should conform to the parent statute and cannot exceed the scope of enabling act.¹⁸

While determining a case of excessive delegation a court should take into account the subject-matter and the scheme of the statute, the provisions of the statute including its Preamble and the facts and circumstances and the background on which the statute is enacted.¹⁹

It is also a settled principle that the rule making power cannot be sub-delegated by the executive, unless such power is clearly granted by the enabling act. Such sub-delegation without being expressly granted by the parent act will be void.²⁰

Many rules of the proposed guidelines fall outside the permissible limit of the enabling statute, which is the IT Act. These include Rules 3(5) and 3(7), and specific issues with these rules have been discussed below.

SPECIFIC CLAUSES

RULES 3(1) AND 3(2)

One of the conditions to receive immunity under Section 79 of the IT Act is the observance of due diligence by the intermediary.²¹ The current due diligence

¹⁶ *Avinder Singh v. Punjab*, (1979) 1 S.C.C. 137.

¹⁷ *Agriculture Market Committee v. Shalimar Chemical Works Ltd.*, (1977) 5 S.C.C. 516.

¹⁸ See *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C. 641; *State of Karnatak v. Ganesh Kamath*, (1983) 2 S.C.C. 40. See also Ujjwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011* (July 16, 2012), <https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules>.

¹⁹ *K.T. Plantation Pvt. Ltd. v. State of Karnataka*, (2011) 9 S.C.C. 1.

²⁰ See *India v. M/s Bhanamal Gulzarimal*, A.I.R. (1960) S.C. 475; *Bhagwati Saran v. Uttar Pradesh*, A.I.R. (1961) S.C. 928.

²¹ For a detailed discussion of the various requirements for an intermediary to claim immunity under Section 79, Information Technology Act, 2000, see Chinmayi Arun and Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF

requirements were introduced by the government in the intermediary guidelines which were notified by the Central Government on April 11, 2011, in exercise of the powers conferred by Section 87(2)(zg) read with section 79(2) of the Act.

Under the proposed guidelines rule 3(1) require intermediaries to publish rules and regulations, privacy policies, and user agreements. Subsequently, Rule 3(2) require intermediaries to inform users to not make available or circulate a range on content provided in Rules 3(2)(a) to 3(2)(j). While the draft rules add Rules 3(2)(j) and (k), we believe that most of the provisions under Rule 3(2) should be removed from the guidelines, especially after the *Shreya Singhal* judgment.

The constitutionality of Rule 3(2) was challenged in the *Shreya Singhal* case.²² This has been cursorily noted in the judgment, but there is no substantive discussion on the same and the conclusion refers only to Rule 3(4). Any future challenge to these rules will be upheld based on the principles laid down in *Shreya Singhal* and discussed below.

▫ **BEYOND THE REMIT OF ARTICLE 19(2)**

The *Shreya Singhal* judgment categorically states that Section 79 and by implication the guidelines framed under it cannot be used to regulate unlawful acts which are not relatable to Article 19(2) of the Constitution.²³ This builds on the Court's reasoning by a five-judge constitution bench which held that any limitation on Article 19(1)(a) which does not fall within the purview of Article 19(2) cannot be upheld.²⁴

In the draft rules, as well as the existing guidelines, numerous grounds under Rule 3(2) are not even legal standards, but merely subjective terms with no constitutional basis.

NATIONAL CASES STUDIES 71-74 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

²² *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 119.

²³ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 122 and 124.3.

²⁴ *Express Newspaper (Private) Ltd. v. Union of India*, (1959) S.C.R. 12.

Apart from Rules 3(2) (e), (i), and the terms “defamatory”, “obscene”, “pornographic”, and “pedophilic” under Rule 3(2)(b), and in certain contexts Rule 3(2)(c), and arguably Rule 3(2)(k) and part of Rule 3(j) pertaining to “threatens public health or safety”, none of the other grounds are cognizable under Article 19(2).²⁵ However, even certain terms which may fall within the ambit of Article 19(2), as used in the proposed rules are vague and overboard.

▫ **VAGUE AND OVERBROAD TERMS**

The Supreme Court has repeatedly held that vague provisions must be struck down as being arbitrary and unreasonable.²⁶ Many of the terms listed under Rule 3(2) are subjective and not defined either in the current version of the proposed rules or the IT Act itself. These include terms like “grossly harmful”, “harassing”, “blasphemous”, “hateful”, “racially”, “ethnically objectionable”, “invasive of another’s privacy”, “disparaging”, “harms minors in any way”, “grossly offensive”, “menacing” and “insulting any other nation”.

Many of these terms were declared vague by the Supreme Court in *Shreya Singhal*.²⁷ Majority of the remaining terms are nebulous in nature²⁸ and provide no opportunity to know what is prohibited.²⁹ The *Committee on Subordinate Legislation* as far back as 2013 stated that these terms are ambiguous and asked MeitY to incorporate the definition of all these terms within the guidelines itself, and also ensure that no new category of offences are created by these guidelines.³⁰

²⁵ See Ujwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011* (July 16, 2012), <https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules>.

²⁶ *State of Madhya Pradesh v. Baldeo Prasad*, (1961) 1 S.C.R. 970; *A.K. Roy & Ors. v. Union of India & Ors.*, (1982) 2 S.C.R. 272; See *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 67-79.

²⁷ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 85.

²⁸ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 79.

²⁹ *Kartar Singh v. State of Punjab*, (1994) 3 S.C.C. 569, ¶¶ 130-131.

³⁰ STANDING COMMITTEE ON SUBORDINATE LEGISLATION, THIRTY FIRST REPORT ON THE INFORMATION TECHNOLOGY RULES (March 21, 2013), ¶ 25-26, available at <http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf>.

Some terms under Rule (2) arguably fall within the scope of Article 19(2) including terms from Rule 3(2)(b) - “defamatory”³¹, “obscene”³², “pornographic”³³, and “pedophilic”³⁴, Rule 3(2)(i) – “threatens the integrity, defense, security or sovereignty and of India”³⁵, “friendly relations with foreign states”³⁶, “public order”³⁷, “incitement to commission of any cognizable offence”³⁸, Rule 3(2)(j) – “threatens public health”³⁹ and “safety”⁴⁰ and Rule 3(2)(k) – “threatens critical information infrastructure”⁴¹. However, since these terms have been lifted from Article 19(2) of the Constitution, the body making the determination of whether a piece of content falls within the purview of Article 19(2), has to follow the judicial interpretation and the legal jurisprudence which has developed and provides the scope of these grounds.

For example, for a piece of content to be a threat to public safety, it must meet the public order standard⁴² and a threat to critical information infrastructure must meet the very high threshold of the security of state standard.

³¹ Will fall under the “defamation” ground, the Constitution of India, 1950, art. 19(2).

³² Will fall under the “decency or morality” ground, the Constitution of India, 1950, art. 19(2).

³³ Will fall under the “decency or morality” ground, the Constitution of India, 1950, art. 19(2).

³⁴ Will fall under the “decency or morality” ground, the Constitution of India, 1950, art. 19(2).

³⁵ Will fall under the “interests of the sovereignty and integrity of India” and “the security of the State” grounds, the Constitution of India, 1950, art. 19(2).

³⁶ Will fall under the “friendly relations with foreign States” ground, the Constitution of India, 1950, art. 19(2).

³⁷ Will fall under the “public order” ground, the Constitution of India, 1950, art. 19(2).

³⁸ Will fall under the “incitement to an offence” ground, the Constitution of India, 1950, art. 19(2).

³⁹ Will arguably fall under the “public order” ground, the Constitution of India, 1950, art. 19(2). See *Romesh Thappar v. State of Madras*, (1950) S.C.R. 594. However, according to the Supreme Court in *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶ 45, “Public order is not the same thing as public safety and hence no restrictions can be placed on the right to freedom of speech and expression on the ground that public safety is endangered”.

⁴⁰ Will arguably fall under the “public order” ground, the Constitution of India, 1950, art. 19(2). See *Romesh Thappar v. State of Madras*, (1950) S.C.R. 594. However, according to the Supreme Court in *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶ 45, “Public order is not the same thing as public safety and hence no restrictions can be placed on the right to freedom of speech and expression on the ground that public safety is endangered”.

⁴¹ Will fall under the “the security of the State” or presumably “public order” grounds, the Constitution of India, 1950, art. 19(2).

⁴² See CHINMAYI ARUN, ARPITA BISWAS AND PARUL SHARMA, HATE SPEECH LAWS IN INDIA 14-16 (2018); Sarveet Singh, Parul Sharma and Kritika Bhardwaj, *Public Order, Hate Speech and the Indian*

The constraint on promotion of cigarettes, tobacco products, consumption of alcohol and electronic nicotine delivery system (ENDS) is also vague and overbroad⁴³, since promotion is not defined.

Rule 3(2) in the present form regulates protected speech and because of its overbreadth has a chilling effect on the freedom of expression.

RULE 3(4)

Under rule 3(4) an intermediary is obligated to inform all its users “at least once every month” that noncompliance with rules and regulations and other agreements and policies may lead to termination of services being provided by the intermediary.

The proposed provision is paternalistic and will lead to notice/ consent fatigue. However, there is no apparent violation of users’ fundamental rights.

The draft rule lumps all intermediaries together, while possibly being aimed at intermediaries where the users have to register or sign-up or actively generate or communicate content.

The provision does not define what a “user” is in this context. It will be technically unfeasible for a large number of intermediaries to undertake this task. For instance, users may not regularly use services such as search engines (when not signed in), cyber-cafes or provide any contact information to the service provider, creating a situation where it is difficult to effectively communicate these terms to the user in a regular manner, or identify how often each user has been informed of the terms and record actual implementation of the rule.

Constitution, XXXV (4) Common Cause India Journal 5-11 (2016). However, according to the Supreme Court in *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶ 45, “Public order is not the same thing as public safety and hence no restrictions can be placed on the right to freedom of speech and expression on the ground that public safety is endangered”.

⁴³ See Yesha Tshering Paul, *Fake News: Misguided Policymaking To Counter Misinformation*, BLOOMBERGQUINT (Jan. 14, 2019), <https://www.bloombergquint.com/opinion/fake-news-misguided-policymaking-to-counter-misinformation>.

Moreover, if the owner of the intermediary is an Indian citizen, she can raise a potential claim (albeit a bit weak) of violation of Article 19(1)(g) of the Constitution.

RULE 3(5)

Rule 3(5) require intermediaries to provide assistance or information concerning state security to a government agency within a period of 72 hours of being asked by such agency. The rule also requires them to provide traceability of the originator⁴⁴ of certain information.

This rule is a substantive amendment of Rule 3(2)(7) of the existing guidelines. The current rule provides that only a lawfully authorized government agency can ask an intermediary for certain information or assistance. However, the proposed rule expands the nature of agencies to “any government agency”. Any agency will include among others any ministry, department, commission, board, authority, municipal and other local authority, and statutory body.

The proposed language provides unbridled power to thousands of government agencies to request information and assistance from the intermediary. This will be violative of the right to privacy. The rule should retain the language from the current guidelines and allow only lawfully authorized government agencies to seek such information and assistance.

There is also a need to define/ clarify as to what is meant by lawful order in this instance. Unlike Sections 69 and 69B of the Act and rules framed under those sections⁴⁵, there are no safeguards provided in the instant case. Without any safeguards, the proposed rule and even the existing rule will fall foul of the tests laid down in the *Puttaswamy* judgment⁴⁶ for infringing the right to privacy.

The proposed rule is also ambiguous. The first part of the rule states that “*when required by lawful order, the intermediary shall, within 72 hours of*

⁴⁴ The Information Technology Act, 2000, s. 2(1)(za).

⁴⁵ The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

⁴⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.

communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto.”

While “security of state” is a term found in the Constitution, “cybersecurity” needs to be defined or at least the gravity of threat to cybersecurity after which the intermediary has to undertake these obligations. The phrase “protective or cyber security” is not clear and leads to ambiguity. The phrase should be “protective of cyber security”. However, that is unnecessary since this is covered by the phrase “concerning security of the State or cybersecurity”. Additionally, an expansive reading of “and matters connected with or incidental thereto” will allow the state an unfettered access to data which would violate the right to privacy.

▫ **TRACEABILITY AND ENCRYPTION**

The second part of the rule mandates an intermediary to provide traceability to find the originator⁴⁷ of certain information. Traceability needs to be defined and it should be specified as to what exactly the government requires when it requires the intermediary to trace the originator. This will help to pre-empt the claim that it may be technically impossible to provide the kind of traceability that the state expects. Even in case an intermediary is not end-to-end encrypted, an originator may be using a VPN to browse the Internet or Tor to connect to it. In such instances there is only very limited information that an intermediary will be able to provide.

There are conflicting opinions whether the provision of traceability (as generally understood) can be introduced without breaking encryption.⁴⁸

The U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated that encryption and anonymity are

⁴⁷ The Information Technology Act, 2000, s. 2(1)(za).

⁴⁸ See Press Trust of India, *Building traceability will undermine end-to-end encryption: WhatsApp*, INDIAN EXPRESS (Aug. 23, 2018), <https://indianexpress.com/article/technology/tech-news-technology/building-traceability-will-undermine-end-to-end-encryption-whatsapp-5321806/>; Himanshu Gupta and Harsh Taneja, *WhatsApp has a fake news problem—that can be fixed without breaking encryption*, COLUMBIA JOURNALISM REVIEW (Aug. 23, 2018), https://www.cjr.org/tow_center/whatsapp-doesnt-have-to-break-encryption-to-beat-fake-news.php.

essential to protect the rights of privacy and freedom of expression online, and any limitations on them should be narrow.⁴⁹

The freedom of speech and expression across the whole of the internet as a medium is seriously and disproportionately undermined by this requirement, if it requires breaking encryption. Where speakers in the offline context were assured a limited degree of secrecy and obscurity in their communications, the proposed measure renders encrypted and therefore secret communication impossible.

In *Puttaswamy*⁵⁰, it was recognized that a right to cognitive privacy – that is the right to think and work through one’s thoughts and beliefs and develop opinions and positions without interference – was a part of the right to privacy. Without the opportunity for this right to reflect, a key object of Article 19(1)(a) which is to lay the foundations for a vibrant and deliberative electorate and democracy whose citizens are genuinely informed and aware,⁵¹ is seriously impaired.

By creating the capacity for surveillance at will and with neither the opportunity for speakers to be served any notice nor any opportunity for them to contest improper uses of the capacity, such a provision expands the state’s capacity for invisible and unaccountable surveillance.

This measure is problematic in three respects. *First*, as explained above, unlike in respect of the processes under Sections 69 and 69B of the IT Act⁵², not even a minimally rights respecting procedure for the exercise of this sweeping power is specified. *Second*, this measure amounts to shifting the natural presumption from one of innocence to one of guilt. It is ordinarily understood that ordinary citizens will be left untouched in the enjoyment of their rights – including the rights to speak, to associate and to privacy – until the state demonstrates some reasonable justification for limiting their rights. By the proposed measure, the expressive capacity of citizens

⁴⁹ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 56, A/HRC/29/32 (May 22, 2015) (David Kaye).

⁵⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (Bobde, J., sep. op.).

⁵¹ *Union of India v. Association for Democratic Reforms*, 2002 (3) S.C.R. 294.

⁵² For an analysis of safeguards under Section 69 and Section 69B of the Information Technology Act, 2000 see Chinmayi Arun and Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASES STUDIES 75-79 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

is diminished without the showing of any cause sufficient under constitutional law. *Third*, by applying this inverted presumption to all citizens and all speech online, this proposed draft rule assures its unconstitutionality under any standard of review – whether rigorous or minimal. In contrast to a basis in targeted suspicion, generalized suspicion would neither satisfy the classic test in *V.G. Row*⁵³, nor would it meet the new standard of proportionality adopted in respect of privacy in *Puttaswamy*⁵⁴.

▫ **EXCESSIVE DELEGATION**

Sections 69 and 69B of the Act read with their respective subordinate legislations⁵⁵ provide the procedure for access by law enforcement agencies to information available with the intermediary.

A delegated legislation apart from being challenged on the ground that it exceeds the parent statute, can also be challenged for being contrary to other statutory provisions.⁵⁶ In the present case, parts of the proposed Rule 3(5) that are in conflict with Sections 69 and 69B and rules framed under those. Rule 3(5) is beyond the mandate of the parent provision i.e. Section 79(2) and thus void.

RULE 3(7)

The proposed rule requires that any intermediary with more than 50 lakh users in India or who is in a list notified by the government, needs to incorporate in India, have permanent office in India and appoint a nodal officer in India.

The rule, like a lot of other proposed rules is vague and ambiguous. It does not define/ explain what a “user” is for the purposes of this rule. India has over 560

⁵³ *State of Madras v. V.G. Row*, (1952) S.C.R. 597.

⁵⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (Chandrachud, J.) and (Kaul, J., sep. op.) whose opinions represent a majority of 5 judges of the 9 on the bench in this case).

⁵⁵ The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

⁵⁶ *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C. 641. See Ujjwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011* (July 16, 2012), <https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules>.

million Internet subscribers as of September 2018⁵⁷, and this number is probably over 600 million currently⁵⁸. There is no rational given as to why this number is chosen. MeitY should also clarify how it will determine the number of users, once the term is defined. Otherwise it will be impossible to implement this rule.

▫ **POTENTIAL VIOLATION OF ARTICLE 19(1)(A)**

If the burden of incorporation and maintaining an office in India proves to be too onerous certain intermediaries will probably stop providing services in India. Such a situation will give rise to a potential violation of the right to freedom of expression.⁵⁹ The right to freedom of speech and expression includes the right to receive information⁶⁰, and the court has held the right to a diverse media environment as an integral part of Article 19(1)(a) of the Constitution.⁶¹ This interpretation is consistent with the internationally recognized principle of freedom of expression codified in Article 19 of the International Covenant on Civil and Political Rights⁶² to which India is a signatory.

▫ **EXCESSIVE DELEGATION**

Rule 3(2)(7)(i) and (ii) are beyond the scope of Section 79(2) of the IT Act. The executive in the garb of rulemaking is legislating and widening the scope of the

⁵⁷ Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators: July – September 2018*, ii (Jan. 8, 2019), available at <https://main.trai.gov.in/sites/default/files/PIR08012019.pdf>.

⁵⁸ India is adding 10 million active internet users per month: Google, BUSINESS STANDARD (June 27, 2018), https://www.business-standard.com/article/current-affairs/india-is-adding-10-million-active-internet-users-per-month-google-118062700882_1.html.

⁵⁹ See Chinmayi Arun, *The 'Purdah' amendment: Proposed changes to the IT Act could draw a veil over the Indian internet*, SCROLL (Jan. 24, 2019), <https://scroll.in/article/910601/the-purdah-amendment-proposed-changes-to-the-it-act-could-draw-a-veil-over-the-indian-internet>.

⁶⁰ *Bennett Coleman v. Union of India*, (1972) 2 S.C.C. 788 (Mathews, J., dissenting); *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C. 641; *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161; *Sahara India Real Estate Corporation Ltd. & Ors. v. SEBI & Anr.*, (2012) 10 S.C.C. 603; *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 21.

⁶¹ *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶¶ 201(3)(a)-(b).

⁶² International Covenant on Civil and Political Rights, art. 19, (Dec. 16, 1966), 999 U.N.T.S. 171.

Act. Moreover, since section 79(2) does not expressly allow the executive to sub-delegate, any list of specific intermediaries prepared will be void.⁶³

RULE 3(8)

The proposed rule 3(8) is an amendment to Rule 3(4) of the current guidelines. It incorporates the changes laid down in the *Shreya Singhal* judgment regarding the actual knowledge standard and the scope of content that can be taken down.

The rule states that on receiving actual knowledge in form of a court order or on being notified by an appropriate government agency, an intermediary shall remove or disable access to content relating to unlawful acts within the scope of Article 19(2) within a period of 24 hours. It also requires the intermediary to preserve information relating to such take downs for a period of at least 180 days and maybe longer if required by a court or authorized agencies.

The proposed rule in accordance with *Shreya Singhal* incorporates the language of Article 19(2) to the guidelines. Therefore, any court or any other body determining whether a piece of content is unlawful and within the purview of Article 19(2) has to be very careful about the boundaries and judicial interpretation of these terms, and not to expand their scope. It may not be enough to state one of the grounds under Article 19(2), but will possibly require the exact unlawful act to be identified⁶⁴. The phrase “appropriate Government” and “its agency” should be defined. This will limit the unfettered power to various government bodies and specify who can ask for the takedown of content.

Moreover, the new rule reduces the maximum time period available to the intermediary for removing or disabling content from 30 days⁶⁵ to 1 day. The

⁶³ See *India v. M/s Bhanamal Gulzarimal*, A.I.R. (1960) S.C. 475; *Bhagwati Saran v. Uttar Pradesh*, A.I.R. (1961) S.C. 928; S.P. SATHE, *ADMINISTRATIVE LAW* 56-57 (2008).

⁶⁴ See Shrutanjaya Bhardwaj, *Comments on the Draft Intermediary Guidelines (Amendment) Rules, 2018*, 1 (Jan. 4, 2019).

⁶⁵ Ministry of Electronics & Information Technology, Government of India, *Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000* (Mar. 18, 2013), available at [http://meity.gov.in/sites/upload_files/dit/files/Clarification%2079rules\(1\).pdf](http://meity.gov.in/sites/upload_files/dit/files/Clarification%2079rules(1).pdf). See Chinmayi Arun and

proposed rules should differentiate between content⁶⁶ and have different time period for different content.

Unlawful acts relating to “the sovereignty and integrity of India”, “the security of the State”, and potentially “public order”, which require an urgent response can have a period of 24-48 hours. Unlawful acts relating to other grounds in Article 19(2) can have a time period of at least 14 days⁶⁷. While the authority issuing the order will (presumably) apply its mind, this period will also allow the intermediary to review the content and decide its validity in relation to this rule.

If the time period remains 24 hours for all the content, to claim the immunity under Section 79, the intermediaries will err of the side of removing content and in most instances will take down the content without adequately examining it.⁶⁸ This will lead to censorship and takedown of lawful speech.⁶⁹

The rule also requires retention of content that is disabled or taken down. However, it does not provide for conditions of such preservation, or describe what kind of investigation is permitted into such information. Where such data consists of personal information, the rules will need to ensure that data retention procedures, as well as the procedures to be followed at the time of investigation, or transfer of the information to the government agencies or courts for such investigation are respectful of the right to privacy and the principles of data protection in *Puttaswamy*

Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASES STUDIES 74-75 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

⁶⁶ See Jens-Henrik Jeppesen, *The European Commission’s draft regulation on ‘terrorist content’ requires significant revision*, CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 21, 2018), <https://cdt.org/blog/the-european-commissions-draft-regulation-on-terrorist-content-requires-significant-revision/>.

