Public Comments

On

DRAFT

INTERMEDIARY GUIDELINES RULES, 2018

Addendum1

Date: 08-02-2019

Published by Ministry of Electronics & IT

Government of India

MIT/79/156

Dear Sir,

This is with reference to the Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 ("**Draft Notification**") which has been notified for comments by the Ministry of Electronics and Information Technology ("**MeitY**") on 24th December 2018.

At the outset, we would like to take this opportunity to welcome this step. We are mindful of the fact that these amendments have been proposed to prevent spreading of fake news through misuse of social media platforms by imposing reasonable restrictions upon freedom of speech and expression. We are also cognizant of the fact that such social media platforms are also covered under the definition of Intermediaries u/s 2(w) of the Information Technology Act, 2000 ("IT Act 2000").

However, there is a need to appreciate that there are many other business models such as e-commerce/online marketplaces, payments and recharges platforms, server spaces etc. which are also covered under the definition of Intermediary. While making an amendment to the guidelines due consideration should be given the difference in their business, their opertional methodolgies and the kind of social impact they create.

It is our humble submission that MeitY should treat e-commerce/online marketplaces as a separate form of Intermediary for sub-rule 3, basis the understanding above and the development of international jurisprudence to this effect. We would be happy to work along MeitY for any assistance that may be needed for understanding or rule making.

We however, wish to submit our suggestions/comments as below for your kind consideration:

Rule 3 - Information Technology (Intermediaries Guidelines) (Amendment) Rules, 2018 – DRAFT	**Suggestions/Comments**
(7) The intermediary who has **more than fifty lakh users in India** or is in the list of intermediaries specifically notified by the	Given the increasing number of internet users in India, the basis of deciding on the threshold of fifty lakh users is not discernible. We submit that the classification must have a rational basis in relation to the object sought to be achieved by the IT Act,

government of India shall: be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; have a permanent registered office in India with physical address; and 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.	which inter alia is to facilitate e-commerce in India[1]. We believe, that instead of addressing the issue basis the Users, (which may not pass through the rationale laid down under various Supreme Court decisions relating to reasonable classification under Article 14 of the Constitution), there should be classification only basis the country of incorporation. Instances of such classification can be found to be made by RBI for regulating foreign banks which need to satisfy additional requirements for operating in India. Such additional requirements relate to either having a 'branch form of presence' called as the Branch Office or 'representative office form of presence', called as Representative Office, or setting up a wholly owned subsidiary in the form of a company. Such corporate structuring is allowed through nuanced regulations which are mandatory to comply with and operations are allowed basis the compliance submitted by foreign banks We believe, that if the classification is based as per above parameters, then it would be a reasonable classification and would stand the scrutiny of the Supreme Court. Since online marketplaces are an integral source of information with regard to the identity and co-ordinates of sellers transacting on the platform, all marketplaces seling in India / shipping to India should be required to be have a physical branch office in India and an Indian national as the nodal person for co-ordination with law enforcement and tax authorities. In addition, it is also suggested that the IT Act should be amended to have extra territorial jurisdiction as is in the case of Competition Act 2002 in India or anti bribery legislations in UK and US.
(9) The Intermediary shall deploy technology based automated tools	Intermediaries are tasked with the responsibility to expeditiously take down unlawful information or

or appropriate mechanisms, with appropriate controls, **for proactively identifying and removing or disabling** public access to unlawful information or content.	content. Such take down is mandated to happen upon receiving actual knowledge (by a court order) or on being notified (by the appropriate government). In circumstances, where such take down is not initiated expeditiously, the Intermediary stands on the verge of losing the exemption to it being an intermediary granted under section 79. This has been further clarified and observed in the Shreya Singhal[2] matter where the Supreme Court observed that an intermediary's responsibility is only to expeditiously remove or disable access to material 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) are going to be committed. While we understand that this amendment has been proposed to prevent spreading of fake news through misuse of social media platforms, we believe that such broad guidelines for all kind of intermediaries may not solve the object of the proposed amendment, and rather create difficulties for online marketplaces, which only act as a platform for commercial transactions. Given the nature of commerce related content hosted on the marketplace, the mandate to proactively identify and takedown unlawful information or content is not practical and will severely hamper businesses operations of marketplaces. Further, it will obfuscate their role as intermediaries providing a technology platform connecting buyers and sellers. We propose that a carve-out be made for online marketplaces from the proposed amendment, so that commercial transactions are not hit by the broad sweep of the mandate.