⁶⁷ Recent initiative in Europe have a different time periods ranging from 1 hour to

⁶⁸ See Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India*, 7 N.U.J.S. L. Rev. 73, 83 (2014).

⁶⁹ See Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET & SOCIETY, BANGALORE 20-23 (Apr. 10, 2012), <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf/view>; Daphne Keller, *Empirical Evidence of “Over-Removal” by Internet Companies under Intermediary Liability Laws*, CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Oct. 12, 2015), <http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws>.

(in the absence of any specific data protection laws in India). The term “government agencies” also needs to be defined. The rule also lacks any outer time limit for retention of the data, and this will be violative of test laid down in *Puttaswamy*.

It is also useful to note that preservation and retention of information by intermediaries is already dealt under Section 67C of the IT Act, and ideally the issue of retention should be dealt under that section.

The proposed rule or the existing rule have no safeguards against misuse. To remedy that, it should be mandatory for the body asking for takedown to record its reasons in writing. In all cases except for those that fall within the 1-2 days takedown period, the intermediary and the originator (if identified) should be heard before passing an order.⁷⁰ In cases of 1-2 days takedown period, there should be an ex-post facto hearing, and the content should be enabled/ put-up again if the committee is satisfied that such content does not fall within the ambit of Article 19(2).

It may be useful to set up a dedicated body/ bodies in different states (like under Section 69A) to deal with these issues. However, to avoid misuse and adhere to the scope of restrictions in Article 19(2) it is necessary to have judicial oversight⁷¹. While the exact nature and scope of the body will require an in-depth examination, MeitY should start considering this option.

RULE 3(9)

This rule mandates the intermediary to use automated tools or other appropriate mechanisms to proactively identify and disable/ remove unlawful content.

Shreya Singhal has already held that an intermediary should not be made to judge the validity of any content.⁷² Moreover, since the proposed rule does not define “unlawful information or content” it suffers from vagueness and is void. The rule also

⁷⁰ See *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 115.

⁷¹ See *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) S.C.C. OnLine S.C. 1642, ¶ 447(4)(f).

⁷² *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 121-122.

does not define what is “appropriate mechanisms” which can be used in place of automated tools.

A programme for proactive monitoring and censorship, such as by using algorithms in order to detect and block content, raises several other concerns. These obligations will require encrypted intermediaries to break their encryption. The problems relating to this have already been discussed above. Additionally, since these rules apply to all the intermediaries it will be practically impossible for some like cyber-cafes to follow these rules and the rule will not be of relevance to several others like ride hailing platforms among others.

Further, at the threshold, any programme for automatic censorship and prior restraint by an intermediary, rests on the foundation of total prior surveillance.⁷³ Under this rule private entities (namely, the intermediary) are left in total control of users’ rights freedom of expression and to privacy online. As these entities are not ‘State’ for the purposes of Part III of the Constitution, they are under no legal obligation to respect or protect fundamental rights or even to apply basic requirements of natural justice, including the rights to notice and to a hearing when decisions adverse to a citizen’s rights are taken. The state under this rule is outsourcing the judicial function to private entities.

At a general level, the impulse to introduce technical measures to address problematic speech online is understandable, given the volume of communication on each online service at the content layer of the Internet. The Supreme Court has recognized this concern and noted the tremendous difficulties associated ensuring review and takedown of content on individualized basis.⁷⁴ Nevertheless, algorithmic blocking must be approached with circumspection and careful advance consideration.

⁷³ See Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism 9-10, OL OTH 71/2018 (Dec. 7, 2018) (David Kaye, Joseph Cannataci and Fionnuala Ní Aoláin).

⁷⁴ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 122.

There is a growing awareness of the limitations and pitfalls of algorithmic systems.⁷⁵ These technologies are inaccurate⁷⁶ and prone to both over inclusive and under inclusive outcomes.⁷⁷ Automated tools are a blunt instrument, with an incapacity to correctly register tone and context (which can vary across cultures, classes and other social dimensions) in the manner a human reader would be able to⁷⁸ and disproportionately affect marginalized speakers and communities⁷⁹.

Finally, over-censorship, by which a great deal of lawful content is disabled, is a near certainty.⁸⁰ The legal consequence of failing to screen content through these means is a lifting of the intermediary safe harbour under Section 79 of the parent act. Intermediaries acting rationally and in their ordinary best interests are offered no real incentive to preserve users' freedom of speech and a serious disincentive to the retention of problematic content on their services. The natural choice for any rational actor would be to over-censor and thus limit liability.⁸¹

⁷⁵ See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (Aug. 29, 2018) (David Kaye); EVAN ENGSTROM AND NICK FEAMSTER, THE LIMITS OF FILTERING: A LOOK AT THE FUNCTIONALITY & SHORTCOMINGS OF CONTENT DETECTION TOOLS (March 2017); NATASHA DUARTE, EMMA LLANSÓ AND ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS (November 2017).

⁷⁶ Daphne Keller, *Problem with Filters in the European Commission's Platforms Proposal*, CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Oct. 5, 2017), <http://cyberlaw.stanford.edu/blog/2017/10/problems-filters-european-commissions-platforms-proposal>.

⁷⁷ Jens-Henrik Jeppesen and Laura Blanco, *Taking 'Illegal' Content Online: The EC continues push for privatized law enforcement*, CENTER FOR DEMOCRACY & TECHNOLOGY (Oct. 7, 2017), <https://cdt.org/blog/tackling-illegal-content-online-the-ec-continues-push-for-privatised-law-enforcement/>.

⁷⁸ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 15, A/73/348 (Aug. 29, 2018) (David Kaye); NATASHA DUARTE, EMMA LLANSÓ AND ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 16, 19 (November 2017).

⁷⁹ NATASHA DUARTE, EMMA LLANSÓ AND ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 13-15 (November 2017).

⁸⁰ Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET & SOCIETY, BANGALORE 20-23 (Apr. 10, 2012), <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf/view>; Daphne Keller, *Empirical Evidence of "Over-Removal" by Internet Companies under Intermediary Liability Laws*, CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Oct. 12, 2015), <http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws>.

⁸¹ See Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India*, 7 N.U.J.S. L. Rev. 73, 83-86 (2014); Emma Llansó, *German Proposal Threatens Censorship on Wide Array of*

CONCLUSION

There is a need to make the Internet a safer space. However, the proposed guidelines do not fulfil that aim and will instead lead to prior restraint, chilling effect, complete loss of anonymity and surveillance. The proposed guidelines are vague and do not contain adequate safeguards against misuse, and in their current form violate a number of fundamental rights enshrined under the Constitution.

MeitY must take into account and adhere to the constitutional and international human rights principles, as well as the Supreme Court's jurisprudence on the freedom of speech and expression and the right to privacy, while updating the rules to bring them in consonance with the current India law.

We appreciate MeitY's open and consultative approach and hope that it will adopt the same approach before finalizing the rules.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Online Services, CENTRE FOR DEMOCRACY AND TECHNOLOGY (Apr. 7, 2017), <https://cdt.org/blog/german-proposal-threatens-censorship-on-wide-array-of-online-services/>.

Comments on

Intermediary Guidelines (Amendment) Rules 2018

1. Definition of 'Intermediary'

The definition provided under IT Act 2000 is as under

"intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;"

Comment: - The above definition do not cover inventory model of e Commerce sites and need to be expanded to cover them also. As per Consumer Protection Bill, 2018 both market places as well as inventory models are considered as electronics service providers liable to service deficiencies affecting consumers.

Definition of 'User'

The definition provided under IT intermediary guideline rules, 2011 is as under

"user means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary."

Comment:- The above definition do not cover consumer using the electronic platform for making purchases and only covers business transactions. Hence user definition should also include any person who access the computer resources of the intermediary for the purpose of purchasing goods or services.

3. Due diligence to be observed by intermediary — The proposed amendment to the Rules adds clause (j) and (k) to sub rule 3(2).

“The intermediary shall observe following due diligence while discharging his duties, namely : —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

- (a) belongs to another person and to which the user does not have any right to;*
- (b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;*
- (c) harm minors in any way;*
- (d) infringes any patent, trademark, copyright or other proprietary rights;*
- (e) violates any law for the time being in force;*
- (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;*
- (g) impersonate another person;*
- (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;*
- (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.*
- (j) threatens public health or safety; promotes smoking or consumption of intoxicants including alcohol*

(k) *threatens critical information infrastructure*".

Comments- The proposed amendment do not cover the following:-

- The intermediary should publish the terms and conditions of the agreement between the intermediary and the user hosting or publishing his products or services for sale.
- The intermediary shall not host or display any information that is misleading or likely to mislead users who access the platform for purchase of goods and services.
- ✓ Intermediary being a service provider will have vicarious liability along with users of the site for displaying or selling their goods or services
- Disclose complete information relating to products and services displayed on the sites
- Provide for appropriate security and transparency clauses in the terms of agreement with sellers and payment gateways for protecting the users personal data
- Should not influence advertisement or prices or discounts offered by sellers on the site.
- Shall follow the RBI rules in guidelines in respect of payments or money transactions.

4. Responsibility of Intermediary – clause 9 of the proposed amendment do not actually overcome the situation created by the supreme court judgment as discussed below

Clause 4 of the rule states as under *“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 as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least one hundred and eighty days for*

investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorized”.

Comments-

The supreme court landmark judgment in the case of **Shreya Singhal v Union of India**, it held that the provisions regarding the issue of ‘knowledge’ of the intermediary, and the consequent actions to be taken by the intermediary, i.e. section 79(3) (b) of the IT Act, and Rule 3(4) of the Intermediary Rules are to be read down to mean that the intermediary must receive a court order / notification from a government agency requiring the intermediary to remove specific information. Further, the Supreme Court has also stated that any such court order or notification must necessarily fall within the ambit of the restrictions under Article 19(2) – therefore providing that any order for removal of content that is considered ‘illegal’ must fall within the reasonable restrictions provided for under Article 19(2) of the Constitution of India i.e such removal must be in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. The judgment of the Supreme Court though provided some clarity by reading down the provisions of Section 79 and the Intermediary Rules and stating that the intermediary must receive a court order/ notification from a government agency for removing specific information/ content, it left two issues open.

- a) There is no clarity on which specific administrative agencies would have the authority to issue such an order.
- b) Whether such a reading down hampers protection of individuals, since intermediaries would not be obligated to undertake any take down/ removal action upon receipt of third parties complaints (however grave and severe) even if the complaint on its face merits take down.

As a result, illegal content (that could potentially cause loss or injury) may continue to be viewed in public domain until a court order or administrative order is received- a process which may take substantial time and militates against the veins of basic consumer protection principles.

5. Clause 8 under the amended rule:-

Clause 8 states that the intermediary who has more than fifty lakh users in India shall:

- (i) Be a company incorporate under the Companies Act, 1956 or the Companies Act, 2013;*
- (ii) Have a permanent establishment in India;*
- (iii) Appoint a Grievance Officer located in India.*

Comments:-

✓ We do not agree with this clause as the above conditions are applicable only to intermediaries who has more than fifty lakh users. There may be many e Commerce sites operating less than fifty lakh users especially inventory models and platforms selling particular types of goods and services. The provisions proposed above do not cover such sites and can create consumer ~~determent~~ *deteriment*.

✓ **6. Clause 12 of the amended** rules states that *“the intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule (3) can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint”.*

Comments: - We may suggest that the intermediary may publish on its website the toll free no. of National Consumer Helpline also as part of grievance redressal. Intermediaries may also mandatorily join convergence platform of National Consume Helpline operated by the DOCA.



MIT/79/085

To,
Shri Ajay Prakash Sawhney
Secretary
Ministry of Electronics and Information Technology
secretary@meity.gov.in

CC: Cyber Laws & E-Security Division
Ministry of Electronics and Information Technology
gccyberlaw@meity.gov.in; pkumar@meity.gov.in; dhawal@gov.in
January 31, 2019

Dear Sir,

Re: "Comments / suggestions invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018"

We are a consumer rights group that advocates for tobacco harm reduction as a public health strategy to combat the alarmingly high tobacco health burden of our country. We are a grassroots organization that works with tobacco users from across the country to disseminate information on risk reduction and help them make the transition to less harmful alternatives. We are globally recognized for our efforts and are a part of international consumer advocacy efforts on tobacco harm reduction. Following is our considered response to the proposed bill, specifically in regards to item 3(j), which we believe will be highly detrimental to public health.

Background (India's tobacco problem)

As you are aware, India is reeling under a tobacco epidemic – 267 million Indians (42.4% of men, 14.2% of women and 28.6% of all adults) use tobacco in some form, of whom 106 million smoke, according to GATS-2 survey. Nearly a million Indians die every year from tobacco-related illnesses, with annual economic loss of over Rs1 lakh crore, according to the Ministry of Health & Family Welfare (1).

Though there was a 6% decline in tobacco use from 2010 to 2017 (GATS-1/2), at this rate it will be decades before use of tobacco is eliminated, during which time millions more Indians will die. India had the lowest quit rates among the countries surveyed in GATS-2 and despite the decline in use, the disease demography shows tobacco is becoming a bigger killer. Ischemic heart disease and chronic obstructive lung disease, both attributable to tobacco, ranked in positions 1 and 2 among causes of death in India in 2016, having ranked 6 and 8 respectively in the 1990s (2). It should be noted that the disease burden associated with smoking is predicted to rise further in low- and middle-income countries (LMICs), which includes India (3). This clearly shows that smoking and tobacco use is a public health priority in India, with urgent and effective measures needed to reduce the burden to society and the healthcare system.



The three state-sanctioned interventions – encouraging cold-turkey quit attempts, cessation services and counselling, and nicotine replacement therapy (NRT) – are not enough. Quit lines and media outreach have done little to change the overall 95% failure rate of willpower-led cessation. Tobacco cessation clinics remain woefully inadequate, with just 19 functional for a 27 crore population (4). The effectiveness of NRTs is also limited, hovering near 7% (5).

Further, a recent study showed that a large majority of medical professionals in India have reported having insufficient experience to offer cessation assistance (6). Additional barriers for smoking cessation include deeply ingrained cultural habits, tobacco use by healthcare professionals and limited motivation of physicians to document tobacco use and provide appropriate consultation (7). Crucially, in 2018 a secondary analysis of cross-sectional data from nationally representative Household Consumer Expenditure Surveys (1999–2000; 2004–2005 and 2011–2012) found that India's National Tobacco Control Programme (NTPC) may not have produced reductions in tobacco use (8).

Raising taxes also has limitations cost increases above a certain threshold forces smokers to shift to cheaper, more harmful variants, thus causing more harm than good. High taxes also do little to limit uptake when the average cost of loose cigarettes (sold across the country despite bans in a few states) is extremely low.

Risk mitigation

It is hence imperative that we expand and intensify our tobacco control efforts. While continuing the interventions aimed at elimination of tobacco use, adequate focus has also to be laid on reduction in harm from tobacco by switching current users to lower-risk alternatives, including technology-driven Nicotine Delivery Systems (ENDS). This approach has been adopted by 65 nations worldwide (9), many of whom have since witnessed historic decline in smoking prevalence.

E-cigarettes are now the most popular method of assisted quit attempts in the United States, used in 35% of smokers' most recent quit attempts (10). In the UK, where physicians prescribe ENDS to heavy smokers, there has been a sharp reduction in smoking prevalence (11, 12). Along with the 9 million Americans who have quit smoking with ENDS, so have 2.9 million in UK, 1.2 million in France, 1.5 million in Russia, 1.38 million in Italy, a million in Malaysia, 711,000 in Indonesia, 308,000 in Canada, and many more millions across the world (13).

ENDS have also been found by credible institutions – Public Health England, Royal College of Physicians (UK), American Cancer Society, National Academies of Science Engineering & Medicine, US FDA and many others – to be up to 95% safer than smoking as they eliminate combustion, which is recognised by WHO to be the main cause of harm as it produces tar and releases 76 known carcinogens.



ASSOCIATION OF VAPERS INDIA

contact@vapeindia.org | www.vapeindia.org

Health organizations, agencies and governments that have reviewed the evidence on tobacco harm reduction	
	US National Academies of Sciences, Engineering and Medicine (NASEM): <i>While e-cigarettes are not without health risks, they are likely to be far less harmful than combustible tobacco cigarettes.</i>
	US Food & Drug Administration: <i>Make no mistake. We see the possibility for ENDS products like e-cigarettes to provide a potentially less harmful alternative for currently addicted individual adult smokers who still want to get access to satisfying levels of nicotine without many of the harmful effects that come with the combustion of tobacco.</i>
	American Cancer Society: <i>Based on currently available evidence, using current generation e-cigarettes is less harmful than smoking cigarettes.</i>
	American Association of Public Health Physicians: <i>Smokers unable or uninterested in quitting should consider switching to a less hazardous smoke-free tobacco/nicotine product [including] nicotine replacement therapy; electronic cigarettes; snus; other forms of moist snuff, and chewing tobacco.</i>
	Royal College of Physicians: <i>Available data suggest that e-cigarette health risks are unlikely to exceed 5% of those associated with smoked tobacco products, and may well be substantially lower. In the UK, harm reduction is a recognised element of comprehensive tobacco control. E-cigarettes are effective in helping people to stop smoking. There are as yet no identified health risks from second hand vapour.</i>
	British Medical Association: <i>There are clear potential benefits to e-cigarette use in reducing the substantial harms associated with smoking, and a growing consensus that they are significantly less harmful than tobacco use.</i>
	British Lung Foundation: <i>There's more evidence than ever that e-cigarettes are safer than smoking, and a way to give up altogether. Swapping cigarettes for an e-cig can improve your symptoms of lung conditions like asthma and COPD.</i>
	Public Health England: <i>Our new review reinforces the finding that vaping is a fraction of the risk of smoking, at least 95% less harmful, & of negligible risk to bystanders. Yet over half of smokers either falsely believe that vaping is as harmful as smoking or just don't know.</i>
	Cancer Research UK: <i>Evidence so far indicates e-cigarettes are far less harmful than tobacco and may help smokers to cut down or quit. We do not believe there is justification for an indoor ban, either on the basis of potential harm to bystanders from 2nd-hand vapour or that they renormalize smoking.</i>
	Royal Society for Public Health: <i>Endorses new Public Health England (PHE) report reflecting up-to-date evidence that is increasingly pointing in the same direction: not only is vaping at least 95% less harmful than smoking, but it is also helping increasing numbers of smokers to quit.</i>
	Royal College of General Practitioners: <i>The evidence so far shows that e-cigarettes have significantly reduced levels of key toxicants compared to cigarettes, with average levels of exposure falling well below the thresholds for concern.</i>
	Cochrane Tobacco Addiction Group (Cochrane TAG): <i>Electronic cigarettes may increase the chance of quitting smoking long term [and] no serious side effects were associated with their use (up to two years).</i>
	Government of Canada: <i>Vaping is less harmful than smoking. Adults can now legally get vaping products with nicotine as a less harmful option than smoking. Switching from tobacco cigarettes to vaping products will reduce a person's exposure to many toxic and cancer-causing chemicals.</i>
	Truth Initiative: <i>Some smokers may be unable or unwilling to quit using nicotine and would benefit by completely switching to a much lower harm nicotine delivery mechanism (including potentially a well-regulated e-cigarette).</i>
	New Zealand Ministry of Health: <i>The evidence on vaping products indicates they carry much less risk than smoking cigarettes. Vaping products could disrupt inequities and contribute to Smokefree 2025.</i>
	Royal Australian & New Zealand College of Psychiatrists: <i>Research shows that 70% of people with schizophrenia and 61% of people with bipolar disorder smoke compared to 16% of those without mental illness. E-cigarettes and vaporizers provide a safer way to deliver nicotine to those who are unable to stop smoking, thereby minimizing the harms associated with smoking tobacco and reducing some of the health disparities experienced by people with mental illness.</i>
	Philippines House of Representatives: <i>Voted unanimously to adopt a resolution promoting harm-reduction as part of its National Tobacco Control Strategy, particularly the use of electronic cigarettes as a less harmful alternative for smokers (August 2018).</i>
	Drug and Alcohol Nurses of Australasia: <i>E-cigarettes are a much safer alternative to smoking for those who are unable to quit with conventional therapies. DANA supports the use of e-cigarettes as a harm replacement tool or cessation aid for smokers who cannot quit with approved therapies, and supports low or no taxation on vaping products to maintain a price advantage to encourage smokers to switch.</i>
	National Health Service Scotland consensus statement on e-cigarettes: <i>Smoking kills. Helping people to stop smoking completely is our priority. There is now agreement based on the current evidence that vaping e-cigarettes is definitely less harmful than smoking tobacco. It would be a good thing if smokers used them instead of tobacco.</i>
<p><i>Created and endorsed by:</i> Action on Smoking & Health Scotland • Cancer Research UK • Chest Heart & Stroke Scotland • Chief Medical Officer for Scotland • Directors of Public Health • Faculty of Public Health • NHS Ayrshire and Arran • NHS Greater Glasgow and Clyde • NHS Lothian • NHS Tayside • Roy Castle Lung Cancer Foundation • Royal College of General Practitioners • Royal College of Physicians of Edinburgh • Royal College of Physicians and Surgeons of Glasgow • Royal Environmental Health Institute of Scotland • Scottish Collaboration for Public Health Research and Policy • Scottish Consultants in Dental Health • Scottish Thoracic Society • UK Centre for Tobacco and Alcohol Studies • University of Edinburgh • University of Stirling</p>	



Moreover, the first major clinical trial into the effectiveness of ENDS as a smoking cessation method found them to be almost twice as effective as nicotine replacement therapies (NRTs) such as gums, lozenges and patches (14).

Right to harm reduction

India's over 10 crore smokers therefore have an unalienable right to access information on ENDS which can mean the difference between life and certain death to them as smoking statistically kills half of all users, and passive smoking causes 800,000 deaths worldwide every year (15). ENDS have also been found to produce no second-hand harm (16).

No Indian should be denied information or access to technology that can save their lives, since harm reduction and the right to lead a healthier life are enshrined in our Constitution through Article 21. Banning any information that "promotes ENDS" violates the fundamental rights of citizens to reduce harm to themselves since this vague definition can include even communicating the risk differential of ENDS being 95% safer than smoking. It is also a serious case of spreading misinformation and gravely detrimental to public health that a proven and globally adopted risk-mitigation tool is being clubbed with serious risks such as alcohol and smoking.

The concern that ENDS will lead to smoking among teens is unfounded and there is little research to show ENDS act as gateway to smoking. A large study of 60,000 teen respondents in the UK found no evidence of the gateway theory (17). The concern that ENDS are becoming popular among teens can be addressed through sensitive guidelines such as age-verification and responsible communication of risks instead of imperiling the lives of millions of Indians by denying them access to potentially life-saving information.

Legally too, the central advisory on ENDS on which this draft amendment is based has been ruled to be nonbinding by the Delhi High Court (18). In the absence of any law prohibiting ENDS, the clampdown on ENDS-related information is unlawful. Putting the onus of ensuring implementation, because of the vague norms, will lead to overregulation and denial of services to parties who are genuinely working towards advancing public health and in reducing the enormous tobacco health burden of our country.

Kind Regards

Samrat Chowdhery

Director

Association of Vapers India



References

1. [Economic Burden of Tobacco-Related Diseases in India](#) (MOHFW)
2. Dandona L, Dandona R, Kumar GA, et al. Nations within a nation: variations in epidemiological transition across the states of India, 1990-2016 in the Global Burden of Disease Study. *Lancet*. 2017;390(10111):2437-2460
3. The Lancet (editorial). Progress towards a tobacco-free world. *Lancet*. 2018;392(10141):1.
4. Thankappan KR. Tobacco cessation in India: a priority health intervention. *Indian J Med Res*. 2014;139(4):484-486
5. Hughes JR, Shiffman S, Callas P, Zhang J. A meta-analysis of the efficacy of over-the-counter nicotine replacement. *Tob Control*. 2003;12(1):21-7
6. McKay AJ, Patel RKK, Majeed A. Strategies for Tobacco Control in India: A Systematic Review. *PLoS ONE* 2015;10(4): e0122610.
7. Murthy P, Saddichha S. Tobacco cessation services in India: recent developments and the need for expansion. *Indian J Cancer*. 2010;47 Suppl 1:69-74.
8. Nazar GP, Chang KC, Srivastava S, et al. Impact of India's National Tobacco Control Programme on bidi and cigarette consumption: a difference-in-differences analysis. *Tobacco Control*, doi: 10.1136/tobaccocontrol-2018-054621
9. [Report by the FCTC Convention Secretariat on ENDS](#) (2018)
10. Caraballo RS, Shafer PR, Patel D, Davis KC, McAfee TA. Quit Methods Used by US Adult Cigarette Smokers, 2014–2016. *Prev Chronic Dis* 2017;14:E35.
11. [Smoking rate in UK falls to second-lowest in Europe](#) (The Guardian)



12. Beard E, West R, Michie S, Brown J.. Association between electronic cigarette use and changes in quit attempts, success of quit attempts, use of smoking cessation pharmacotherapy, and use of stop smoking services in England: time series analysis of population trends. *BMJ* 2016;354:i4645.
13. ENDS users in [US](#), [UK](#) and [France](#)
14. A Randomized Trial of E-Cigarettes versus Nicotine-Replacement Therapy. DOI: 10.1056/NEJMoa1808779
15. [WHO key facts on tobacco](#)
16. [Evaluation of Chemical Exposures at a Vape Shop](#) (NIOSH-CDC)
17. Adolescents and e-cigarettes: Objects of concern may appear larger than they are. DOI: 10.3390/ijerph14090973
18. [Government advisory on e-cigarette ban not binding on states: Delhi HC](#) (Hindustan Times)

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

MIT/79/086

Introduction

Star India Private Limited (“Star India”) welcomes the efforts by Ministry of Electronics and Information Technology (“MEITY”), Government of India, to strengthen the legal framework for intermediaries in India. We believe that such efforts are needed to protect the integrity of India’s digital economy and all its sub-sectors, including media and entertainment (“M&E”). At the same time, we re-affirm our commitment to the Government’s vision to protect its citizens from unlawful content, mis-information and dis-information through online means.

Government’s Digital India vision is finally being realized across the length and breadth of the country with unprecedented internet penetration. This has created the need to overhaul and upgrade India’s regulatory regime for the new digital economy including the Information Technology Act and the Rules, most specifically, Intermediary Guidelines Rules.

These rules were drafted under Section 79 of the Information Technology Act, 2000 (“IT Act”), which was enacted at a time when internet penetration was mostly an urban phenomenon. Today, the scenario is quite different as India is home to the world’s second largest internet user base and internet companies, both foreign and domestic, have thrived.

Hence, as India attains prominence on the global digital space, it is necessary that regulation keeps pace to create a digitally empowered knowledge society that conforms to principles and norms prescribed in its constitutional and legal regime.

With this background we submit our comments on Rule 3(5), 3(7), 3(8) and 3(9) of the proposed amendment.

I. Protecting intellectual property online under Rule 3(9)

Internet consumption in India has grown manifold in the past few years and this is manifested by the fact that average monthly internet consumption has grown from 353 million gigabytes in 2016 to 4 billion gigabytes in 2018, which is highest globally. Most of the growth in data consumption has been on the back of availability of cheap and reliable access to 3G/4G LTE mobile internet and phenomenal rise in smartphone penetration. It is interesting to note that most of the growth in data consumption – in which rural and semi-urban areas lead metros – has been on the back of video consumption.

With this growth, tremendous increase has been witnessed in online piracy, which has caused massive losses to digital content producers and artists. According to industry estimate¹, pirates make 35% more than the actual producers of the same content. Much of this revenue has been on the back of pirated content being uploaded on so-called “user-generated” content platforms, social media platforms, torrent sites and others which enable selling advertising to make money off it. The problem is compounded by search engines, micro-blogging sites and online forums which further accentuate the distribution of links to pirated content.

¹ FICCI-EY Report 2018

A lot of money generated through online piracy ends in financing unlawful activities including terrorism, drugs, trafficking among others.

The content industry has been making attempts at curbing this massive leakage. However, it runs into rough weather when dealing with online platforms, most of whom qualify to be protected as “intermediaries”.

On the other hand, several intermediaries have misused the provisions of Section 79 of the IT Act and the Rules by wrongly interpreting the provisions to mean that they have complete immunity from compliance with Indian laws and enforcement agencies. On the back of this abuse of this law and due process, they have built advertising-led business models using third party owned copyrighted content. While some may have collaborated with content creators, the lack of legal provisions under the current Section 79 of the IT Act and Rules mandating them to actively screen and remove infringing content is the lacuna that needs to be plugged with immediate effect before the illegal use of copyrighted content reaches uncontrollable proportions.

Also, as intermediaries develop their web-hosting capabilities, they have developed highly effective monetization mechanisms utilizing technological tools that analyze the type of content being uploaded² by the originator of the information and other attributes related to it, such as viewership, preferences and others. Therefore, intermediaries, specifically social media, search engines and user-generated content platforms, have knowledge of the type of content being made available on their platforms. Furthermore, the safe harbour of 36 hours to acknowledge complaint and 30 days to resolve the same is subjected to compliance under sub-section 2 of Section 79 which clearly requires that *“the intermediary observes due diligence while discharging his duties under this Act.”*

Basis the above discussion, we urge MEITY to amend the IT Intermediary Rules and insert Rule 3(9) which mandates intermediaries to deploy tools, measures and mechanisms, technological or otherwise, to *“proactively identifying and removing or disabling public access to unlawful information or content”*.

However, the proposed Rule 3(9), even though well intentioned, shall be able to achieve its full purpose only if a corresponding amendment is made to clarify that the phrase *“unlawful information”* refers to information including the categories mentioned in Rule 2 which encompasses information which *“infringes any patent, trademark, copyright or other proprietary rights”*.

Thus, Rule 3(9) should be amended to read:

“The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content including information specified in sub-clauses (a) to (l) of Rule 3(2)”.

²A survey report by Pew Research Center, 2018: <http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/>

This shall ensure that intermediaries are required to adequately strengthen their due diligence processes to monitor, screen and remove pirated content from their platforms. This shall prove to be very effective in bringing down the volume of copyright infringing content available through intermediaries.

It may be pointed out by some that India already has a robust regime of judicial orders requiring the take down of infringing content, commonly known as *John Doe Orders*. However, it must be noted that such orders are *post-facto* in nature and title/content specific and do nothing to pre-empt the uploading of infringing content.

Thus, the entire creative fraternity of this country implores the Government to amend the IT Intermediary Rules as per the deliberations mentioned above.

II. Requirement to create local entity under Rule 3(7)

Internet as a medium has been able to build cross-border reach and enable economic and human linkages globally at levels hitherto unseen. Due to the rapid scalability of internet infrastructure, it is reckoned as the fastest growing technology in human history, and this has enabled applications developed in one country to be used in others at the click of a button. Quite simply, one does not need to create a physical or even corporate presence in jurisdiction where the actual service is provisioned.

We acknowledged that this had created challenges on the enforcement of some of the provisions of the intermediary guidelines and we recommend that this rule be amended as follows:

“The intermediary who has more than fifty lakh users in India shall appoint in India a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/ requisitions made in accordance with provisions of law or rules.”

III. Access to information and removal of content should be subject to Court supervision under Rule 3(5) and 3 (8)

While we agree on the need for such information and assistance on matters concerning security of the State or cyber security, we recommend that the powers to request for such information or removal of unlawful content be restricted only to court of competent jurisdiction.

The spread of disinformation over social media platforms and other forms of unlawful activities a legitimate law and order concern, however the demands placed upon these platforms by the proposed The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 cast far too wide a net, will the dampen free and open discourse that is a hallmark of democracy and in its current avatar is likely to cause more harm than good.

Clause: 3(8): *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 Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.*

UNNECESSARILY WIDE GAMUT:

The nebulous category of “unlawful information”, which includes any content perceived as a threat to “interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to

contempt of court, defamation or incitement to an offence” brings us full circle to Shreya Singhal v. Union of India which brought up the unconstitutionality of Section 66A's similarly unclear list of offences. To hold an intermediary accountable for such a wide, easily-misused list of content is both an unreasonable demand on the resources of the intermediary as well as a worrying chokehold on free speech.

Since the core problem this act wishes to address is, as elucidated above, a law and order issue, the Intermediary Guidelines seem to cast a disproportionately wide net. Paired with another proposed bill, the Personal Data Protection Bill (2018) which mandates that data fiduciaries store a copy of personal data of Indian users in India, the government will be able to demand access to personal information of online media users for a wide range of perceived offences to the detriment of free and open discourse online.

DATA RETENTION IS ANTITHETICAL TO PRIVACY

The amendment requires storage of content requested by law enforcement agencies for 180 days at first and then for as long as deemed necessary by a court or government agencies. By leaving the duration for storage of such data open-ended, the provision is runs contrary to the principle of ‘Storage Limitation’ recommended by the Srikrishna Committee.¹ Instead of providing for indefinite storage of data beyond 180 days the amendment should require a periodic authorization every 60 days by a court or government agency should the data be deemed valuable for an investigation. In the absence of such an authorization the data preservation request would automatically lapse.

¹ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, “A Free and Fair Digital Economy Protecting Privacy, Empowering Indians,” p.60 available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Clause 3(5): *When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.*

TRACEABILITY IS ANTITHETICAL TO PRIVACY

The amendments require intermediaries – defined under Indian law to include ISPs as well as communication platforms – to trace the originator of information on their platform when served with an order by an authorised government agency.

On communications platforms this would entail examining a chain of forwards to track down the individual who composed the original message or first uploaded a media file in question. For end-to-end encrypted services, this is not technically feasible, since the communication service providers do not have access to the content of the messages.

While MEITY has insisted² that the traceability requirement does not automatically mean breaking encryption, there is little doubt that enforcement of these rules will mean that

² Ministry of E & IT (@GoI_MeitY), “[@DialogueIndia](https://twitter.com/GoI_MeitY/status/1081505492059467776) We are asking to trace origin of messages which lead to unlawful activities without breaking encryption. [#SaferSocialMedia](https://twitter.com/GoI_MeitY/status/1081505492059467776),” January 5, 2019, 1629 Hrs, available at: https://twitter.com/GoI_MeitY/status/1081505492059467776.

some companies would have to roll back encryption entirely. To be clear, traceability is incompatible with end-to-end encryption.

Encryption as a service is used by journalists and whistleblowers to legitimately protect their privacy and in that is an enabler of the right to privacy and the freedom of expression. Apart from protecting privacy, encryption also makes communications more secure and helps ensure integrity of information.

Moreover, in many cases traceability that requires service providers to roll back or reduce the strength of encryption over their services is also likely to be ineffective. For example content that poses a threat to public order and national security (such as fake news) can be created on platforms and on forums that are not subject to Indian law and then released on to popularly used platforms where they can go viral. In situations such as these, tracing the pathway through which the content was shared by well-meaning users is unlikely to result in the apprehension of the true authors of such content.

To
Shri Pankaj Kumar
Additional Secretary
Cyber Laws and E-security group
Ministry of Electronics and Information Technology

25th January, 2019

Dear Sir,

Subject: ShareChat's views on the draft Intermediaries Guidelines (Amendment) Rules 2018

We thank your offices for giving us the opportunity to provide inputs to the draft Intermediary Guidelines (Amendment) Rules 2018 (**Draft Rules**).

ShareChat is a regional language social networking and content discovery platform built by Indians and for Indians. Our founders are a team of engineers from IIT Kanpur, who had started the platform with an aim to provide Indic language users with an ability to discover, create and share content. Our platform embraces the diversity of the Indian users, by ensuring that they can communicate in their local language. In-fact, ShareChat today supports 14 Indian languages, and specifically does not support communication in English (in favour of the Indian regional user).

We at ShareChat as a domestic Indian technology company welcome the decision to reform the governance of intermediaries such as ours and ensure greater scrutiny on the compliance with domestic Indian laws.

We would like to take this opportunity to provide our support, comments, and alternative perspectives on the Draft Rules, based on our experience in operating a large homegrown social media intermediary platform in India. Our comments and suggestions have been set out for your benefit in the subsequent sections below. In addition, please also find an annexure attached to our letter, setting out the specific language of some of our proposals in greater detail.

The Draft Rules propose to include an additional condition in our user agreements to prevent users from uploading, displaying, or modifying any information that threatens public health. Any content that is illegal and incites violence, or threatens public health is already be captured under Rule 3(2)(i) as it prohibits content that incites the '*commission of any cognizable offence*'. The Indian Penal Code, 1860 today contains several provisions that criminalizes offences that threaten public health, such as:

Section of IPC	Offence	Consequence of violation
269	Negligent Act likely to spread infection	Cognisable, bailable, 6 months jail or fine
270	Malignant likely to spread infection	Cognisable, bailable, 2 years jail or fine
271	Disobedience of quarantine	Cognisable, bailable, 6 months jail or fine

A broadly worded obligation to prevent any content that threatens public health and safety would be difficult to comply with meaningfully.

The proposed Rule 3(4), requires the platform to communicate the rules and regulations of the platform including its privacy policy on a monthly basis. Various cyber security researchers have

over time commented on how excessive notification may lead to a **notification fatigue** among users, resulting in disregarding key information and reducing the functionality of the platform. We recognize and agree to the intent behind the recommendation. Users must be informed and made aware of their obligations and the consequences of breach when using intermediary platforms. However, prescribing a set timeline, would only result in compliance with the letter and not help achieve the spirit of the policy. Instead we recommend a principle-based approach, which would require the platform to **meaningfully and periodically** inform the users of the consequences of non-compliance. This approach would be similar to the language adopted by the government in framing the Personal Data Protection Bill, 2018. Additionally, with a number of first time Internet users joining the Internet, it is imperative that these guidelines be made available in multiple Indic languages

The Draft Rules as proposed look to extend the obligations for intermediaries to assistance to law enforcement authorities. ShareChat today already provides attribution to an individual who publishes content on our platform thus ensuring traceability for content that leaves the ShareChat network.

However, we would request that the need to intercept is already sufficiently addressed, providing adequate power to the government and safeguards to protect citizen interest, under the rules framed under section 69. To the extent required, we would request that amendments be made to the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and not the Intermediary Rules.

Moreover, for us to be meaningfully contribute to law enforcement goals, and yet be able to continue to operate our business, would request that any obligation proposed in this regard should be graded, based on the associated risk to the content. In line with evolving global practice, assistance relating to terrorism, i.e. specific to legal charges for waging war against India, should ideally be provided as soon as possible, and not later than 3 hours from a valid legal request. Other serious offences that have associated risks to public order at large, such as creating enmity between groups, and rioting should be complied with within the 72 working hour's time limit. All other requests could be required to provide assistance/ information promptly, **and in no event later than 7 working/business days from the date of request.**

We welcome the move under Rule 3(7) to provide greater responsibility to offshore, social media applications that are generating and distributing large volumes of content to Indian citizens in an unregulated manner. These platforms have come under scrutiny globally for various reasons. Thus, we would recommend that the fifty lakh user limit should be lowered to ten lakh users and clarified to be applicable to ten lakh 'daily active users'. We believe that ten lakh users are a significant threshold that would require a platform to set up offices in India and be responsible to Indian law enforcement.

Moreover, we would request that this obligation is limited to platforms that permit creation and mass dissemination of social content, such as text, images, audio, and video. Expanding this obligation to all classes of intermediaries such as e-commerce companies, intermediaries such as Wikipedia, or blogging platforms may be dis-proportionate to the public policy goal of the government and impede innovation in the tech sector.

Takedown requests under Rule 3(8) could also be graded in a similar structure, with an immediate responsiveness obligation for intermediaries in relation to terrorism related content (of again 3 hours), a threshold of 72 working hours for offences that threaten public order at large, such as creating enmity between groups, and rioting, and a 7 working day period for other requests.

Finally, we would request that the Draft Rules refrain from the need to mandate proactive monitoring of content. We at ShareChat along with other social media platforms strongly believe in the need to develop and invest in the capacity to tackle content that may break Indian laws. To this end, we are taking several steps internally as well as with third party partners to limit the effectiveness of ‘bad actors’ on our platform. We would be happy to share these measures in a separate discussion if required.

However, the need to proactively monitor content may lead to platforms being required to moderate content before it is posted on our platform. This would be against the very nature of social media platforms that allows users to post freely within the ambits of our community guidelines. Moreover, it would require platforms such as ours to monitor all content, as opposed to focus our efforts on the small section of content that has the potential to negatively impact public order, thereby imposing a significantly high cost of conducting business in the Indian ecosystem.

We look forward to participating in any consultation or discussions that you may conduct to deliberate on these issues.

Warm regards,



Berges Y. Malu
Head of Public Policy and Policy Communications
ShareChat

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

Annexure: Suggested Language Changes to the Draft Rules

Rule	Proposed change	Our suggestion/ industry feedback	Proposed edit to the Draft Rules												
3(2)(i)	<p>threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p>	<p>The obligation to protect health and safety is extremely wide and difficult from a compliance perspective.</p> <p>In any case, rule 3(2)(i) as it prohibits content that incites the 'commission of any cognisable offence', which would contain provisions such as:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Section of IPC</th> <th style="text-align: center;">Offence</th> <th style="text-align: center;">Consequence of violation</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">269</td> <td>Negligent Act likely to spread infection</td> <td>Cognisable, 6 months jail or fine</td> </tr> <tr> <td style="text-align: center;">270</td> <td>Malignant likely to spread infection</td> <td>Cognisable, 2 years jail or fine</td> </tr> <tr> <td style="text-align: center;">271</td> <td>Disobedience of quarantine</td> <td>Cognisable, 6 months jail or fine</td> </tr> </tbody> </table>	Section of IPC	Offence	Consequence of violation	269	Negligent Act likely to spread infection	Cognisable, 6 months jail or fine	270	Malignant likely to spread infection	Cognisable, 2 years jail or fine	271	Disobedience of quarantine	Cognisable, 6 months jail or fine	<p>threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery to those below the legal age for consumption as permitted under law; except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p>
Section of IPC	Offence	Consequence of violation													
269	Negligent Act likely to spread infection	Cognisable, 6 months jail or fine													
270	Malignant likely to spread infection	Cognisable, 2 years jail or fine													
271	Disobedience of quarantine	Cognisable, 6 months jail or fine													
3(4)	<p>The intermediary shall inform its users at least once every month, that in case of noncompliance with rules and regulations</p>	<p>The obligation to inform every month may lead to notification fatigue. A number of researchers have demonstrated how users tend to disregard repeated messages. We understand that the proposed change flows from the need to simplify terms and conditions and make them meaningful for users.</p> <p>Instead a principle based obligation that requires platforms to communicate the obligation in simpler terms, with the use of simple language, and maybe multi media on a periodic basis will help achieve the policy</p>	<p>The intermediary shall inform its users <i>meaningfully periodically, and in clear and simple terms, of their obligations, and the consequences of at least once every month</i>, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, <i>such as the intermediary's</i> has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.</p>												

Rule	Proposed change	Our suggestion/ industry feedback	Proposed edit to the Draft Rules
3(5)	When required by lawful order, the intermediary shall, <i>within 72 hours of communication</i> , provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. <i>The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.</i>	<p>goal better.</p> <p>There is a need for law enforcement to trace the origin of messages on their platform, especially to prevent terrorism, and disturbances of public order.</p> <p>However, there is a significant push back from various corners of industry and academia to have these rules be a part of the intermediary rules.</p> <p>We would request that any changes to the technical assistance provisions are better dealt with under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which have inbuilt procedural safeguards.</p> <p>Additionally, in line with the proposed EU standard platforms should be more responsive for terrorism related content. This can be a standard of providing assistance within 3 hours of request. However, other forms of requests should ideally be dealt within a higher timeline for companies to review the request and provide the information without disrupting business</p>	<p><i>Request to be removed from the Draft Rules.</i></p> <p><i>Potential language under Section 69 Rules, rule 13(2)</i></p> <p><i>The intermediary on being issued a direction under Rule 3 Shall also provide assistance concerning security of the State within:</i></p> <p>(i) <i>3 hours of issuance of a valid legal request, in relation to requests relating to waging war against India,</i></p> <p>(ii) <i>72 hours of issuance of a valid legal request, in relation to requests relating to creating enmity between groups, unlawful assembly, and rioting, or a threat to a critical information infrastructure, and</i></p> <p>(iii) <i>7 days of issuance of a valid legal request, in all other cases relating to cyber security, or investigation or detection or prosecution or prevention of offence(s), protective or cyber security and matters connected with or incidental thereto.</i></p> <p><i>Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.</i></p>
3(7)	<i>The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall: (i) be a company incorporated under the</i>	We welcome the need for bringing in accountability and responsibility for foreign platforms. There are several small and medium sized e-commerce platforms today run by offshore, especially Chinese social media applications that are generating and	<p>A social media intermediary who has more than fifty lakh 10 lakh daily active users in India or is in the list of intermediaries specifically notified by the government of India shall:</p> <p><i>For the purposes of this provision, daily active users shall</i></p>