In view of the above, we humbly request MeitY to consider our comments/suggestions on the Draft Notification . We would be pleased to be of any further assistance in framing these guidelines.

Thanking You,

Sincerely,

Pawan Kaul

---

[1] Statement of Object & Reasons to IT Act 2000. The IT Act 2000 was enacted to give effect to the Resolution by the UN General Assembly to adopt Model Law on Electronic Commerce.

[2] Shreya Singhal v/s Union of India (2015) 5 SCC 1. Decided on 24th March 2015.

Pawan Kaul

Head - Corporate Affairs | Corporate Affairs & Communication

M: +91 9717182929 | T: +91-124-4739850
5th-6th Floor, Cyberscape, Golf Course Extension
Sector – 59, Gurugram -122002, Haryana, India

Comments on the Proposed Amendments to Intermediary Liability Framework
("**Amendment**")

1. On-soil requirement

1.1. The Amendment makes it mandatory for any intermediary having more than 50 lakh users in India to be an entity to mandatorily be a company incorporated in India. This has far reaching implications on intermediaries who operate global platforms from offshore locations. One may argue that the requirement for local presence is essential to enable enforcement agencies to effectively manage any potential cause for concern. However, the requirement of having an appointed nodal person of contact and an alternate senior designated functionary (as prescribed under the Amendment) would serve exactly this purpose. The Government can just as easily liaise and co-ordinate with these appointed officials for the purpose of enforcing law and order. Mandating local presence in the form of an incorporated entity appears to be an excessive measure undertaken by the Government.

1.2. Notably, all companies incorporated in India are mandated to have a physical registered office in India, which information is also required to be intimated to the Registrar of Companies soon after incorporation. Consequently, the second requirement of ensuring that the intermediary has a permanent registered office in India with physical address would be superfluous.

1.3. Another important concern that begs clarification is that of the consequence of not complying with the local-presence requirement. Would such non-compliance imply that the intermediary is prevented from offering Indian users access to their platform itself, or does it solely imply that the intermediary would not be able to take advantage of the safe harbour provisions that would, otherwise, have been available to it? To suggest the former position be taken would mean that any intermediary seeking to provide services to Indian residents would need to do so from India. These entities would not only have to set up shop in India, but also replicate its platform solely for India. This would certainly pose great practical and economic challenges for intermediaries.

1.4. It must be noted that intermediaries are covered by the Information Technology Act, 2000 (**IT Act**). The scope and applicability of the IT Act as captured in Section 1 thereof does not require persons to whom it is applicable (including intermediaries and other internet service providers) to be entities incorporated or established in India, as is the case for various statutes applicable to other sectors (such as insurance companies under the Insurance Act or access/internet service providers under the Unified Service Guidelines). Given this, the local presence requirement would be beyond the current scope of the IT Act and hence, also beyond the rule making powers of the Government.

1.5. Further, requiring intermediaries to be incorporated in India, may lead to a situation where well-established intermediaries, conducting business in India, in absolute compliance with applicable local laws may now be running afoul of the foreign investment (FDI) policy and would consequently be required to wind up their service offerings, significantly affecting the ease of doing business in India.

1.6. Lastly, the eligibility criteria of fifty lakh users appears to be an arbitrarily fixed number, not based on statistical study of usage patterns. This number is significantly low and is likely to impose an unreasonable burden on start-ups/smaller intermediaries who would not have the ability or infrastructure to comply with the requirements under the Amendment (and consequently impacting innovation and start up growth in India).

2. Pro-active content monitoring

2.1. Rule 3 (9) of the Amendment 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.

2.2. The importance of placing greater responsibility on intermediaries for content hosted on platforms provided by intermediaries, cannot be denied in the wake of recent incidents such as the mob violence based on fake news and similar matters. However, to require the intermediaries to *pro-actively* filter content would be grossly unfair and impractical to implement. Intermediaries such as social media platforms may not be able put in place such pro-active censoring mechanisms owing to the volume of information received, processed or hosted by it on a daily basis.