Rule	Proposed change	Our suggestion/ industry feedback	Proposed edit to the Draft Rules
	<p><i>Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.</i></p>	<p>distributing large volumes of content to Indian citizens in an unregulated manner. These companies and their activities should be scrutinized and prevented in India.</p> <p>However, the obligations mentioned are applicable to all forms of online platforms, and not only social media platforms. This can impact the ease of doing business for the country at large.</p>	<p><i>mean the number of unique visitors who access and take an action on the intermediary platform.</i></p>
<p>3(8)</p>	<p><i>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 Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and</i></p>	<p>Takedown requests under Rule 3(8) could also be graded in a manner as discussed for technical assistance provisions above. The intermediary should be required to respond within 3 hours for terror related content, 72 hours for offences that threaten public order at large, such as creating enmity between groups, and rioting, and a 7 working day period for other requests.</p>	<p><i>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 Act shall, without vitiating the evidence in any manner, remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India on its computer resource as far as possible immediately, but in no case later than:</i></p> <ul style="list-style-type: none"> <i>(i) 3 hours, in relation to acts that threaten the sovereignty and integrity of India, the security of the State,,</i> <i>(ii) 72 hours, in relation to acts that threaten friendly relations with foreign States, and public order, and</i> <i>(iii) 7 days, in relation to decency or morality, or in relation to contempt of court, defamation or incitement to an offence.</i>

Rule	Proposed change	Our suggestion/ industry feedback	Proposed edit to the Draft Rules
	<p><i>eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.</i></p>		
3(9)	<p><i>The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content</i></p>	<p>We would request that the platforms should not be required to proactively monitor. It would impose a high cost of doing business, especially for Indian startups. Typically large companies are better placed to meet the cost of compliance for such regulations.</p> <p>The current due diligence obligations under Rule 3(2) are sufficient to mandate a platform to take steps that ensure oversight for mis-information, impersonation, and terror related content. One approach could be by way of a guidance note, or a documentation of best practices to be followed by intermediaries to comply with Rule 3. This could help bring out the various practices that an intermediary could adopt to prevent the spread of mis-information and fake news across platforms.</p>	<p><i>Request to be removed from the Draft Rules.</i></p>

S.No	Ref. No.	Comments
1	MIT/79/001	<p>I'm an information security professional with more than 15+ years of experience. I have reviewed the bill and would like to offer the following feedback for your consideration.</p> <p>1) There is no penalty defined for non compliance. We routinely see and hear of data breaches, unauthorized access granted by intermediaries, sale of personal data, but no incident gets reported to CERT IN. While you have made it mandatory for the intermediary to inform CERT IN in point 3, subpoint 10, you have no where pointed out the penalties for non compliance. This needs to be documented clearly so that there is no room for ambiguity. A recent breach of Uber data including Indian customer data was penalized in France, but no report was filed in India. Similarly no penalty was levied or paid in India.</p> <p>2) There is no mandatory requirement for the intermediary conducting a periodic Vulnerability Assessment & Penetration testing. It is often seen that a 3rd party VAPT throws up several known vulnerabilities which are often otherwise unpatched. Request you to also cover that aspect by mandating all intermediaries to conduct an external VAPT at least annually and all Critical and High level vulnerabilities to be closed within a period of 2 weeks.</p> <p>Thank you,</p> <p>Wishing you all the very best,</p>
2	MIT/79/002	<p>Sir,</p> <p>I am Bingi. Vivek varun from hyderabad,composing this email to the response/ suggestions that meity is welcoming for IT(INTERMEDIARIES GUIDELINES (AMENDMENT)RULES)2018 regarding the social media networking sites or applications.</p> <p>I went through the guidelines mentioned in the "meity" website and my suggestion for the socialmedia networking sites is, "there should be a mark on the message mentioning the ORIGINATOR of the uploaded (picture or vedio) when he/she is uploading some content from his/her account just like a feature in WATSAPP APPLICATION which makes FORWARDED caption on the forwarded messages in that particular application".</p> <p>This makes to catch the ORIGINATOR of unlawfull content easily for the law enforcing agents and it will also makes people to think about the sharing or following such miscreants is not good for them.</p> <p>Hope this suggestion will make a positive step towards fulfilling the goal set by the government sir.</p>

S.No	Ref. No.	Comments
3	MIT/79/003	<p>In Rule 3 of the Draft Amendment Rules, the following clause to be added :-</p> <p>Neither to publish and circulate nor allow its platform for circulation of any video or a clip concerning any food article, which is based on non- verified information and/ or un-substantiated facts, with a tendency to create fear amongst public at large thus eroding the confidence and trust of people in the food control system and the food businesses.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
4	MIT/79/004	<p>Dear Sir,</p> <p>Please find my Comments / Suggestions below.</p> <p>Reference to Point 9</p> <p>(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content</p> <p>This should be limited to Social media platforms.</p> <p>There are hundreds of small web hosting companies hosting thousands of websites. It is practically not possible to manually scan each and every website. Additionally, there are no such automated tools available, which can identify unlawful information or content.</p> <p>Another question is, how does a Hosting company identify, if information is unlawful ? There needs to be a clear guidelines for the same.</p> <p>Such rules can easily be misused against smaller hosting companies.</p> <p>This will have negative impact on Web Hosting industry in India and it may lead to end of Hosting services in India all together.</p> <p>Government should provide proper guidelines and tools which can help Hosting Companies to scan all websites and identify unlawful contents.</p> <p>Reference to Point 4</p> <p>(4) The intermediary shall inform its users at least once every month, that in case of non- compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.</p>

S.No	Ref. No.	Comments
6	MIT/79/006	<p>Please find our Comments / suggestions (in red) on the Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018’</p> <p>Rule 3. Due diligence to be observed by intermediary;</p> <p>(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —</p> <p>(L) contains or promotes a hoax or fake news/information, with a malicious intention to deceive the public, knowingly.</p> <p>(4): The intermediary shall inform notify its users either on their website or through e-mail, messages etc. at least once every month, that in case of noncompliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove any noncompliant information or Data, without any further notice.</p> <p>(10) The intermediary shall report Cyber security incidents and also share Cyber security incidents related information with the Indian Computer Emergency Response Team within 72 hours of occurrence or identification of such Cyber security incidents.</p> <p>Yours Sincerely,</p> <p>Divya</p>

S.No	Ref. No.	Comments
7	MIT/79/007	<p>Further our note of January 2 on the Information Technology [Intermediaries Guidelines (Amendment) Rules, 2018, the Commonwealth Human Rights Initiative (CHRI) wishes to detail further on the proposed Bill.</p> <p>We hope your ministry will consider the widespread discussion and debate over the right to privacy, and worries of censorship and surveillance, that this draft has triggered. Freedom of Expression is an inviolable and essential part of democracy and is protected by the Constitution. We offer some recommendations for your consideration.</p> <p>Rule 3(2):</p> <p>This rule includes terms that are not defined under any existing law, such as “blasphemy”, “hateful”, “disparaging”. If these are to be retained in the law, we request that any ambiguity or scope for misinterpretation be removed by spelling them out with illustrative examples, as in Contract Act, 1872. The intermediary can then provide these to users as instructive examples and not as an exhaustive enumeration. Alternatively, we request that these terms be removed from the Rule.</p> <p>We recommend that the term “grossly harmful” be removed as it is too vague.</p> <p>We recommend that the term “otherwise unlawful in any manner whatsoever” be changed to “or constitutes an offence under any law” since minor violations should not be a factor to curb content dissemination.</p> <p>We recommend that the term “ethnically objectionable” be changed to “ethnically discriminatory” since ‘objectionable’ is, once again, a very subjective filter for content.</p> <p>Rule 3(5): We recommend that</p> <p>Every instance of the mention of “government agency” should be replaced with “independent investigative agency”.</p> <p>The definition clause should offer an exhaustive list of all agencies that can seek such information from intermediaries.</p> <p>The law should define legally justifiable grounds (such as those spelt out in Article 19(2) of the Constitution) for seeking user information.</p> <p>The law must put in place a Standard Operating Procedure (SOP) to guide independent investigative agencies in their investigation as stipulated under this Rule.</p>

S.No	Ref. No.	Comments
10	MIT/79/010	<p>Dear Sir/Madam</p> <p>There is ambiguity in the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 when it comes to the issue of the removal of objectionable content. First, subsection 8 says that the intermediary "shall remove or disable access to... unlawful acts" no later than 24 hours on receiving a court order or being notified by a government agency. Does this imply that an aggrieved person shall first need to file an official complaint about unlawful content and obtain a court order or have a case deemed suitable by the appropriate government agency for a takedown of content?</p> <p>Further, subsection 9 states that the intermediary shall take proactive steps with "technology-based automated tools" to identify and remove or disable public access to unlawful information or content. Does subsection 9 then indicate that the removal of unlawful content is a prerogative of the intermediary failure to fulfil which will be visited by legal action.</p> <p>Also confusing is the role of the Grievance Officer as stipulated by subsection 12. Specifically what kind of content can be flagged with the Grievance Officer? Also, if the Grievance Officer can receive complaints about unlawful/objectionable content, isn't the period of one month for redressing such complaints too long in social media terms? And, if the aggrieved party has to demand removal of content armed with a court order or complaint to a government agency wouldn't the process to obtain one lead to delays in targeting content on social media, defeating the purpose of guidelines to check unlawful content?</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Publishing Agency)

S.No	Ref. No.	Comments
13	MIT/79/013	<p>Dear Sir,</p> <p>I am very much concerned on the effect of the proposed intermediary policy on Web Hosting companies. especially point no 9 of due diligence.</p> <p>There are 100+ small web hosting companies operating in India, hosting thousands of websites.</p> <p>Web Hosting companies are not competent enough to develop technology to scan thousand of websites for content. Websites may use different languages and it is practically not possible for Web Hosting companies to take a decision, if content is unlawful or no.</p> <p>Any content monitoring and self censorship by Web Hosting companies, will lead to lose of customers to foreign providers eventually resulting in data moving out of India and publishing of content from outside India which is against interest of India.</p> <p>Any such move may also affect businesses of of Web hosting companies in India.</p> <p>All other points suggested in draft policies must be followed by Web Hosting companies, including blocking of content within 24 hours.</p> <p>I suggest that, Web Hosting companies should do KYC of every customers they host. This will ensure that, customers who host objectionable contents are traceable.</p> <p>Thank you.</p> <p>Bhavin Chandarana</p>

S.No	Ref. No.	Comments
15	MIT/79/015	<p>Hi,</p> <p>As an Indian Citizen, this is my response to the Section 79 of the Information Technology (IT) Act proposed by Government to proactively watch social media, messengers to prevent unlawful content.</p> <p>I'm Indian and hope I still live in a democratic country where free speech and privacy are fundamental human rights. But looks like central government doesn't like that anymore because privacy is empowering people rather than the ruling party. That is why in the name of security, terrorism, unlawful content (and blah blah..) government is trying to implement rules which enables surviellence on internet like China, Cuba and other dictatorship countries.</p> <p>More people are dying due to road accidents, pollution, murders, depression than terrorism and lynchings. We can clearly sense that the proposed rules are not to stop attacks but to surviell the entire country to sense the mood of people, journalists etc.</p> <p>Moreover proactive prevention doesn't work if that is really your intention. Bad guys like terrorists or corrupt politicians are always going to find a way to hide. It'll be the common people who will be subject to surviellence for no reason. Removing encryption and proactive censorship is no different than living in panopticon jail.</p> <p>This act undermines freedom of expression on social media platforms. As a citizen, I don't want to live in a country where surviellence is the norm and government has the power.</p>

S.No	Ref. No.	Comments
17	MIT/79/017	<p>Dear Sirs, As a resident citizen of India, I herewith submit my comments according to invitation on MEITY site, on the draft amendment to IT ACT via Intermediary Guidelines Rules 2018. Please record the comments as per procedure and evaluate them sincerely and lawfully under our constitutional rights and duties, before this draft is finalized.</p> <p>Comment #1. Is this going to an amendment to IT Act in 2011? If yes, they why is the word "Guidelines" used here. My Conclusion - This word should be dropped.</p> <p>Comment #2. In clause 2(c) there is a mixup between communication link and hyperlink. I do not see a need for this clause in this amendment or guidelines. Communication link is defined as - The means of connecting one location to another for the purpose of transmitting and receiving data. or see https://en.wikipedia.org/wiki/Telecommunications_link Hyperlink is defined as - a hyperlink, or simply a link, is a reference to data that the reader can directly follow either by clicking or tapping. A hyperlink points to a whole document or to a specific element within a document. My Conclusion - 2(c) should be deleted.</p> <p>Comment #3. Refer to Clause 3(4)(4) on page 3 (The intermediary shall inform its users at least once every month,). No users of internet or intermediaries anywhere in the world shall accept this nonsensical requirement of informing its users at least once every month. It is something that is meaningless. My Conclusion - This clause should be deleted forthright.</p>

S.No	Ref. No.	Comments
18	MIT/79/018	<p>#1: There is the large issue of end-to-end encryption that prevents most modern intermediaries to be able to look at the message content. Therefore, while the intermediary can publish in its EULA the conditions specified in sub section 2, given the current technology landscape, it is virtually impossible for most intermediaries to apply that. Additionally it becomes in direct contravention with privacy that these technology intermediaries promise, the expectations of their users, and is also mandated by law in various countries. Putting too much burden of monitoring could potentially make these platforms as infeasible businesses.</p> <p>#2: Items in sub section 2</p> <p>a) It is not quite clear as to which one relates to promulgation of fake news/rumors on the intermediary platform. Perhaps point f/g come closest but it is not entirely explicit. Additionally as being seen, especially in Indian social context, people don't often differentiate between "intermediary" and the "information carried by intermediary". For e.g. words like 'google', 'whatsapp' and 'facebook' have become synonymous with 'internet' and are treated as sources of information themselves instead of a mere aggregators/disseminators of information. This distinction can only come thru education and somewhat of a very specific notification on these platforms to the effect that the information/content on these platforms should not be blindly trusted and users should apply their diligence. This kind of notice should be in the localized languages as well.</p> <p>b) There are many clauses related to lifestyle choices e.g. promotion of intoxicating substances or ethnic sensitivities. What is the meaning of 'promotion'? Does it have a commercial connotation in-built? Additionally lifestyle choices and ethnic sensitivities vary from cultures and countries. Intermediaries operate in a border less world. So what is expected from an intermediary here?</p> <p>I understand that these are broad guidelines that an intermediary has to publish but since they can't implement any enforcement, the merit of such detailed and specific guidelines might become questionable.</p> <p>#3: Section 10 talks about reporting of the cyber security incidents. Is that related to the cyber fabric of India or does it need to be global in scope? For e.g. if whatsapp-US has a breach, does whatsapp-India need to report it? In my opinion yes, because the networks are inter-connected, unless localized storage of data is mandated.</p>

S.No	Ref. No.	Comments
19	MIT/79/019	<p>It is suggested that our focus should be on working closely with citizens in India to educate people about misinformation and help keep people safe.</p> <p>The law enforcement agencies in India along with social media platforms can create public awareness campaigns to prevent misuse of such apps.</p> <p>Moreover, if such regulations are to be brought in, a law for data protection on the lines of Justice BN Srikrishnacommitee recommendations should be a pre-requisite.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
(Published by MeitY)

SUBMISSION BY THE BOMBAY CHAMBER OF COMMERCE AND INDUSTRY

MIT/79/026

Please find below our comments on the Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (“**Draft Rules**”) issued by the Ministry of Electronics and Information Technology (“**MEITY**”) on December 24, 2018 for public comments.

S. No.	RELEVANT CLAUSE	CHANGE	RATIONALE
1.	General	To insert: “The Rules shall amend and replace in their entirety The Information Technology (Intermediaries Guidelines) Rules, 2011”	This is a clarificatory change.
2.	Commencement	To insert following in Short Title and Commencement: “These Rules shall be applicable in respect of information which is hosted, published or transmitted by an Intermediary on or after [●].”	<p>It is well established that legislation, particularly legislation with penal consequences cannot have retrospective effect.¹ The Draft Rules create substantial new obligations² on Intermediaries with respect to information dealt with by them.</p> <p>Accordingly consequences under the rules should be applicable in respect of such information only after their becoming operative.</p> <p>Further, given the potential complexity of complying with the requirements, particularly for smaller intermediaries, we would recommend that a lead in period (between enactment and operation) be considered to permit compliance by intermediaries with these requirements. By way of an example, intermediaries may need to change the underlying operating architecture of their websites or applications,</p>

¹ Article 20(1) of the Constitution of India; *Nayyar GP v State (Delhi Administration)* AIR 1979 SC 602; *Soni Devarajbhai Babubhai v State of Gujarat* AIR 1991 SC 2173.

² See Rule 3(7) below.

S. NO.	RELEVANT CLAUSE	CHANGE	RATIONALE
			in order to provide access to encrypted information.
3.	Rule 3 (5)	<p>When required by lawful order, the intermediary shall, within 72 hours of communication of such lawful order, provide such information or assistance as asked for by any government agency authorized to request such information for concerning security of the State or cyber security, or investigation or detection or prosecution or prevention of offence(s); <u>preserving the security of the State, protective or cyber security and or matters connected with or incidental thereto.</u> Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall, <u>provide all information within its possession,</u> to enable tracing out of such the originator of information on its platform as may be required by government agencies <u>making pursuant to such order.</u></p>	<p>It is well established the natural persons in India enjoy a fundamental Right to Privacy which can be infringed upon only when the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them,³ is met. Additionally, the law should be fair, just and reasonable.⁴</p> <p>Accordingly requests under this Rule should be made only if it is required for investigation, detection, prosecution or prevention of an offence and or for preserving the security of the state including cyber security in order to satisfy the ‘legitimate aim’ requirement. Further, such requests should be fair, just and reasonable.</p> <p>The proposed changes to the language clarify that any requests under this section will be consequent to a lawful order, and consequently, to the judicial review process averred to by the Hon’ble Supreme Court of India in the context of section 66A of the IT Act.⁵</p>

³ Justice K.S. Puttaswamy v Union of India WP Civil No. 494 of 2012 (Right to Privacy Judgment). See: Chandrachud, J. at page 264-265, Part T. In relevant part, “In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.”

⁴ Ibid.

⁵ Shreya Singhal v Union of India (UOI) AIR 2015 SC 1523.

S. NO.	RELEVANT CLAUSE	CHANGE	RATIONALE
			<p>Further, an intermediary is unlikely to be able to track the “originator” of each item of information on its platform. Accordingly, the language surrounding this requirement has been modified to refer to information within the intermediaries’ possession, and the origin of such information.</p> <p>Furthermore, the term ‘government agency’ should be defined and limited to certain key security agencies in order to prevent speculation, confusion and litigation on this issue. It may perhaps be limited to agencies notified under Section 69 of the IT Act.</p>
4.	Rule 3(7)	<p>“The Any intermediary who has more than fifty lakh users derives annual revenues in excess of [], whether directly or indirectly, from sales, advertising or operations targeted at users or Computer Resources in India, or [Insert alternative criteria] is in the list of intermediaries specifically notified by the government of India shall:</p> <p>(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;</p> <p><u>(i) have a duly incorporated or registered entity in India;</u></p> <p>(ii) have a permanent registered office in India with physical address; and</p> <p>(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 responsible for ensuring coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made with directions made in accordance with these Rules. in accordance with</p>	<p>The word ‘users’ as used in this definition has not been appropriately defined and may be interpreted in a variety of different ways ranging from one time users, to active users and revenue generating users.</p> <p>Additionally, the term ‘users’ may have no significance where the intermediary is providing infrastructure, carriage or services that do not require any registration. Indeed, it may be not be possible for any intermediary to determine the number of users arising from any location particularly where IP/MAC addresses are dynamic or relate to shared devices.</p> <p>More pertinently, a requirement for compliance based on the number of users may suffer from the mischief of arbitrariness, given that the number of users has no rational connection with the amount of information that</p>

S. No.	RELEVANT CLAUSE	CHANGE	RATIONALE
		<p>provisions of law or rules.”</p>	<p>may be dealt with by an intermediary. A user based requirement may also prompt intermediaries to reduce their non-revenue generating engagement with India. For instance, a platform for revenue free educational content may block access to Indian users to avoid having to set up operations in India.</p> <p><u>Perhaps exploring a revenue based threshold may form a more manageable and rational classification for this purpose. Accordingly, one has been suggested as it will provide a rational business nexus in India. Additionally, we are of the view that the term revenue is more ‘boundable’ as opposed to the term user provided of course, the method of calculation of revenue is clearly specified.</u></p> <p><u>Furthermore, we understand that there may be certain entities which may not be sufficiently covered by the revenue based threshold. However, for such entities, it is open to the government to resort to the second criteria and specifically notify such entities (especially if they have a significant presence in India).</u></p> <p>Similarly, it would be impossible for an intermediary to automatically become a company incorporated in India merely because a certain number of Indian users it to store or forward information. Given that the object sought to be achieved here is co-operation with Agencies pursuant to the Draft Rules, the provision has been modified accordingly.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S. No.	RELEVANT CLAUSE	CHANGE	RATIONALE
5.	Rule 3 (9)	The Intermediary shall deploy <u>suitable</u> technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively to identifying and removing or disabling public access to unlawful information or content which is, <u>to its actual knowledge, unlawful.</u>	<p>In <i>Shreya Singhal v Union of India</i>,⁶ the Hon'ble Supreme Court has read down the meaning of Section 79(3)(b) of the Information Technology Act, 2000 to mean that the “intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then expeditiously remove or disable access to that material.”</p> <p>Indeed, the Supreme Court observed that, “This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.”</p> <p>Accordingly, any requirement to identify and remove content must be limited only to situations where the intermediary has actual knowledge of the content being unlawful, pursuant to a court order.</p> <p>The language has been modified accordingly.</p> <p>Additionally, the nature of information that is removed</p>

⁶ *Shreya Singhal v Union of India* (UOI) AIR 2015 SC 1523; The Supreme Court opined that, “Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).”

S. NO.	RELEVANT CLAUSE	CHANGE	RATIONALE
			should be disclosed to ensure transparency in the process and to avoid a chilling effect on free speech.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

IBM Inputs to the Draft Intermediary Rules

<u>Existing Provision</u>	<u>Proposed Amendment</u>	<u>Recommendations /</u>
Rule 3, sub rule (2), sub rule 2(j) and 2(k) - Due diligence to be observed by intermediary	<p>“3. Due diligence to be observed by intermediary –</p> <p>(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that –</p> <p>(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p> <p>(k) threatens critical information infrastructure.”</p>	<p>There should be guidance on, or threshold for what would constitute ‘threatening’ to public health or a ‘promotion’ of tobacco products, to avoid situations of disputes and ambiguity.</p> <p>Recommend</p> <p>Above all, the intermediary should not be made legally liable to determine if certain content is or is not inappropriate or harmful. For instance, under the guidelines on tobacco products, there is a need for guidance on what constitutes “threatening”, to avoid ambiguity and unnecessary disputes. It must be noted that even today, many cigarette / tobacco and alcohol firms promote their products through various means and putting the burden on intermediaries to regulate this may be beyond the expertise of such intermediaries.</p>
Rule 3, sub rule (4)	<p>(4) The intermediary shall inform its users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.”</p>	<p>Frequent notification requirement in B2B scenarios (for example enterprise cloud service providers) can be tiresome and lead to fatigue. Enterprises have robust contract management processes, and it should not be mandated.</p> <p>Recommend</p> <p>Mandate to notify users monthly should be removed.</p>

Existing Provision	Proposed Amendment	Recommendations
Rule 3, sub rule (5)	<p>“(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.”</p>	<p>It is extremely important that the modalities of notification and what constitutes a legal and lawful request be unambiguously clarified. Without such details, corporates would find it difficult to offer necessary assistance, wherein what constitutes assistance will be linked to the request and change on a case to case basis.</p> <p>Any timelines for assistance is dependent on the nature of assistance sought and information available to start with, following a lawful request received. In addition, corporates require to review and assess their legal obligations under contract with users and may need clarifications from agencies. Therefore, the law should provide for flexibility in terms of timelines for response, based on factors such as technical feasibility and reasonableness. While corporates may acknowledge the request within a certain specified time, the actual time taken to share information, if possible, should be case dependent.</p> <p>There are certain cases for exemption and a one-size-fits-all approach cannot work for Intermediaries. For example,</p> <ul style="list-style-type: none"> • The Indian IT sector, who process data for global clients, there could be instances, where information is processed, but not retained in India, making it impossible to comply with requests for tracing originator of information etc. • Requirement on Intermediaries like Cloud Service Providers to trace originator or information could result in violation of contractual terms and conditions related to data privacy and access to Enterprise data. This can have a long-term impact on how India is perceived as a destination for Technology business operations. • It may be technically infeasible to access information sought from Cloud Service Providers who do not have access to the data customers place on their servers, and therefore will not be able to comply regardless of the time frame • On cloud, there is a possibility that the account owner is a re-seller or a provider of service and therefore such entities may be approached for compliance under the Act on these provisions, instead of the cloud service providers <p>Recommend</p> <ol style="list-style-type: none"> 1. Suitable exemptions be provided for a class of intermediaries such as cloud service providers under this provision. We also urge the Government to consider the impact of mandatory requirements of tracing the originator on privacy and contractual terms and agreements for entities like cloud service providers who operate in B2B scenario. The liabilities and obligations should remain vested with the party that has a direct relationship with the originator of the information, and the intermediary can provide information related to the entity it has a direct relationship with <p style="text-align: right;">.....contd</p>

<u>Existing Provision</u>	<u>Proposed Amendment</u>	<u>Recommendations</u>
		<p>2. We further recommend guidelines on process to be followed on receiving such requests be made available. It must be noted that there are already existing legal obligations, for instance, under the Code of Criminal Procedure, and hence it may not be necessary to introduce additional requirements in this manner. It is also suggested that the provisions related to law enforcement agencies be clarified; for instance, only officers above a certain rank may pass orders seeking assistance; there should be scope for appeal against such decision; the intermediary should be permitted to pass on the request to its own customer, who should be given an opportunity to comply/ appeal through means such as judicial review.</p> <p>3. We also recommend that the law enforcement agencies shall take appropriate measures to safeguard the commercial confidentiality of such information and keep confidential any information that is not necessary to be disclosed in the interests of effective law enforcement. There should be requirement that a very narrow interpretation be made of “necessary information”, and only information that is deemed necessary be sought.</p> <p>Finally, we believe that the privacy norms would be clearly laid down by the enactment of the Personal Data Protection Bill. And the Government may consider aligning the provisions suitably to avoid disruptions when the Bill is passed.</p>
Rule 3, sub rule (8)	<p>“(8) 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 the Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public</p>	<p>The proposed rules need to be modified to include safeguards for appeal and discussions to prevent misuse. For instance:</p> <ul style="list-style-type: none"> (a) Designate a single agency under the appropriate government, with technical as well as judicial expertise (b) Permit the originator/ custodian of the information an opportunity to appeal (c) Provide technical guidance on removing information “without vitiating the evidence”. (d) Consider that an intermediary, especially in the B2B or reseller context, may not be technically able to “disable” access, or can only disable such access if it also disables access to other legitimate and lawful users. <p>Recommend</p> <p>We recommend that the time limit to remove / disable access to content should be increased from current 24 hours. Instead, entities should be asked to acknowledge receipt of such request within 24 hours.</p> <p style="text-align: right;">.....contd.</p>

<u>Existing Provision</u>	<u>Proposed Amendment</u>	<u>Recommendations</u>
	<p>order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.”</p>	<p>We also recommend that an intermediary should be given a reasonable time to respond to any request under these Rules, and request reconsideration by the appropriate authorities under the following circumstances:</p> <p>(a) Technical feasibility.</p> <p>(b) the intermediary believes that the authorities should be making such request of another entity, and not the intermediary. A test of “appropriateness” should be followed, i.e., is the intermediary the most appropriate entity to which such a request should be made?</p> <p>(c) complying with the request could have adverse consequences or impact on other users, or may be disproportionate in respect to the rights of other users.</p> <p>(d) the request is overly broad, and seeks information that is disproportionate to that which is needed by the law enforcement agencies.</p> <p>A suitable authority with technical and/ or judicial expertise may be appointed to review such requests.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
(Published by MeitY)

<u>Existing Provision</u>	<u>Proposed Amendment</u>	<u>Recommendations</u>
<p>Rule 3, sub rule (9) – Due diligence to be observed by intermediary</p>	<p>“(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.”</p>	<p>Proposed monitoring and removal of information will impact privacy of clients. Proactive monitoring of content and removing them etc. goes against the principles of Intermediary, and the basis of safe harbour accorded to them. Further, for entities such as cloud service providers, deploying automated tools to monitor content, would be in complete violation of trust and contractual terms and conditions. Such requirements can vitiate the B2B environment of the IT sector in India.</p> <p>In addition, as cloud service providers, entities do not have access to the content, and therefore will not be in any position to filter it.</p> <p>Recommend</p> <p>This provision should be deleted. At the least, exemptions should be carved out for entities such as Cloud Service Providers etc wherein such monitoring is against the business model and places an undue burden on such entities. It is also submitted that Cloud Service Providers may not have the expertise to determine what constitutes problematic content.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY REGULATIONS, 2019
(Published by MeitY)

Concerns related to existing provisions that maybe considered to be amended

<u>Provision under existing Intermediary Rules, 2011</u>	<u>Recommendations</u>
<p>Rule 2 (f) – Definition of Cyber Security Incident</p> <p>"Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;</p>	<p>This is extremely broad and vague. A materiality threshold should be applied, basis standards and threshold that maybe notified.</p>
<p>Rule 3, sub-rule (3)</p> <p>The intermediary shall not knowingly host or publish any information.....</p>	<p>It is requested that this be clarified to state that the intermediary shall not host or publish such information, if it has been notified through court order/ by the appropriate government.</p> <p>It is also requested that the provisions related to "temporary" or "transient" storage be reviewed in the context of cloud service providers.</p>
<p>Rule 3, sub-rule (10)</p> <p>The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.</p>	<p>A materiality standard needs to be provided, otherwise this can become very subjective, and can lead to notification fatigue.</p>
<p>Rule 3, sub-rule (11)</p> <p>The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource...</p> <p>Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.</p>	<p>This can become very subjective, and can inhibit innovation, enhancements, etc.</p> <p>The words "sole purpose" are very vague and can lead to uncertainty. They should be deleted. An intermediary, especially a cloud service provider, should have freedom to innovate and make improvements, enhancements, etc. It is also submitted that there are other provisions related to tampering and hacking in the IT Act.</p>

S.No	Ref. No.	Comments
32	MIT/79/032	<p>I have the following suggestions to make on the draft as under :</p> <p>A) Para 3 (2) (a) of the draft amendment states :</p> <p>{(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that — (a) belongs to another person and to which the user does not have any right to;}</p> <p>This is very stringent and looks like an antithesis to the way FaceBook/ Youtube and many other digital platforms are used by wide spectrum of the society. The word 'belongs' may be changed to some expression which is more definitive to indicate legal ownership on the content.</p> <p>B) Para 5 of draft amendment</p> <p>I feel that the State should have the right to access digital materials stored or transmitted through a platform if there is sufficient and reasonable suspicion or apprehension that activities inimical to the State by way of violence, by way of money laundering are involved or an act which invades into the intimate privacy of a person. The cause of action leading to access should be clearly defined. With cursory browsing of IT Act 2000 I find that under Section 67 (2), as quoted below, controllers have the power to ask for decryption of contents:</p> <p>{ (2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.}</p> <p>Para (5) of the amended Rule further empowers legally authorised government agencies to ask for particulars of the originator of information on the platform among other information. This power to trace originator can collaterally lead to fear to express freely which is a legitimate freedom enshrined in the constitution. So the precise framework to determine a valid case to trace originator should be defined in the Rules. Para (5) of the draft has left it open for any one from government agency to ask for such information. Thus the authority which can ask for such information should be of sufficient seniority. There should also be a monthly review mechanism of all such cases relating to tracing the originator by a committee comprising of representatives of CIC and CVC as a mitigating mechanism.</p>

S.No	Ref. No.	Comments
38	MIT/79/038	<p>I would like to add following comments & suggestions to my earlier email related to intermediary guidelines.</p> <p>Intermediary as defined by IT act, covers Social media platforms, ISPs, Data Centres, Website owners and Web Hosts. Draft intermediary guidelines as proposed covers all intermediaries and it is not specific to any particular segment of intermediary.</p> <p>Proposed guidelines will have negative effect on Web Hosting companies in India without meeting the purpose of the guidelines. (Specific to Point # 9, Automated Tools).</p> <p>Technical Difficulties</p> <ul style="list-style-type: none"> - Although Web Hosting companies are considered tech companies, they are pure infrastructure provider and may not know technicality except server management. - Web Hosts are not competent enough to develop automated tools to detect unlawful contents. - There are no ready tools available for detection of unlawful contents which can be used by Web hosts. - Web Hosts do not have knowledge where website data is uploaded and how it is stored by website owners. - Website data can be in pure HTML files, images, videos or it could be in database. Data can also be encrypted. <p>There are encryption tools available (e.g. source guardian - which encrypts PHP files)</p> <p>These files do show up when you access via websites, however on server side, they remain encrypted. Hence it is practically not possible to scan contents.</p>

S.No	Ref. No.	Comments
47	MIT/79/047	<p>Our comments in respect of the Draft Information Technology (Intermediary guidelines Amendment Rules) 2018 are sent herewith.</p> <p>Comments on the Intermediaries Guidelines (Amendment) Rules 2018</p> <p>We would like to offer our comments on the Draft Intermediaries Guidelines (Amendment) Rules 2018.</p> <p>1. Section 3 (5) of the Draft Intermediaries Guidelines (Amendment) Rules 2018 provides as under:</p> <p>When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto</p> <p>Comments:</p>

MIT/79/066

Existing Provision of Law Information Technology (Intermediary Guidelines) Rules, 2011 (Intermediary Rules)	Proposed Amendment Information Technology [Intermediary Guidelines (Amendment) Rules, 2018 (Draft Amendment)	Recommendations / Suggestions including suggested modified version of the Clause	Rationale for Suggested Changes
Rule 2 – Definitions Sub-rule (e) – Definition of 'Critical Information Infrastructure'	Critical Information Infrastructure” means critical information infrastructure as defined in Explanation of sub-section (1) of section 70 of the Act;	Members have suggested to remove this clause	This definition is not necessary as we have recommended removing the reference to this phrase in Rule 3(2).
Rule 3, sub rule (2), sub rule 2(j) and 2(k) - Due diligence to be observed by intermediary	<p>“3. Due diligence to be observed by intermediary –</p> <p>(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that –</p> <p>(a) to (i) remain unchanged.</p> <p>(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) &</p>	Members have suggested to remove the additional content notices in Rule 3(2)(j) and (k)	<p>The additional content notices in Rule 3(2) should be deleted as the rule does not specifically define, or prescribe a threshold for what would constitute 'threatening' to public health or a 'promotion' of tobacco products or to 'critical information infrastructure'. It may also be noted that the definition of 'critical infrastructure in its present form is subject to capricious use and unguided discretion. In the Supreme Court of India's (Supreme Court) judgment in Shreya Singhal v. Union of India (Shreya Singhal), Section 66A was struck down for imposing vague restrictions on speech. Accordingly, the proposed additions to Rule 3(2) may also be considered as unreasonable restrictions on the right to free speech and expression.</p> <p>The additional content notices in Rule 3(2) also unlawfully discriminate between online and offline expression, contrary to the Shreya Singhal case, as presently content that “threatens public health or safety” or “threatens</p>

	<p>like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p> <p>(k) threatens critical information infrastructure.”</p>		<p>critical information infrastructure” has not been prohibited on any other forum. Only prohibiting online content which falls into these categories would constitute discrimination against online speech and expression which is impermissible.</p> <p>It is recommended that the words terms and conditions be retained in Rule 3 (2) as they would apply to users and their conduct in relation to online intermediaries. The privacy policy applies to intermediaries and their usage of user information, there fore its use in this context is misplaced. In any event, Rule 3(2)(e) provides that a user may not host, display, upload, modify, publish, transmit, update share any information that violates law, which adequately addresses the concerns underlying the insertion of Rule 3(2)(j)</p>
<p>Rule 3, sub rule (4)</p>	<p>(4) The intermediary shall inform its users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.”</p>	<p>“3. Due diligence to be observed by the intermediary –</p> <p>(4) The intermediary shall inform its users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer</p>	<p>This proposed amendment prescribes an onerous and unjustified obligation on intermediaries to inform its users about the possible termination of access or removal of content in case of users’ violation of the rules, regulations, user agreements and privacy policy, on an ongoing basis. As intermediaries already publish the above-mentioned documents containing this information, this amendment is not only unnecessary, but may also lead to notification fatigue among users if done on monthly basis.</p>

		<p>resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.</p>	
<p>Rule 3, sub rule (5)</p>	<p>“(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government</p>	<p>Members have suggested to remove the additional content</p>	<p>This provision should be deleted on the following grounds:</p> <ul style="list-style-type: none"> (i) The provision is ambiguous. It does not clearly define the scope ‘assistance’ that may be sought and the purpose thereof. The rule therefore expands the obligations of the intermediaries by citing grounds of security of the State and cyber security without precisely formulating the scope of the requirements under the provision. (ii) The Code of Criminal Procedure, 1973 already provides for a method to address requests for information made by law enforcement agencies to intermediaries. (iii) The strict timeline of 72 hours to provide such information or assistance is unreasonable, onerous and does not provide the intermediary an opportunity to review or seek hearing with appropriate agencies. (iv) This provision also creates a new mandatory obligation on intermediaries to trace the originator of information when requested by legally authorized



	<p>agencies who are legally authorised.”</p>	<p>PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018 (Published by MeitY)</p>	<p>government agencies. This provision is a violation of privacy of users (recognised in <i>KS Puttaswamy vs. Union of India</i>), and does not satisfy the triple test of legality, necessity and proportionality. Operationalising this provision also requires the adoption of technological measures that allow tracing and break encryption. Thus, the tracing obligation is not just difficult to implement, but may also be unconstitutional. This provision provides no procedural safeguards in order to prevent misuse or protect users’ fundamental rights.</p> <p>(v) Any provision mandating tracing of user or other information, will also need to be in harmony with the telecom licensing regime and the Telegraph Act, as it applies to ISPs. Further, given the prohibition against the deep packet inspection by the ISPs the proposed change will lead to conflict among laws.</p> <p>(vi) Such a requirement on Intermediaries like Cloud Service Providers, ISPs and TSPs when required by a government agency to furnish information, could result in violation of contractual terms and conditions related to data privacy and access to Enterprise data. This can have a long-term impact on how India is perceived as a destination for Technology business operations.</p> <p>(vii) It is also suggested, that the request for information or assistance by ‘any government agency’ can be mishandled or misuse without any procedural safeguards.</p>
--	--	--	--

			<p>(viii) There is an inconsistency in this provision, as the first part requires information and assistance to be provided to ‘any government agency’ whilst the latter part of the provision relates to government agencies who are ‘legally authorized.’</p>
<p>Rule 3, sub rule (7)</p>	<p>“(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:</p> <ul style="list-style-type: none"> (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.” 	<p>“The intermediary who has more than fifty lakh users in shall appoint a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.”</p>	<p>The proposed change requires significant additional costs and regulatory burden. This may prove to be a significant barrier to market entry and thereby compromise competition. The underlying success of the digital economy lies in its ability to significantly reduce costs on account of physical assets. Notably, the proposed amendment empowers the government to notify other intermediaries subject to these requirements. In the absence of any objective criteria this creates an arbitrary regulatory environment. It is therefore proposed that the local office and incorporation requirements be dispensed with.</p> <p>We recognise the law enforcement need for responsive intermediaries. It is proposed that this requirement will be met through a nodal officer designated in this behalf.</p>

<p>Rule 3, sub rule (8)</p>	<p>“(8) 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 the Act shall remove or disable access to that unlawful acts relating to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or</p>	<p>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 of a court order or a direction under Section 69A of any such information mentioned in sub-rule (2) above, shall act within thirty-six hours and where applicable work with user or owner of such information to disable such information that is contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days.</p>	<p>We believe that this provision should be modified so that it is in conformity with the Shreya Singhal judgment, based on the following deficiencies:</p> <p>The Supreme Court in Shreya Singhal’s Case has laid down that there are only two ways in which a blocking order may be passed: (i) by court order or (ii) under Section 69A and the Rules made thereunder. The Court also noted that Section 79 being an exemption provision is closely linked to Section 69A which provides for the offence. The law therefore requires that the procedural safeguards under Section 69A continue to be applicable. Consequential changes are therefore suggested.</p> <p>The Supreme Court has read down Section 79(3)(b) has been read down to require removal of content pursuant to a court order or notification of such order. This is based on the rationale that a court order is presumed to be issued after following due process. The proposed Rule 3(8) has no procedural safeguards that governs the blocking of content. Without such safeguards guiding the agencies to utilise the power provided under this provision, such provision is open to grave misuse. In other words, there is no remedy available for ensuring compliance with the requirements of Article 19(2).</p> <p>The proposed provision also extends the time period for which the associated data must be stored by an intermediary, and also allows this period to be further extended indefinitely. The obligation to preserve the</p>
-----------------------------	--	---	--



	<p>by government agencies who are lawfully authorised.”</p>		<p>information “for such longer period as may be required” is vague and has been formulated without sufficient safeguards. It is notable that such retention of data is likely to result in significant cost related burden for storage and maintenance of such data. Thus, we recommend that the time period mentioned in the Intermediary Rules be continued.</p>
--	---	--	---

**Additionally, please note that few of our members have divergent views on the same, and will be making their separate submission respectively*

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
89	MIT/79/089	<p>Dear Sir,</p> <p>I have gone through the draft thoroughly and really want to appreciate the action taken by MeitY for publishing the same for general comments/suggestions.</p> <p>In today's world of E-commerce and digitization there are thousands of cyber crimes happening each day and there is no direct authority to which we can report our grievances as most of the E- Commerce and Social media companies (Intermediaries) are based at foreign locations. So, I have a Suggestion that there shall be a reporting authority provided by the Intermediaries so that such grievances can be redressed at their level primarily and Intermediaries should have some responsibilities for the acts done through their websites.</p> <p>Thanks for giving the platform to share our comments, hope they will be of some use to the Government.</p> <p>Regards,</p> <p>CA Shubhi Trivedi Senior Associate</p> <p>Blue Consulting Pvt. Ltd.</p> <p>G-1 3rd Floor Sector-11 Noida -201301 India</p> <p>F&A Outsourcing Tax Compliances Internal Audit</p> <p>www.blueconsulting.co.in</p>

S.No	Ref. No.	Comments
90	MIT/79/090	<p>(i) Intermediary shall not provide access to its computer resource to other third parties, including users to eavesdrop, intercept, monitor, decrypt or place on surveillance any information available on its computer resource.</p> <p>(ii) The intermediary allowing sharing or forwarding of content posted on its platform shall appropriately facilitate its users to make an informed choice to do so to ensure compliance with provisions of sub rule 3(2) mentioned above.</p> <p>(iii) Failure to comply with provisions of Rule 3(7), 3(7A) and 3(7B) shall make intermediary liable for action under section 84B of the IT Act and blocking of the services of the intermediary.</p> <p>(iv) Whenever, existence of unlawful information on the platform of an intermediary is notified by an agency of the government, the intermediary shall use appropriate automated technological tools to remove copy of such information wherever it exists on its platform without resorting to manual screening of user content,</p> <p>(v) Intermediary shall deploy technology based monitors, filters, volunteers, trust groups, etc. for proactively identifying unlawful information as defined in 3(2) of the rules for its removal.</p>

S.No	Ref. No.	Comments
91	MIT/79/091	<p>Dear Sir/Madam,</p> <p>I recently read about the ban on e-cigarettes which came as a shock for me. I started smoking when I was 15 years old, and smoked 10 cigarettes a day for over two decades. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 3 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that these products be sold in India through government channels with zero online ads. This information being readily available for nonsmokers or kids is dangerous, but for those who are already smokers, this is a boon. The product has to be made available, but sold only through aadhaar verification or something like that. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p>

PUBLIC COMMENTS ON DRAFT INTERIMINARY GUIDELINES 2018
(Published by MIT)

S.No	Ref. No.	Comments
92	MIT/79/092	<p>Dear Sir/Madam,</p> <p>I reside in Chandigarh where I work as a Trainer with Tech Mahindra. I started smoking when I was 19 years old, and smoked 40 cigarettes a day for over two decades. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 4 months now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p> <p>Yours, Piyush Age - 31</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
93	MIT/79/093	<p>Dear Sir/Madam,</p> <p>I reside in Chandigarh where I work as an IT professional. I started smoking when I was 19 years old, and smoked 20 cigarettes a day for over 15 years. I tried every means possible to quit many times, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for more than 2 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p> <p>Yours sincerely,</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
94	MIT/79/094	<p>Dear Sir, This is regarding the section 3, subsection 2 item number j which reads as following.</p> <p>(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p> <p>I would like to share my experience.i have been smoking for 10 years and used to smoke around 30 cigarettes a day until january 2018 when i switched over to a vape kit . i started with eliquid with 9mg nicotine and current dropped it to zero nicotine. The idea behind vaping is to eventually get rid of the dependence of cigarettes while providing a safer alternative against cigarettes & sheesha (the high temperature burning in cigarettes is a danger). Electronic Nicotine Delivery System (ENDS) requires one to have abit of basic knowledge regarding safe temperatures of vaping ,quality of materials , types of eliquids and support groups with member who have gone on similar journeys have helped in gaining a lot of insight in quitting my nicotine dependance .I believe the scope of this proposal should be better defined to NOT effect support groups and people using ends as a smoking cessation method. I do agree as promoting of cigarettes is prohibited and the same logic applies however i strongly suggest protecting the rights of support groups and individuals who are trying to get rid of their dependence on cigarettes. I would advice amending the draft to "promotion for sales".</p>
95	MIT/79/095	<p>Hi, It's not good to banned vape information on web. Instead of regulate it as it can save millions of people life. And it will not harm tobacoo crop and farmers as nicotine need tobacoo plant to make</p>

S.No	Ref. No.	Comments
96	MIT/79/096	<p>Dear Sir/Madam,</p> <p>I reside in Mumbai where I work as a cinematographer . I started smoking when I was 21 years old, and smoked 20 cigarettes a day for over a decade. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 3 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
97	MIT/79/097	<p>Dear Sirs,</p> <p>I would like to offer my thoughts upon the new restrictions on information about ENDS (Which include vapes).</p> <p>I sincerely believe and urge you to reconsider this motion, even though it is based only on an advisory (one that the honourable High Court has decided invalid).</p> <p>ENDS are actually helping people quit the more harmful and toxic products like cigarettes. I would like to speak more about my own experiences, which have only been positive. I am a borderline diabetic patient and I used to smoke 20 cigarettes a day. After moving to vaping for 2 years, I have been able to lead a more enjoyable lifestyle, with more energy and my lungs are as clean as possible. My wife who developed respiratory problems because of second hand smoke feels much better after I have moved to vaping. This has helped me lead a better lifestyle overall and I would urge you to please take these factors into consideration and re evaluate the restrictions.</p> <p>I would further like to present a further few proofs that ENDS are more helpful than harmful via this link - http://vapeindia.org/research/</p> <p>Please, please reconsider our health and your restrictive motions.</p> <p>Thank you, Aryan "Where's your will to be weird?" - Jim Morrison</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
98	MIT/79/098	<p>Dear Sir/Madam,</p> <p>I reside in Mumbai where I work as a Marketing Professional. I started smoking when I was 8 years old, and smoked a packet of cigarettes a day for over 10 years. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I even went to a doctor for professional help which cost me a lot of money.</p> <p>I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online and sourcing from abroad.</p> <p>I have been away from cigarettes for 3 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke, nor do I need to be an outcast at gatherings. I've stopped smoking entirely, and I barely vape anymore because ITS POSSIBLE TO GET RID OF THE HABIT WITH A SAFER ALTERNATIVE.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole. I wouldn't be here if this information wasn't online.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p>

S.No	Ref. No.	Comments
99	MIT/79/099	<p>Dear Sir</p> <p>This is regarding the section 3, subsection 2 item number j which reads as following.</p> <p>(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;</p> <p>I would like to share my experience.</p> <p>i have been smoking for 10 years and used to smoke around 30 cigarettes a day until january 2018 when i switched over to a vape kit .</p> <p>i started with eliquid with 9mg nicotine and current dropped it to zero nicotine.</p> <p>The idea behind vaping is to eventually get rid of the dependence of cigarettes while providing a safer alternative against cigarettes & sheesha (the high temperature burning in cigarettes is a danger).</p> <p>Electronic Nicotine Delivery System (ENDS) requires one to have abit of basic knowledge regarding safe temperatures of vaping ,quality of materials , types of eliquids and support groups with member who have gone on similar journeys have helped in gaining a lot of insight in quitting my nicotine dependance .</p> <p>I believe the scope of this proposal should be better defined to NOT effect support groups and people using ends as a smoking cessation method.</p> <p>I do agree as promoting of cigarettes is prohibited and the same logic applies however i strongly suggest protecting the rights of support groups and individuals who are trying to get rid of their dependence on cigarettes.</p> <p>I would advice amending the draft to "promotion for sales ".</p>

S.No	Ref. No.	Comments
100	MIT/79/100	<p>Dear Minister</p> <p>I am sending this mail as my suggestion on the “ Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018”</p> <p>I humbly would urge you to exclude information related to vaping as if we see across the globe even the countries that aren’t democratic as our great nation is haven’t done so, a great deal of information regarding vaping is available on Public Health England’s official website as well to exemplify how it would make India look on a global platform.</p> <p>Also I would humbly say to you that screening of information in a democracy is a violation of our rights as citizens as the soul of a democracy is that the people decide what is good for them.</p> <p>Before anything just look at this please</p> <p>https://www.theguardian.com/society/2018/dec/28/vaping-is-95-safer-than-smoking-claims-public-health-england</p> <p>I suggest “Not restricting/screening/withholding any or all information on “vaping/vape/e-cigarette”.</p> <p>Thank You Yours Kindly A Voter -- Thanks & Regards</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
101	MIT/79/101	<p>Dear Sir/Madam,</p> <p>I reside in – where I work as a --. I started smoking when I was 15 years old, and smoked 20 cigarettes a day for over two decades. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 3 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2016
(Published by MeitY)

S.No	Ref. No.	Comments
102	MIT/79/102	<p>Dear Sir/Madam,</p> <p>I reside in Dehradun, Uttarakhand where I work as a restaurant owner. I started smoking when I was 17 years old, and smoked around 20 cigarettes a day for over 15 years. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 2 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p> <p>It is an earnest request to you as a citizen of this country to look into this seriously, regulations are required not banning. I do not want to start smoking again. I am attaching a link with the email, which has many studies showing how e-cigarettes are a better alternative to smoking:-</p> <p>http://vapeindia.org/research/?fbclid=IwAR0alt4bafI43nYXR56Sx9AaarQ0dXGwkjrY-t254Tc_nokYXFnlUM58meo&goal=0_79c75256d4-8de353826a-14394165&mc_cid=8de353826a&mc_eid=b598de2167</p>

S.No	Ref. No.	Comments
103	MIT/79/103	<p>Dear Sir/Madam,</p> <p>I am a resident of Malanchanivas Qtrs, Agartala Tripura, I had started smoking when i was 18 years old and i was addicted to cigarettes and there was not a single day i could pass without smoking at least 5-10 of them, i tried everyway to quit, going to the gym, abstinence, consulting doctors but nothing could ever keep me away from the evil of cigarette addiction, not even the utmost concern of my family members could keep me from smoking. Back in 2016, i had a friend who suggested me i start vaping, initially it was difficult for me to abstain from cigarettes but after a few weeks to months i kept reducing the amount of cigarettes till a day when i was smoking none, whenever i felt like smoking i just picked up my vape to satisfy my smoke cravings.</p> <p>Its been 1 year since i have completely stopped smoking and i couldn't be any more grateful, my stamina is at its peak and i do not cough at all, nor i have felt any shortness of breath.</p> <p>My family and my loved ones are really happy about the fact that now i look a lot more healthy and do not stink of smoke all the time.</p> <p>I really feel that vaping can similarly help a lot more people in a country where smoking is deteriorating the quality of life led by its people. and banning its sale can affect the public health only for the worse.</p> <p>The High court has only order an advisory restricting the sales as seen in here: https://www.thehindubusinessline.com/economy/policy/govt-restricts-import-of-e-cigarettes/article25850299.ece/amp/?__twitter_impression=true&fbclid=IwAR0MjEFRVzPMrWor5CwweCkZGxtPF0oR6GeCjYpm55OYoQeeoX-3KfRv_h4</p> <p>E-ciggerates have also proven to be lot more safer than smoking through numerous studies conducted by establishments like PHE, Royal college of physicians, a more detailed proof with all the articles can be found in the following link: http://vapeindia.org/research/?fbclid=IwAR3qoGVd68-BfSDYjGMDUi5sNfj4PCMaNfotBRkMJPSEIXM_RoFcqra6dhY</p>

S.No	Ref. No.	Comments
104	MIT/79/104	<p>Dear Sir/Madam,</p> <p>I reside in Delhi where I Work as a business man I started smoking when I was 17 years old, and smoked 20 cigarettes a day for over a decade. In last few years I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 1.5 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would therefore request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p> <p>Yours...</p>

S.No	Ref. No.	Comments
105	MIT/79/105	<p>Dear Respected officials, As a Indian citizen I am very displeased at the steps taken to ban ENDS. The ENDS cannot be banned with out any proof of harm or scientific study and merely on the basis of an advisory issued. The honourable High court has also commented the same and by Meity taking such a quick desicion for only a advisory notice. I would strongly recommend for the actual ban to be ratified first before banning content on the world wide web.</p> <p>When an office like yours holds the power to control the newest part of the country a step like this would only show that India is a 3rd world country. You should have a look at the below researches stating where certain countries are actually adopting ENDS to reduce their tobacco consumption by promoting ENDS why would our country want to ban it. Please find a few links below which help you in understanding what developed countries are doing. Instead of a complete ban I would suggest you to regulate the websites for age restrictions, you can also introduce adhar card or kyc registration for purchasing such products, but do not ban as most of the people who quit smoking now a days have only ENDS as their backbone, you would be invinting thousands, may be millions of indian citizens to go back to smoking by doing this.</p> <p>I would request your office from the bottom of my heart to not ban but to regulate sale of such products, being in the 21st century there are enough ways to curb rather than to deny. vaping is actually less harmful compared to smoking tobacco.</p> <p>Links for your referral:</p> <p>https://www.thehindubusinessline.com/economy/policy/govt-restricts-import-of-e-cigarettes/article25850299.ece/amp/?__twitter_impression=true&fbclid=IwAR2DIkJzdBn_HmFtwarzSEXn0zrKaVkJuna_S9YtHYaWODWDkCvDBFjZaWI</p> <p>A glossary attached below of all researches conducted.</p> <p>http://vapeindia.org/research/?fbclid=IwAR2I8yCWQ6j_iREzqhZ7ys0qU0R_IR_e-NcZqI4_cMLxKt6VQU-mmzbh2A</p>

S.No	Ref. No.	Comments
106	MIT/79/106	<p>Dear Sir/Madam,</p> <p>As a resident of this great country, I have always been interested in the civic process of governance. I am happy that departments like yours are putting out drafts for public commenting. This is of course, how good governments work. When I read this draft, I found myself wondering at certain points that directly impact my well being. This email is my way of participating. Please do read this and reconsider parts mentioned.</p> <p>I reside in Mumbai. I started smoking when I was 24 years old and smoked more than 20 cigarettes a day for more than 15 years. I tried every means possible to quit, including cold turkey, using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for a year and some months now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I am much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes to their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>I would, therefore, request you to seriously reconsider the proposal to ban vape information online as many people these days get their information from online sources. If need be, some guidelines can be issued for disseminating this information which has the potential to save many lives in our country.</p>

S.No	Ref. No.	Comments
107	MIT/79/107	<p>Dear Sir/Madam,</p> <p>I am a Swiss citizen and OCI holder living in Goa with my family (wife and 2 small kids). I work as a translator for Zee TV and pay my taxes in India.</p> <p>I smoked 20 to 30 cigarettes a day for more than 20 years and shifted to vaping last February in 1 hour. I successfully quit smoking thanks to vaping which I learnt about while researching online.</p> <p>I did not smoke cigarette since 2nd February 2018 and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier and I did not visit any doctor since then. When I was smoking, I would need to go and see a doctor every 3 to 4 months to treat a chronicle bronchitis.</p> <p>My family members (my wife and my 2 sons of 3 and 8 years old) are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>In my opinion, it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p> <p>In case you would like to check the latest scientific studies and articles, most of them can be found on: http://helveticvape.ch/ressources/litterature-scientifique/</p> <p>Countries like UK and Switzerland (for example) are encouraging their citizens addicted to smoking to shift to a safer alternative even by offering them a free electronic cigarette in the case of Switzerland. http://helveticvape.ch/un-premier-programme-daide-a-larret-tabagique-integrant-le-vapotage-en-suisse/</p> <p>I have attached to this email, for your perusal, a small document in which you can read quotations of different reliable and trustworthy scientific associations which state that vaping is much safer than cigarette smoking.</p>

S.No	Ref. No.	Comments
108	MIT/79/108	<p>Dear Sir/Madam,</p> <p>I reside in Pune where I work as a Software Developer. I started smoking when I was 25 years old, and smoked 20 cigarettes a day for over two decades. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I was away from cigarettes for few months and my health had improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>Unfortunately I lapsed due to lack of e-cigarettes in India and could not go away from smoking. Now I am trying to get back to vaping again. I understand that there is a risk of delivering higher than intended nicotine content through ENDS, but so is the risk with any hazardous material and should not be taken as a reason to ban such devices, especially when they are moving my lungs away from tar to vapor</p> <p>Some links to research on vaping: http://vapeindia.org/research/?fbclid=IwAR0alt4baf143nYXR56Sx9AaarQ0dXGwkjrY-t254Tc_nokYXFnIUM58meo&goal=0_eb3212d8c9-84a7890c1d-68327281&mc_cid=84a7890c1d&mc_eid=f57bdb5f5d</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p>

S.No	Ref. No.	Comments
109	MIT/79/109	<p>Dear Sir/Madam,</p> <p>I have been smoking cigarettes since 2008 and have successfully been able to kick the habit since 6 months now after choosing ENDS. I was unsuccessful in past using other alternate therapies like nicotine gums and going cold turkey. None of them actually helped me to stay away from it. ENDS actually is helping me reducing down my nicotine urges by mindfully reducing the nicotine content in the same gradually also giving me a feeling of smoking a cigarette which is a paramount reason why smokers end up smoking again after quitting.</p> <p>The information over various hardwares and also choosing the right amount of nicotine was only possible through various websites and groups. The whole community is supportive as they are empathetic towards our condition as they also went through the same.</p> <p>Now as per new Information technology {Intermediaries Guidelines (Amendment) Rules} 2018 published dated 24/12/2018 encompasses all e-cigarettes and vapes under ENDS category.</p> <p>now if by any chance this draft is coming into force, we as a citizen who are trying our best to stay away from such deadly habit will lose one sure shot method of quitting it altogether.</p> <p>Going by the population of india and also the percentage of smokers, i really hope government should regulate the use and sell of Vapes and e-cigarettes instead of right away labelling it evil and banning it altogether.</p> <p>There are various studies across health care communities across the world showing results that ENDS are 95% safer than actual cigarettes and are efficient in kicking off the habit. Recent being the Public Health England and Royal College of Physicians.</p> <p>Collective good of citizens who can be safeguarded by such alternatives by available information on social media as well as support from experienced users cannot be undermined by rumour or perception of few individuals deeming it evil or as a health hazard.</p> <p>I would request to remove the ENDS clause from this draft for better good of huge public and request government to see the better prospects of this alternative and rather regulate instead banning the whole concept of it.</p>

S.No	Ref. No.	Comments
110	MIT/79/110	<p>Dear Sir/Madam,</p> <p>I have been smoking cigarettes since 2008 and have successfully been able to kick the habit since 6 months now after choosing ENDS. I was unsuccessful in past using other alternate therapies like nicotine gums and going cold turkey. None of them actually helped me to stay away from it. ENDS actually is helping me reducing down my nicotine urges by mindfully reducing the nicotine content in the same gradually also giving me a feeling of smoking a cigarette which is a paramount reason why smokers end up smoking again after quitting.</p> <p>The information over various hardwares and also choosing the right amount of nicotine was only possible through various websites and groups. The whole community is supportive as they are empathetic towards our condition as they also went through the same.</p> <p>Now as per new Information technology {Intermediaries Guidelines (Amendment) Rules} 2018 published dated 24/12/2018 encompasses all e-cigarettes and vapes under ENDS category.</p> <p>now if by any chance this draft is coming into force, we as a citizen who are trying our best to stay away from such deadly habit will lose one sure shot method of quitting it altogether.</p> <p>Going by the population of india and also the percentage of smokers, i really hope government should regulate the use and sell of Vapes and e-cigarettes instead of right away labelling it evil and banning it altogether.</p> <p>There are various studies across health care communities across the world showing results that ENDS are 95% safer than actual cigarettes and are efficient in kicking off the habit. Recent being the Public Health England and Royal College of Physicians.</p> <p>Collective good of citizens who can be safeguarded by such alternatives by available information on social media as well as support from experienced users cannot be undermined by rumour or perception of few individuals deeming it evil or as a health hazard.</p> <p>I would request to remove the ENDS clause from this draft for better good of huge public and request government to see the better prospects of this alternative and rather regulate instead banning the whole concept of it.</p>

S.No	Ref. No.	Comments
111	MIT/79/111	<p>Dear Sir/Madam,</p> <p>I am Siddhant Singh from Dehradun and i work for a bank in Dehradun as a Manager. I was a smoker for 10 years and i use to have 20_30 cigarettes a day for almost a decade. I used to feel very bad but was unable to stay away from the same due to the addiction. I had tried to quit cigarettes a lot many times using herbal medicines, nicotine gums, excessive caffeine but nothing would help me quit for a long time. My chest used to pain in mornings, i had severe smokers cough and gained excessive weight due to lack of stamina for physical activity.</p> <p>2. 1.5 years ago i came across E-cigs/Vape through an online advertisement and at that time i was in a state where i would try anything to quit smoking. I tried vaping and it changed the way i used to live. From the last 1.5 year i have quit cigarettes completely, and my chest pain and cough is gone. I feel much better during any physical activity. Sir, vaping in India has just started, while cigarettes are available at every nook and corner which make cigarettes a very easy solution for fixing nivotine cravings.</p> <p>3. A ban online information will hurt any new persons chances of quitting cigarettes like me and either the person will keep smoking or will be misinformed by petty sellers regarding Ecigs.</p> <p>4. Sir, these guidelines banning information on the internet regarding Ecigs will affect millions of smokers who want to quit as well as people like me who have already quit and due to lack of availability of Ecigs online will get back to cigarettes.</p> <p>5. While this may cross one's mind that why dont you just quit instead of starting something new, i assure you sir, for some people it can be very difficult to quit cigarettes. And after switching to vape i can feel benefits in my health like clear throat, no coughing, no pain etc</p> <p>6. Sir, i request you to kindly not ban vape related information online, and insted regulate the same. Sir , it really affects a lot of people who have actually quit cigarettes, chose to vape and are living a happy life.</p>

S.No	Ref. No.	Comments
112	MIT/79/112	<p>Hi</p> <p>I am writing with reference to proposed amendments to IT Rules which disables general public from information related to ENDS (Electronic Nicotine Delivery System) .</p> <p>I have been tobacco smoker for 20 yrs, and it was hard for me to quit smoking until while researching on smoking cessation I came across information about electronic cigarettes. E-Cigarettes have helped me to quit smoking tobacco.</p> <p>There has been many research conducted across various prestigious institute which claims e-cigarettes are far less harmful than smoking tobacco cigarette. I am sure you already must have received such references from many people who advocate for e-cigarettes as smoking cessation tool.</p> <p>I hereby OPPOSE the amendment related to ENDS which disables individual of healthier alternative to smoking.</p> <p>Regards</p> <p>Yogesh Tarve</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018
(Published by MeitY)

S.No	Ref. No.	Comments
113	MIT/79/113	<p>Dear Sirs</p> <p>The latest IT Act amendment to ban publishing of any information related to electronic nicotine delivery systems (ENDS), stating that it threatens public health and safety, is a severe step towards restricting an individual's access to information. The amendment is part of the measures proposed by the Centre to curb fake news and includes monitoring the online activity Indian citizens.</p> <p>From Alcohol to TV programmes and social media, bans have been imposed in India based on the premise that conscience of the general public is influenced by such decisions. On the contrary, a blanket ban is curbing democracy and the constitutional rights of citizens. They are based on the flawed premise that by closing our minds we can resolve a problem. The more the political anxiety surrounding an issue, the more is the propensity to ban. ENDS serves as a cessation aid to help an ardent smoker and should surely not fall in list as other items prohibited such as alcohol.</p> <p>Nearly 7 out of every 10 smokers say they want to stop smoking due to its harmful health impacts. People have started to gradually shift from traditional cigarettes to electronic cigarettes, also known as vapes. Not only does it act as a substitute to many of the physical, psychological and socio-cultural elements of cigarette smoking, but is also convenient and cheaper than smoking, making it a promising tool for switching with less harm.</p> <p>India being the world's biggest democracy should provide its citizens with the basic right to access information online, especially in the health and quality of life domain. We need to encourage an open society which can debate and discuss the advantages and disadvantages of various choices available to them.</p> <p>In that context, it is important that this inclusion of ENDS is not taken forward. I would request you to suitably amend Clause 2(j): "products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder";</p>

S.No	Ref. No.	Comments
114	MIT/79/114	<p>Sirs,</p> <p>Proposed ban on Electronic Nicotine Delivery System (ENDS) advertising and its information being available online to public denoting it threatens public health and safety seems unsubstantiated and hasty. ENDS heats a solution to create an aerosol, which usually contains flavours such as vanilla or mint. It is available in many forms such as e-cigarettes and vapes. E-cigarettes however do not burn or use tobacco leaves, but instead vaporises a solution, which the user then inhales. Globally, researchers and people consider it as a substitute considering it helps smoker escape the harmful habit that has grave effects on their body.</p> <p>Nicotine or ENDS device have not been notified as a drug by the Central Government. However, the only type of nicotine that is regulated (and provided certain exemptions) under the Drugs Act is nicotine gum and lozenges containing up to 2 mg/4 mg of nicotine. The rationale for including this category of nicotine within the purview of the Drugs Act is that nicotine gum and lozenges are used in replacement therapy as a substitute for smoking cigarettes. Further, from the information available on the official website of the Central Drugs Standards Control Organization, it appears that nicotine transdermal patch is an approved new drug. Its time the government promotes sharing of information rather than creating hurdles for its citizens to take their owned judged decision. In short, E-cigarettes/ENDS are not covered under the definition of the term 'drug' and therefore do not come under the purview of Drugs and Cosmetics Act, 1940. E-cigarettes therefore cannot be regulated under the provisions of the said Act.</p> <p>regards</p>

PUBLIC COMMENTS ON DRAFT INTERIM GUIDELINES 2016
(Published by MeitY)

S.No	Ref. No.	Comments
115	MIT/79/115	<p>Dear Minister</p> <p>The planned amendment to the IT Act prohibits publishing of any information on Electronic Nicotine Delivery System (ENDS), citing that it threatens public health or safety, specifically mentioning tobacco products, intoxicants including alcohol and also ENDS, is a hollow approach by the regulatory and advisory board. The world over, health and government bodies have promoted use of ENDS in comparison to traditional cigarettes. Many believe that an ideal situation would be to ban all harmful substances and there should be no choice between good or bad.</p> <p>In a way, the government's decision to further curb ENDS will only end up helping large cigarette companies. While Punjab, Haryana and the Union Territory of Chandigarh have declared e-cigarettes and ENDS "poison," entailing a ban on their manufacture and sale under the Drugs and Cosmetics Act of 1940, other states such as Karnataka, Bihar, Kerala, Mizoram, Maharashtra and Jammu and Kashmir have issued "necessary orders banning the manufacture, distribution and sale of e-cigarettes as unapproved drug. The advisory cites 30 countries where the sale of ENDS is banned, however, conveniently excludes the fact that many western countries like US and UK, amongst 60+ other countries allows the use of ENDS in a regulated manner.</p> <p>It's time the Union government takes a scientific view to the matter rather than supporting scaremongering among public.</p>

S.No	Ref. No.	Comments
116	MIT/79/116	<p>this is ashish gupta from gurgaon, haryana. i am writing this email as i came to know about the proposed ban on information on eciggs and vaping.</p> <p>sir, i started smoking at the age of 14 back in 1987 and had been a chain smoker for almost 3 decades (smoking 25-35 sticks a day)</p> <p>while, i appreciate all that our government has done to discourage smoking, it was still hard for me to quit smoking. in fact it was so bad that i even smoked when my wife was pregnant, in an closed environment, with the air conditioning on. this eventually made my wife a asthma patient and even then i just couldn't quit. the guilt was extruding and as a result i tried every trick in the book, from gum to patches. i even tried riekly and acupressure but nothing worked more than a couple of hours/days. it became so bad that even my kids gave up on me after fighting with me for a good 15 years.</p> <p>my health was deteriorating like anything. i couldn't climb the steps of my own house without panting and was coughing all the time. some really weird kind of stuff had started to come out of my lungs while coughing and it actually became quiet scary, my grand father and my biological father both had died of cancer and i had resigned to the fact that i will share their fate.</p> <p>then i fine day, while shopping with my wife at a mall, i told her that i was going to step out for a smoke. she gave me that resigned look which only a loved one can who is worrying sick about you. the shopkeeper there saw it all and suggested that i smoke in his shop right there in the mall. i was dumbfounded as to why and how someone can allow something like that.</p> <p>while smoking that last cigratte, we (i and that saree shop owner) got talking and he suggested i try something that he had used to quit smoking himself.</p> <p>i was very convinced that there cant be anything that could really quit me to smoking but out of respect for his concern and gesture (he had actual allowed me to smoke in HIS SHOP) i decided to give it a shot..... after a single drag i was sold.</p> <p>this was 3 years back and i haven't smoked one single ciggrate since. it ain't that i have become a marathon runner or anything, but i don't pant so easily now. my coughing has stopped. the scary stuff out of my lungs has definitely ceased. and most importantly my wife doesn't need to take the asthma inhaler that she always had to carry, although i still vape in enclosed spaces (air conditioned car and room).</p>

S.No	Ref. No.	Comments
117	MIT/79/117	<p>Dear Sir/Madam,</p> <p>I reside in New Delhi where I have my own business,I started smoking when I was 15 years old, and smoked 20 cigarettes a day for over two decades. I tried every means possible to quit, including using nicotine gums/patches, medicines and Ayurveda, but could not stay quit for long. I could finally quit when I switched to vaping (e-cigarettes), which I learnt about while researching online.</p> <p>I have been away from cigarettes for 5 years now and my health has improved significantly. I can do physical activity without tiring quickly, my taste is back and I feel much healthier. Even my family members are happier as the house does not stink of smoke and they are exposed to negligible harm than passive smoking.</p> <p>I feel it is important that more and more people learn about safer alternatives to smoking and can bring positive changes in their lives. By banning online information on these alternatives, there are greater chances of misinformation spreading about these devices, which will end up harming the society as a whole.</p>
118	MIT/79/118	<p>Dear Sir/Madam,</p> <p>This is in regards to the draft IT bill to ban 'Vaping' contents online.</p> <p>Please do not ban the online content which informs smokers about alternate available to them for quitting smoking through vaping. If required, only get some 'Statutory Warning/Disclaimer' added.</p>

S.No	Ref. No.	Comments
119	MIT/79/119	<p>To whomever it may concern,</p> <p>I want to share my viewpoint on ENDS (Electronic Nicotine Delivery Systems) and vaping and how this has helped me. The sale and use of these products and related products should be promoted online and in fact should NOT be banned.</p> <p>I used to smoke a pack of cigarettes a day everyday for the past 8 years. Recently I traveled to the UK and learned about ENDS and vaporizers. I thought I would give it a try and ever since there was no going back to cigarettes. Vaping has helped me improve my health. I used to suffer from regular sinusitis due the excessive cigarette smoking although ever since I switched to vaping by sinus problems have disappeared. I would definitely encourage the use ENDS/vaporizers and related products to anyone around me to help quit smoking.</p> <p>E-juices or otherwise known as vaporizer liquid is a more safer alternative to tobacco, the primary cause of cancer in our country. E-juices are much safer compared to conventional cigarettes which due to the combustion process, release carbon monoxide, carbon dioxide, Tar and several other harmful chemicals when inhaled. E-juices on the other hand vaporize a nicotine based liquid thus eliminating the combustion process and thus proving to be a safer alternative.</p> <p>I would request the Ministry of Electronics & Information Technology, Government of India to allow the sale of ENDS and related products online. This would help me and other people like me to switch to safer alternatives to smoking. A ban on the sale of these products would deprive the general public of these safer alternatives and would thus lead to more health concerns and deaths related to the use of tobacco in the country. Together with your support we could take a stand on promoting safer alternatives to the people of this country.</p> <p>More information on ENDS/E-cigarettes and related products -</p> <p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p>

S.No	Ref. No.	Comments
120	MIT/79/120	<p>I would like to express my deep sadness on the bill for banning 'ENDS'. I personally have been vaping for 4 years now and have not seen a single negative effect on my body. Instead, my overall health has improved and I can workout much better at the gym. Just because regular measures haven't been brought up in time for 'ENDS' doesn't mean that you ban them.</p> <p>Studies have shown 'ENDS' to be 95% safer than cigarettes, if anything you should ban cigarettes and not 'ENDS' which are helping people lead a healthier life. Many of my friends, who I introduced to 'ENDS' have stopped smoking cigarettes and can feel a positive impact on their health. Even countries like EU and US have legalised 'ENDS' and not banned them.</p> <p>Passing of this bill will prevent me from leading a healthy lifestyle and will add to the cause of me going back to cigarette smoking. Kindly reconsider.</p>
121	MIT/79/121	<p>Dear sir,</p> <p>Being a final year law student and someone who use to smoke those pathetic cancer causing cigarettes and switching to vaping , that vaping is a much safer alternative. there has been N number of studies showing vaping is 95% safer and UK have adopted laws regulating it properly. Hope you don't ruin our freedom to vape and let cigarettes still be available . As thousands of people will switch to smoking .</p>
122	MIT/79/122	<p>Dear it ministry</p> <p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accept the device as a harm reduction tool that helps people quit smoking tobacco and move on to a</p>

S.No	Ref. No.	Comments
123	MIT/79/123	<p>Dear All,</p> <p>This is to bring to notice of how shifting to Vape has enhanced my health to getting better than if I was smoking cigarettes.</p> <ul style="list-style-type: none"> - Vape being vapours and not smoke has helped me in relieving breathing issues. Feel much lighter Vaping than taking in smoke. Also no tar is accumulated in my lungs. - Reduce intake of nicotine, I used to be a chain smoker thankfully with Vape my habits have improved. - Due to excessive smoking my stamina for running and doing activities decreased, after switching to Vape I can now get back to doing activities at a much better level. - Vape has also cause good positive changes on my skin since there are no carcinogenic susbtance present which are there in cigarettes. - Also I don't have to worry about bad odour which comes after smoking cigarettes. <p>This is a humble request to make Vape legal and available for people who want to quit smoking. Please consider the health benefits of shifting to Vape and not the profitability in selling cigarettes.</p>
124	MIT/79/124	<p>sir/madam</p> <p>I just came to know about our Indian government is planning a ban on selling / buying / import / consumption of electronic nicotine delivery system. Which is very much legal in all over EUROPE & UNITED STATES OF AMERICA and in more then 100 countries .</p> <p>There is a proper tax on e cigs in all countries.</p> <p>Its 95% healthier the regular tobacco cigarettes.</p> <p>Every citizen has a right to select a better ...healthier alternative of smoking.</p> <p>Most important thing to be noticed is there is no ban on regular cigarettes sply when its causing cancer 100% . Then why govt is not banning the traditional tobacco ciggerets.</p> <p>In England the govt of u.k is suggesting there citizens to switch to vaping and quit smoking regular cigarettes as it causes cancer and electronic cigarettes are 95% safer. We have many proof to suggest the same.</p> <p>Company's like Indian tobacco company (I.T.C)</p> <p>Are working against the vaping culture in India..they loosing money and customers because of electronic ciggerets. Every person has a right to decide and I strongly suggest Indian govt should not ban this ...India government should make some laws to regulate the sale and purchase and import of these products.</p>

S.No	Ref. No.	Comments
125	MIT/79/125	<p>Hello,</p> <p>ENDS or Vapes have done more good than harm! It has helped me and many others switch to a healthier lifestyle.</p> <p>The inclusion of ENDS or E-Cigarettes in the proposed amendment to the IT Act, which prohibits publishing online information about these products is surprising.</p> <p>Electronic Nicotine Delivery Systems (ENDS) include various types of e-cigarettes, e-hookahs, and vapes which deliver nicotine without some of the known harmful carcinogenic substance from cigarettes containing tobacco. Most reviews of clinical evidence show that the chemicals found in e-cigarettes are far fewer and well below levels in comparison to smoking cigarettes.</p> <p>In a country like India, where there are so many tobacco users, there is an enormous potential for risk reduction by substituting cigarettes with less hazardous products.</p> <p>India is the second largest consumer of tobacco worldwide with nearly 12cr smokers, almost 9 lakh of whom die every year from smoking related diseases. Rather than solving the problem on the grassroots level, the government is incorrectly banning information sharing on ENDS. They should in fact, popularise the idea that e-cigarette are a safer alternative, as this may be a key way to reduce harm for nicotine addicts.</p> <p>In July 2016, Public Health England and eleven other UK public health organisations, including British Lung Foundation, Cancer Research UK, Royal Society for Public Health and Royal College of Physicians, issued a joint statement stating that “the public health opportunity is in helping smokers to quit, so we may encourage smokers to try vaping”. Earlier in 2017, researchers at University College London also reported e-cigarette use has been one of the primary factors in helping the United Kingdom attain higher smoking-cessation rates.</p> <p>India should also adopt a scientific approach to this new technology, rather than comparing ENDS with traditional smoking</p>

S.No	Ref. No.	Comments
126	MIT/79/126	<p>Dear Sir/Maa'm,</p> <p>The Ministry of Electronics and Information Technology (MEITY) proposed amendment to the Information Technology (Intermediary Guidelines) Rules 2018, banning the advertisement or publishing of any online information on ENDS/ E-Cigarettes is a step in the wrong direction. And one that the Ministry does not even have the jurisdiction to go ahead with, given that the matter is subjudice. Furthermore, the court has declared in the recent ruling that the advisory is not binding on states. There is also written evidence that ENDS does not fall under the jurisdiction of the Drugs & Cosmetics Act.</p> <p>It is an established fact that the use of ENDS or Vaping has significantly less health and safety concerns compared to high risk associated with conventional cigarettes, endorsed by the governments of 65 nations across the world such as EU, UK, US and Canada, as well as by credible institutions such as the Public Health England, American Cancer Society and the US Food and Drug Administration (FDA).</p> <p>Electronic Nicotine Delivery Systems (ENDS) include various types of e-cigarettes, also known as vapes which deliver nicotine without the harmful chemicals and compounds found in cigarette smoke. E-cigarettes have emerged as a promising avenue for people who want to quit smoking and has the ability to provide a means to compete with or even replace cigarette use, and has the potential of saving millions of lives.</p> <p>India has more than 100 million adult smokers and around a million people die due to tobacco related diseases annually. Unless the sale of tobacco products is regulated or completely restricted, the restrictions imposed on promotion and sale of ENDS would only further aggravate the health hazards. The MeitY would do well to first understand the facts and then move ahead with any policy decisions.</p> <p>Request you to kindly review unbiased proof and all legal due diligence before taking any step. Information on the 'less harmful' aspects of ENDS should in fact be widely promoted to adult smokers, like how it is being done in UK, New Zealand and other progressive countries.</p>

S.No	Ref. No.	Comments
127	MIT/79/127	<p>Hello Sir(s),</p> <p>I've been without a cigarette since last 3-4 years, my lung function has been improved drastically, running, climbing stairs etc, everything has gone better significantly, I don't have smokers cough anymore. All thanks to Vaping/ENDS.</p> <p>However Sir, honestly, Govt stance about ENDS is making me feel scared. Do you want people like us to switch back to smoking? Or, to use NRTs like nicotine patch, nicotine gum etc, that most of us tried in the past and failed miserably?</p> <p>The restrictions proposed to the IT Act, stating “intermediaries” should ensure they do not publish information on anything that threatens public health or safety specifically mentioning tobacco products, intoxicants including alcohol and also ENDS (Electronic Nicotine Delivery Systems), is a surprising restraint on E-cigarettes. Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p> <p>My only request to you, is to please consider the overwhelming evidence from multiple scientific bodies which clearly establish the fact that Vaping is significantly safer than smoking and help India to throw that cigarette butt.</p>

S.No	Ref. No.	Comments
128	MIT/79/128	<p>The Ministry of Electronics and Information Technology (MEITY) proposed amendment to the Information Technology (Intermediary Guidelines) Rules 2018, banning the advertisement or publishing of any online information on ENDS/ E-Cigarettes is a step in the wrong direction. And one that the Ministry does not even have the jurisdiction to go ahead with, given that the matter is subjudice.</p> <p>It is an established fact that the use of ENDS or Vaping has significantly less health and safety concerns compared to high risk associated with conventional cigarettes, endorsed by the governments of 65 nations across the world such as EU, UK, US and Canada, as well as by credible institutions such as the Public Health England, American Cancer Society and the US Food and Drug Administration (FDA).</p> <p>Electronic Nicotine Delivery Systems (ENDS) include various types of e-cigarettes, also known as vapes which deliver nicotine without the harmful chemicals and compounds found in cigarette smoke. E-cigarettes have emerged as a promising avenue for people who want to quit smoking and has the ability to provide a means to compete with or even replace cigarette use, and has the potential of saving millions of lives.</p> <p>India has more than 100 million adult smokers and around a million people die due to tobacco related diseases annually. Unless the sale of tobacco products is regulated or completely restricted, the restrictions imposed on promotion and sale of ENDS would only further aggravate the health hazards. The MeitY would do well to first understand the facts and then move ahead with any policy decisions.</p> <p>The inclusion of ENDS or E-Cigarettes in the proposed amendment to the IT Act, which prohibits publishing online information about these products is surprising.</p> <p>Electronic Nicotine Delivery Systems (ENDS) include various types of e-cigarettes, e-hookahs, and vapes which deliver nicotine without some of the known harmful carcinogenic substance from cigarettes containing tobacco. Most reviews of clinical evidence show that the chemicals found in e-cigarettes are far fewer and well below levels in comparison to smoking cigarettes.</p> <p>In a country like India, where there are so many tobacco users, there is an enormous potential for risk reduction by substituting cigarettes with less hazardous products.</p>

S.No	Ref. No.	Comments
129	MIT/79/129	<p>Hello,</p> <p>This is to request you to not implement the ENDS draft created for banning e-cigarettes. E-Cigarette products are just used as a substitute to curb the harmful effects of smoking, and several medical body has approved that it's better than tradiional cigarettes.</p> <p>I have been a smoker for last 10 years, continously trying different alternatives for quitting cigarette. Nothing worked until I tried e-vapes, and it worked like a magic. I haved reduced my normal cigarette intake to around 90% in 2 months, and I feel better now.</p> <p>We do not have proper awareness of e-cigarettes in India, and considered as hookah. Which is wrong. Where hookah is used for enjoyment, e-cigarettes/vapes are used as an alternative of cigarette, so that we can get rid of the harmful contents of normal cigarrete.</p> <p>Yes we need to assess how it should be made available and regulate that, so that it doesn't reach to people below 18 years old. But please do not ban vapes/e-cigarettes.</p> <p>When proven harmful tobacco products like normal cigarette/gutkha are not banned but regulated, then why it can't be implemented for e-cigarettes/vapes as well.</p> <p>It's my sincere request to you, please think of the people like me who has been benefitted with vapes, and started improving their life</p>

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES 2018
(Published by MeitY)

S.No	Ref. No.	Comments
130	MIT/79/130	<p data-bbox="329 389 607 419">Respected Sir/Madam,</p> <p data-bbox="329 469 2145 576">After trying numerous times to quit smoking cigarettes either cold turkey or with nicotine gum, I finally quit my 18 year old 20 cigarettes/day habit with electronic cigarettes 3 years ago. After switching to electronic cigarettes (often referred to as Electronic Nicotine Delivery Systems or ENDS in literature), I have observed a great reduction in breathing problems, increased stamina, reduction in dental issues and general overall well being.</p> <p data-bbox="329 625 2157 927">A simple google search will show you that nicotine, while being addictive, is not much more harmful than caffeine if taken in small quantities. It is the products of tobacco combustion in cigarette smoke that are the cause of most of the adverse health effects of smoking. Many observers point out that a user of electronic cigarettes is still addicted to nicotine. So the question then arises, whether the fight against tobacco is a fight for better health of citizens by eliminating the harmful effects of tobacco or a religious/cultural fight against addiction. If it is the latter case then the ban should also include sugar which has been proven to be addictive in many studies. For me personally, I wanted better health for myself and to get rid of the increased risk of cancer/ heart disease that come with smoking and I believe I have done myself a huge favor in that regard by switching to electronic cigarettes. Countless studies have proven that electronic cigarettes are at worst 5% as harmful as smoking, and most governments worldwide have chosen to regulate not ban them.</p> <p data-bbox="329 976 2123 1121">There is a great deal of misinformation regarding electronic cigarettes in popular media. The truth is that Smoking has killed about 100 million people during the 20th century, and electronic cigarettes are our best bet as a society in combating this killer. Therefore I beg you that we as a society wield this weapon against smoking in a sensible manner instead of completely throwing it out of the window with a blanket ban on electronic cigarettes, information sources about them and means of procuring them for those looking to quit smoking</p>

S.No	Ref. No.	Comments
131	MIT/79/131	<p>Gentlemen,</p> <p>It is with a great deal of trepidation that I am made aware of the Government's proposed steps vis a vis electronic cigarettes!</p> <p>It is a well-established, scientific fact that using e-cigarettes is humongously LESS HARMFUL than smoking regular cigarettes. Common sense alone dictates that one consider the chemical constituents of both forms.</p> <p>On the one hand, one is ingesting a HUGE amount of chemicals caused by the burning of tar, paper, leaf (and god knows what else!) in smoking a cigarette, as opposed to the harmless (with due acknowledgement of the addictive qualities of nicotine) substances such as propylene glycol, glycerine & water which are products used in the food industry)!</p> <p>It has been established by governments worldwide that not only are electronic cigarettes CONSIDERABLY less harmful than tobacco cigarettes, they are a valuable tool for weaning off cigarette smokers from the dangerous habit.</p> <p>I, myself, was a 2-pack a day man (with attendant respiratory problems) for over 50 years but am now a very moderate user of e-cigarettes & my body is thanking me for it.</p> <p>An attendant problem with the Government's proposal is that the move is being seen widely, as being influenced by the tobacco lobby as there is no proposal to stop the sale of regular cigarettes. This, further, behooves the thought that by allowing the continuing sale of tobacco cigarettes, the Government is not concerned with the welfare of it's citizens but only with revenue generated by tobacco taxes.</p> <p>Further, there could be a legal perspective to the issue as the proposal could be construed as denying millions, the right to a healthier alternative.</p> <p>THIS IS A SERIOUSLY FLAWED (to use mild terminology) PROPOSITION and I would fervently pray that you rethink your position.</p>

S.No	Ref. No.	Comments
132	MIT/79/132	<p>Dear Sir/Madam</p> <p>I have been a smoker for 15 years now, finishing a complete pack a day. Thanks to vaping products I have not touched a cigarette for the last year. I tried many other cessation devices like nicotine gum and patches but none of them worked for, forcing me to go back to smoking.</p> <p>I am now a father to a 15 day old daughter and really happy that she does not have to smell smoky fingers or grow with the fear that I use cancerous cigarettes.</p> <p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p> <p>In closing I would like to state that many countries from EU to US have regulated them, not banned. A ban on info and access will deny you the right to lead a healthier life</p>

S.No	Ref. No.	Comments
133	MIT/79/133	<p>Dear Sir,</p> <p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p> <p>Kindly do not ban vaping contents online.</p> <p>Thanks & Regards,</p>
134	MIT/79/134	<p>Dear Sir/Ma'am,</p> <p>I am writing to you today with sincere hope that you will reconsider including ENDS in 3(J) of Draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018.</p> <p>ENDS or E-cigarettes with nicotine have come about to save my life. I used to smoke a pack of 20 cigarettes everyday and my health was fast deteriorating. I couldn't breath and was constantly sweating. With the use of ENDS I have completely given up smoking cigarettes and have been feeling much better. My lungs and throat are completely fine now. All Research taken place in Europe and USA says that ENDS are 95% safer than smoking traditional cigarettes since it doesn't contain tar and 100's of harmful chemicals which regular cigarettes contain.</p> <p>In view of the same I feel, ENDS should be promoted through digital media and campaign and not curtailed under the new IT act. I hope you would reconsider!</p>

S.No	Ref. No.	Comments
135	MIT/79/135	<p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p>
136	MIT/79/136	<p>Hi,</p> <p>I'm writing this email to share my experience on vaping and how it changed my life for the best. I was a heavy smoker for almost 5 years and it was my biggest regret in life. I've tried to quit smoking several times in the past and it never worked until a friend introduced me to vaping and since then I haven't smoked a cigarette and I have also made few of my friends to switch to vaping and they are so thankful that I made them quit smoking. There is a stigma attached to vaping that it is equally harmful to health. But it's not it is proven to be much healthier than cigarettes. Even hospitals in the UK and US allow vaping as it is a healthier alternative. I have experienced a lot of changes in my health, breathing, and eating habits after switching to vaping. If the government bans vaping and restricts vaping related news to us users we will be forced to go back to cigarette which will give us cancer for sure. By banning vaping products you are only forcing us to smoke cigarettes which is the main cause of cancer. The vaping community in India has helped a lot of people quit cigarette and lead a healthier and happier life by making the switch to a safer alternative. There are also 100's of research paper on the the benefits of vaping and I would be happy if our government can educate and spread on the benefits of vaping to others so they can lead a happier life too. Many countries in the EU, US and UK have regulated the laws for vaping for the betterment of the people.</p>

S.No	Ref. No.	Comments
137	MIT/79/137	<p>Dear Sir's,</p> <p>I smoked for 15 years, and I smoked a lot. I knew smoking was killing me, and I tried so many ways to quit. Nothing worked. patches, cold turkey, nicotine gum, self hypnosis didn't work. I felt like a failure. I had a few co-workers who were vaping. I thought it was stupid, but gave it a try. I smoked my last cigarette the day that I bought my first personal vaporizer. That was 2.5 years ago. Vaping saved my life!</p> <p>Numerous credible institutions have found ENDS to be 95% safer than smoking.</p> <p>People should not be denied information on safer alternatives as it can help save lives Many countries from EU to US have regulated them, not banned.</p> <p>A ban on info and access will deny you the right to lead a healthier life.</p> <p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – 'Cigarettes'. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p>

S.No	Ref. No.	Comments
138	MIT/79/138	<p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p> <p>I do not see how cigarettes can be legally sold but not this much safer option. It is sad to see that such bills and laws are regressive in nature and are nothing but paying obeisance to the corporate lobbying. It would be a shame if Indians do not have the means to choose a safer option - I believe the choice should be the individual and cannot be banned like we live in a dictatorship government. At least regulation bills make sense, an outright ban is just foolish.</p> <p>Ananth</p>
139	MIT/79/139	<p>Dear Sir,</p> <p>I used to be a heavy smoker till a few years back, and used to constantly fatigued. I had heard about vaping from a relative in the UK, and started. Today I vape regularly. I have no cough, shortness of breath or fatigue. My quality of life has significantly improved since i switched to vaping.</p> <p>The NHS in the UK recommends vaping to switch over from traditional cigarettes, as they have been repeatedly found to be safer in real world studies. Public vaping is permitted there.</p> <p>Vaping if encouraged can lead to a significant difference in incidence of cancers and mortality associated with traditional cigarettes. More and more smokers must be encouraged to switch to vaping.</p> <p>Regards, Dr. Kevin Joseph</p>

S.No	Ref. No.	Comments
140	MIT/79/140	<p>Namaste ,</p> <p>My name is Naren kumar R, from Bangalore city. I was smoking cigarettes since the age of 19, I am now 35 years of age. I tried to quit smoking cigarettes many times since I started smoking and all methods to quit failed. Smoking cigarettes was making my health weak and decided to try vaping (e- cigarettes) last January to check if vaping could help me quit smoking cigarettes. To my surprise vaping felt exactly like smoking cigarettes except that it was a safer alternative to tobacco and nicotine. In the first week since vaping last January my count of cigarette smoking reduced drastically and now after a year I have stopped smoking cigarettes. Vaping has definitely helped me and countless others to give up smoking cigarettes in a short space of time, it also helped us to recover our health from the bad health effects of chronic cigarette smoking. Now I have no urge to smoke cigarettes thanks to E- cigarettes (vaping). Please do not ban E- cigarettes(vaping) as it is a proven and safest way to stop smoking cigarettes.</p> <p>Thank you. Namaste</p>
141	MIT/79/141	<p>Dear Sirs,</p> <p>I am a regular vaper (consumer of electronic cigarettes) and have been for the last few years.</p> <p>I am firmly of the view that Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes and ENDS/e-cigarettes present a much less harmful option to the millions of cigarette smokers in the country.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. 'Cigarettes'. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco. I have other research from reputed sources which I am happy to share with you if you like.</p> <p>The awareness of e-cigarettes is low in India and moves towards curbing the right to information online will only increase the health hazards and lead to more deaths from cigarette smoking. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries/regions accept these devices as a harm reduction tool that helps people quit smoking tobacco and today have the lowest rates of disease and deaths due to smoking.</p> <p>Yes I agree there is a need to regulate vaping/e-cigarettes from the point of view of preventing the youth from consuming addictive substances very early but please don't cause harm to those who derive significant health benefits from vaping/e-cigarettes.</p> <p>Please let me know if you have questions or if I can share any of the research I have stored.</p> <p>Thank you & regards,</p>

S.No	Ref. No.	Comments
142	MIT/79/142	<p data-bbox="331 225 672 252">Respected Sirs and Madams</p> <p data-bbox="331 301 2145 368">It is highly unfortunate that the Institutions set up by the people, of the people and for the people is bent upon killing its own people mercilessly, for its own short term gains.</p> <p data-bbox="331 418 2123 485">Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p data-bbox="331 534 2145 639">The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p data-bbox="331 689 2130 836">The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accept the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p> <p data-bbox="331 885 2112 952">Therefore, I sincerely request that such amendments proposed which do more harm than good in its current form be discarded and consultations be held with the people before such draconian decisions are made.</p>

S.No	Ref. No.	Comments
143	MIT/79/143	<p>It is undeniably abysmal that under the appearance of control of spreading of counterfeit newscasts you have chosen to comprise in the same the entire scheme of e-cigarettes and vapes communally categorized as ENDS under section 2(j) under the draft The Information Technology (Intermediaries Guidelines (Amendment) Rules) 2018 published on 24.12.2018.</p> <p>The exploration for smoking cessation rehabilitation needs to be stimulated, be it nicotine gums, lozenges, blotches or ENDS in equal quota and not be selectively battered as it is currently being projected in your amendment act. ENDS have been making stern breakthroughs in the combined scientific and the healthcare community across the world and it would not be correct to sole out the Indian populace from access to evidence on this advancement which has been put forward as one of the most effective ways of quitting smoking.</p> <p>I have benefited tremendously from this knowledge-base as it helped me kick a 22-year-old habit of smoking over 15 cigarettes a day and have been smoke free for over 2 years now. Unless information is available in the public sphere on possible replacements and remedies, people like me will not be able to read, adapt and take knowledgeable conclusions on their life's adoptions, even if deemed contentious by a group of entities. It is my acceptance that e-cigarettes/ENDS/vapes should not form any part of this amendment and that it needs to be obliterated.</p> <p>Some Food for thought as mentioned below</p>

S.No	Ref. No.	Comments
144	MIT/79/144	<p>Hello Sir,</p> <p>I was a smoker for 15 years , ecig has helped me to get rid of cigarettes, initially I stated of with higher mg of nic, but now I use 6mg, plan is to get down to 3mg and probably 0mg of nic....</p> <p>Tobacco, Cigarettes and Alcohol cannot and should not be clubbed with ENDS or e-cigarettes, considering there is no legal classification that exists for such products and that these products are just used as a substitute to curb the harmful effects of smoking.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and researches conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of cigarettes. In the United Kingdom, Europe and Canada, the use of e-cigarettes is properly and formally regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful. These countries today have the lowest rates of disease and deaths due to smoking.</p> <p>=====</p>
145	MIT/79/145	<p>The Ministry of Electronics and Information Technology (MEITY) proposed amendment to the Information Technology (Intermediary Guidelines) Rules 2018, banning the advertisement or publishing of any online information on ENDS/ E-Cigarettes.</p> <p>It is an established fact that the use of ENDS or Vaping has minimum health and safety concerns compared to high risk associated with conventional cigarettes, endorsed by the governments of 65 nations across the EU, UK, US and Canada, as well as by credible institutions such as the Public Health England, American Cancer Society and the US Food and Drug Administration (FDA).</p> <p>Electronic Nicotine Delivery Systems (ENDS) include various types of e-cigarettes, also known as vapes which deliver nicotine without the harmful substances from cigarettes containing tobacco. E-cigarettes has emerged as a promising avenue for people who want to quit smoking and has the ability to provide a means to compete with or even replace cigarette use, saving more lives. It focuses on harm minimization and smoking cessation.</p>

S.No	Ref. No.	Comments
146	MIT/79/146	<p>Proposed ban on Electronic Nicotine Delivery System (ENDS) advertising and its information being available online to public denoting it threatens public health and safety seems unsubstantiated and hasty. ENDS heats a solution to create an aerosol, which usually contains flavours such as vanilla or mint. It is available in many forms such as e-cigarettes and vapes. E-cigarettes however do not burn or use tobacco leaves, but instead vaporises a solution, which the user then inhales. Globally, researchers and people consider it as a substitute considering it helps smoker escape the harmful habit that has grave effects on their body.</p> <p>Nicotine or ENDS device have not been notified as a drug by the Central Government. However, the only type of nicotine that is regulated (and provided certain exemptions) under the Drugs Act is nicotine gum and lozenges containing up to 2 mg/4 mg of nicotine. The rationale for including this category of nicotine within the purview of the Drugs Act is that nicotine gum and lozenges are used in replacement therapy as a substitute for smoking cigarettes.</p> <p>Further, from the information available on the official website of the Central Drugs Standards Control Organization, it appears that nicotine transdermal patch is an approved new drug. Its time the government promotes sharing of information rather than creating hurdles for its citizens to take their owned judged decision.</p> <p>In short, E-cigarettes/ENDS are not covered under the definition of the term 'drug' and therefore do not come under the purview of Drugs and Cosmetics Act, 1940. E-cigarettes therefore cannot be regulated under the provisions of the said Act.</p>

S.No	Ref. No.	Comments
147	MIT/79/147	<p>Dear Ministry</p> <p>The latest IT Act amendment to ban publishing of any information related to electronic nicotine delivery systems (ENDS), stating that it threatens public health and safety, is a severe step towards restricting an individual's access to information. The amendment is part of the measures proposed by the Centre to curb fake news and includes monitoring the online activity Indian citizens.</p> <p>From Alcohol to TV programmes and social media, bans have been imposed in India based on the premise that conscience of the general public is influenced by such decisions. On the contrary, a blanket ban is curbing democracy and the constitutional rights of citizens. They are based on the flawed premise that by closing our minds we can resolve a problem. The more the political anxiety surrounding an issue, the more is the propensity to ban. ENDS serves as a cessation aid to help an ardent smoker and should surely not fall in list as other items prohibited such as alcohol.</p> <p>Nearly 7 out of every 10 smokers say they want to stop smoking due to its harmful health impacts. People have started to gradually shift from traditional cigarettes to electronic cigarettes, also known as vapes. Not only does it act as a substitute to many of the physical, psychological and socio-cultural elements of cigarette smoking, but is also convenient and cheaper than smoking, making it a promising tool for switching with less harm.</p> <p>India being the world's biggest democracy should provide its citizens with the basic right to access information online, especially in the health and quality of life domain. We need to encourage an open society which can debate and discuss the advantages and disadvantages of various choices available to them.</p> <p>--</p>

S.No	Ref. No.	Comments
148	MIT/79/148	<p>Respected Sir/Madam,</p> <p>I am commenting on my personal capacity as a concerned citizen on a specific below mentioned section/sub-section in the Draft amendment to the information Technology (Intermediary Guidelines) Rules 2018 proposed by the The Ministry of Electronics and Information Technology (MEITY).</p> <p>(2) Such rules and regulations, privacy policy terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —</p> <p>(j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made there under;</p> <p>Kindly note that there is no nation wide ban on ENDS issued by the Centre and the issued advisory can't only be the reason to restrict ENDS over the internet.</p> <p>As per Delhi HC, "The advisory is not binding and it would be open to the respective states and union territories to take an informed decision in this regard," Justice Vibhu Bakhru said. Unless there is any strict BAN memo such rigorous restriction as drafted by MEITY is highly questionable and open to challenge in court of law as per Delhi HC. As a concerned citizen I would like to request to your kindness to not restrict ENDS in any way unless there is any nation wide ban first.</p> <p>Also I would like to draw your kind attention to the fact that ENDS are widely established as a smoking cessation tool far far safer than conventional cig and is a very popular since it can not only mimic the nicotine craving of the user but also deals with the oral fixation of smoking. I myself have quit smoking 1.5 years ago overnight with the help of ENDS. Its the only thing worked for me and billions like me. Restricting ENDS over the internet via blocking its promotion display and publication will be equivalent to snatching away healthier alternatives from smokers which would have saved millions from premature death.</p> <p>I have listed several studies for your kind information and request you not to restrict ENDS over the vast internet without a proper ban MEMO. Kindly note that such action will invite black-marketing and bad quality products will end up being at the hands of vapers which can result in serious health hazard. Such strict action will push millions of ex-smokers to go to black-market just to save their lives. India regulates and allows Conventional Cig openly while restricting tremendously safer alternatives which saves lives, this is plain violation of our fundamental rights. If this section and sub-section is not removed this will be open for challenge in court of law and this will seriously hamper the credibility of Ministry among the citizens of India.</p> <p>Study 1 - E-cigs are twice as effective as NRTs at helping smokers quit, a major clinical trial finds</p> <p>Study 2 - E-cigarettes: an evidence update A report commissioned by Public Health England</p> <p>Study 3 - Electronic cigarette vapor alters the lateral structure but not tensiometric properties of calf lung surfactant</p> <p>Study 4 - Comparing the cancer potencies of emissions from vapourised nicotine products including e-cigarettes with those of tobacco smoke -</p> <p>Study 5 - Evidence review of e-cigarettes and heated tobacco products 2018A report commissioned by Public Health England</p> <p>Study 6 - Characterization of the Spatial and Temporal Dispersion Differences Between Exhaled E-Cigarette Mist and Cigarette Smoke</p>

S.No	Ref. No.	Comments
149	MIT/79/149	<p>महोदय आईटी अधिनियम में प्रस्तावित संशोधन में ईएनडीएस या ई-सिगरेट को शामिल किया गया है, जो इन उत्पादों के बारे में ऑनलाइन जानकारी प्रकाशित करना प्रतिबंधित करता है। इलेक्ट्रॉनिक निकोटीन डिलीवरी सिस्टम (ईएनडीएस) में विभिन्न प्रकार के ई-सिगरेट, ई-हुक्का, और वेप शामिल हैं जो तम्बाकू युक्त सिगरेट से कुछ ज्ञात हानिकारक कार्सिनोजेनिक पदार्थ के बिना निकोटीन वितरित करते हैं। नैदानिक साक्ष्यों के अधिकांश समीक्षाओं से पता चलता है कि ई-सिगरेट में पाए जाने वाले रसायन सिगरेट पीने की तुलना में बहुत कम और अच्छी तरह से नीचे स्तर पर हैं। भारत जैसे देश में, जहां बहुत सारे तंबाकू उपयोगकर्ता हैं, वहाँ कम खतरनाक उत्पादों के साथ सिगरेट को प्रतिस्थापित करके जोखिम में कमी की भारी संभावना है। भारत दुनिया भर में तंबाकू का दूसरा सबसे बड़ा उपभोक्ता है, जिसमें लगभग 12cr धूम्रपान करने वाले (दिन के हिसाब से) बढ़ रहे हैं, जिनमें से 900k हर साल मरते हैं। जमीनी स्तर पर समस्या को हल करने के बजाय, सरकार गलत तरीके से ईएनडीएस पर सूचना साझा करने पर प्रतिबंध लगा रही है। उन्हें वास्तव में, इस विचार को लोकप्रिय बनाना चाहिए कि ई-सिगरेट एक सुरक्षित विकल्प है, क्योंकि यह निकोटीन नशेड़ी के लिए नुकसान को कम करने का एक महत्वपूर्ण तरीका हो सकता है। जुलाई 2016 में, सार्वजनिक स्वास्थ्य इंग्लैंड और ग्यारह अन्य ब्रिटिश सार्वजनिक स्वास्थ्य संगठनों, जिनमें ब्रिटिश लंग फाउंडेशन, कैंसर रिसर्च यूके, रॉयल</p>
150	MIT/79/150	<p>Sirs</p> <p>The recent ban proposed to the IT Act, stating “intermediaries” should ensure they do not publish information on anything that threatens public health or safety specifically mentioning tobacco products, intoxicants including alcohol and also ENDS (Electronic Nicotine Delivery Systems), is a surprising restraint on e-cigarettes.</p> <p>Tobacco, Cigarettes and Alcohol cannot be possibly clubbed with ENDS or e-cigarettes considering there is no legal classification that exists and that one of these products is just used as a substitute to curb the harmful effects of the other.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and research conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’.</p> <p>A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in a country like India and such amendments to further curb the right to information online will only increase</p>

S.No	Ref. No.	Comments
151	MIT/79/151	<p>The new proposed amendment in the IT act prohibits the distribution of information on ENDS (Electronic Nicotine Delivery Systems) citing it threatens public health and combines it along with other sin products such as cigarettes. The fact of the matter although is that e-cigarettes does not burn tobacco, and thus should be excluded from this category.</p> <p>The act further prohibits information release on any products which do not comply with the Drugs and Cosmetics Act 1940, the last amendment of which was passed in 1995. E-cigarettes which were commercially launched only in early 2000's, obviously have no way to defend its use, even though it reduces the harmful impact of nicotine use in comparison to traditional cigarettes.</p> <p>Our government's arbitrary view on this topic is totally contrary to many developed countries who are in fact promoting information dissemination on ENDS as a favourable alternate for smokers.</p> <p>Thanks</p> <p>PRitha</p>
152	MIT/79/152	<p>The inclusion of ENDS or E-Cigarettes in the proposed amendment to the IT Act, which prohibits publishing online information about these products is surprising.</p> <p>Electronic Nicotine Delivery Systems (ENDS) include various types of e-cigarettes, e-hookahs, and vapes which deliver nicotine without some of the known harmful carcinogenic substance from cigarettes containing tobacco. Most reviews of clinical evidence show that the chemicals found in e-cigarettes are far fewer and well below levels in comparison to smoking cigarettes. In a country like India, where there are so many tobacco users, there is an enormous potential for risk reduction by substituting cigarettes with less hazardous products.</p> <p>India is the second largest consumer of tobacco worldwide with nearly 12cr smokers (increasing by the day), 900k of whom die every year. Rather than solving the problem on the grassroots level, the government is incorrectly banning information sharing on ENDS. They should in fact, popularise the idea that e-cigarette are a safer alternative, as this may be a key way to reduce harm for nicotine addicts.</p>

S.No	Ref. No.	Comments
153	MIT/79/153	<p>Dear Shri/Madam,</p> <p>I'm writing to you from Nagpur, Maharashtra. I am a 31 years young traveler, collector, numismatist, visual artist and a wannabe photographer. I have a hobby of looking for extraordinary in the most ordinary things around us and finding joy in them. I run a small museum in central India where I showcase a Numismatic collection and encourage others to start a hobby, any hobby for that matter.</p> <p>I began smoking when I was about 18 thanks to curiosity and peer pressure in college, just like most beginners. I always hated the taste and smell but I couldn't quit despite several attempts. Every time there was a little pressure in college or life (or so it appeared) I'll be back to the cigarettes. I hated the taste so much that I used to chew on a blackcurrant/lemon candy everytime I smoked. I guess this is why I got hooked on to Hookah as well and it became a regular affair. I smoked for about 5 years and was facing the usual health effects that smoking brings along with it and then around late 2010 while I was pursuing my Masters degree in the UK my landlord introduced me to a Skycig e-cigarette which looked just like a regular cigarette but it was smoke free and came in different flavors. Vaping had just begun then and it was starting to become popular in the UK. It took me a while to quit the traditional cigarettes completely but after vaping came in I reduced my cigarette consumption and finally 26th of January 2012 was the day when I had my last cigarette and never looked back and I couldn't be happier. I started with 24mg Nicotine level juice and gradually brought it down to 3mg. It not only improved my health but brought along so many good things with it.</p> <p>I felt good, I smelt good, with people I dealt good. I started to get more curious about vaping and went online to look up information on websites, forums and social media groups. Through this I got to know about several communities and forums where people across the globe care and share information about vaping, I joined them and started to share my own experiences and views along with my vape pictures and made a lot of friends in the local and international vaping industry sharing the same level of enthusiasm for vaping and through them I got the encouragement to restart a long lost hobby of photography and started clicking again regularly. Vape photography has become a passion, an exercise, a therapy almost and it brings me immense joy to keep doing it and it keeps me motivated to stay focused, positive and hopeful.</p> <p>Through the years, I have experienced the vape industry and vape devices evolve into safer, more efficient and more user friendly systems. Today there are several options to choose from ranging from tiny starter kits to big powerful mods for a smoker to begin vaping depending on their needs and preferences from a Cigarette-like draw through Mouth-To-Lung to a Hookah-like draw through Direct-Lung, from High Nicotine juices for long time heavy smokers to Low or No Nicotine juices for occasional smokers or Hookah smokers. Its particularly important to consider that a majority of Hookah smokers think that its safe to do it as it's only a flavored smoke and not harmful but they don't realize that it's in fact combustible flavored tobacco along with all the chemicals which is probably more harmful than a traditional cigarette.</p> <p>In almost a decade of vaping, I have tried almost every form of vaping, from starter to advanced, from 24mg nic to 0mg nic, from international Eliquids to local Eliquids and even made some of my own. And there's one thing I have realized that with an unregulated growth of the industry there's bound to be errors and mishaps along the way and that's where the government comes in. Instead of dismissing the entire idea of vaping altogether the government needs to look into it more deeply, do more in-house research, talk to and take inspiration from other countries who have regulated vaping and find ways to make it safer, approachable and acceptable while focusing more towards regulating it in order to make sure only the safest devices and liquids are sold to an appropriate age group while generating revenue to support the government.</p> <p>Vaping today is not just a habit or an alternative option. It has become a culture of its own, with millions of ex-smokers across the world coming together for a cause sharing their success stories and how vaping helped them and improved their life and of their near and dear ones. I feel proud to have been able manage to help over a couple of dozen smokers learn about vaping and got them to understand its benefits and quit smoking completely and successfully make the switch.</p> <p>Vaping is a global phenomenon and We as a country can't afford to simply ban them or cease any opportunity for all the existing smokers from knowing and trying out an effective and efficient medium to help them quit smoking and have a happier and healthier life. Therefore, it's a humble request to you to reconsider the proposal and give the people of Free India a chance to make a rightful decision for the betterment of their own lives.</p>

S.No	Ref. No.	Comments
154	MIT/79/154	<p>The recent ban proposed to the IT Act, stating “intermediaries” should ensure they do not publish information on anything that threatens public health or safety specifically mentioning tobacco products, intoxicants including alcohol and also ENDS (Electronic Nicotine Delivery Systems), is a surprising restraint on e-cigarettes. Tobacco, Cigarettes and Alcohol cannot be possibly clubbed with ENDS or e-cigarettes considering there is no legal classification that exists and that one of these products is just used as a substitute to curb the harmful effects of the other.</p> <p>The evidence is unambiguous that vaping is much safer than smoking as established in many studies and research conducted by multiple countries across the world. But misinformation and scaremongering could still be putting people off switching the killer substance – ‘Cigarettes’. A 2016 report by the Royal College of Physicians in the UK concluded the health risk from long-term vaping was unlikely to exceed 5% of the harm from smoking tobacco.</p> <p>The awareness of e-cigarettes is still low in a country like India and such amendments to further curb the right to information online will only increase the health hazards and eventually lead to more deaths from the regular use of tobacco. In the United Kingdom, Europe and Canada, the use of e-cigarettes is restricted and regulated. These countries accepts the device as a harm reduction tool that helps people quit smoking tobacco and move on to a habit that is less harmful.</p>

PUBLIC COMMENTS ON DRAFT PHARMEDICAL REGULATIONS
(Published by MeitY)