2.3. While intermediaries could potentially develop and launch AI programs to assist with the filtration process, doing so would take an enormous amount of time and investment, not to mention that this would not automatically solve the issues surrounding unlawful content online. Censorship by such platforms would (in addition to introducing AI programs) involve recruiting several moderators, who would then be expected to pore through copious amounts of information and either approve it, or proceed to block access to it. Although this may be done on a reactive basis as and when the intermediary is made aware of such content, requiring proactive censorship on such a wide basis, would be extremely onerous. Notably, several smaller entrepreneurs may not have the wherewithal to undertake cumbersome process during the initial years of their business. Imposing additional costs may also create barriers to competition, entry and un uneven playing field as expensive content filtering technology burdens start-ups and scale-ups. Such moves potentially strengthen the position of only a few well-established players who can afford such tools. This assumes even more importance, in light of the ambiguousness of the term 'unlawful content' (*please see our analysis below*).

2.4. This also appears to be in direct contrast with the notice and takedown process which has heretofore formed one of the pillars of India's safe harbor regime. 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". The Amendment changes would negate the Supreme Court's verdict in *Shreya Singhal v Union of India*, where the court noted the dangers of requiring private parties to adjudge the lawfulness of content on their platforms. It has been well established that Courts and government agencies are much better suited than online platforms to judge illegality of content. Enacting the Amendment is likely to promote mass private censorship and may see a wave of possibly over aggressive content censorship being undertaken by the intermediaries for fear of attracting unwanted attention and liability.

3. Scope of 'unlawful content'

3.1. A key concern that remains unaddressed in the Amendment is the exact scope of what would constitute 'unlawful content'. Rule 3 (2) prohibits intermediaries from knowingly hosting or publishing information which amongst other things may be '*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*'. Several terms such as 'harmful', 'blasphemous', 'obscene' are subjective and may vary from person to person.

3.2. The lack of clarity in the definition of what unlawful content is, may lead to the much-feared censorship creep. Without specific illustrations and reasoned guidelines, ambiguous terms may be susceptible to broad and expanded interpretations, which exceed their legislative intent. For example, unclear definitions of 'hate speech' may be used to suppress legitimate dissent or prevent newsworthy content from being made public. On the other hand, limiting unlawful content to material containing child pornography, rape videos and gang rape videos would be easier to monitor, while at the same time balancing users' right to privacy.

4. Enabling Traceability of Unlawful Content

4.1. As per the Amendment, intermediaries must now enable law enforcement authorities to trace the origins of any unlawful content on their platforms. Essentially, this requirement would disallow true end-to-end encryption for communications (as currently provided by WhatsApp), thus potentially jeopardizing users' right to privacy. Again, while the need to identify offenders cannot be denied, doing away with encryption in totality and thus

restricting the ability for users to express their opinions freely without fear of surveillance, would not be desirable.

4.2. Stakeholders must instead work with the Government to find a solution which strikes a balance between these two seemingly opposing ideas.

5. Checks and balances

5.1. We note that the Amendment does not appear to make any room for checks and balances to be implemented in order to ensure that the power to censor is not abused or overused, both by the Government and the intermediaries, alike.

5.2. It may be useful to have the intermediaries publish reports with details of the agencies who have made requests for take-down, the frequency of such requests, as well as a brief description of the unlawful content. This would, to a certain extent, ensure that newsworthy matters, including any political criticism and dissent is not being supressed under the garb of unlawful content.

6. Other Comments

6.1. The current language lays down a 72-hour response period for all types of requests for information. This is extremely onerous, given the complexity of issues, the wide nature of products and services that may be provided by intermediaries, the vast scope of incoming requests, the availability of content in different Indian languages and dialects, and the likely contextual background. Similarly, fixed turn-around times are not the solution for effective enforcement, and 24 hours are a particularly stringent requirement, with no concrete justification or rationale. They raise significant implementation challenges (e.g., for a company with only a few employees working daytime shifts) and the risk of excessive takedowns that run counter to the fundamental rights of citizens.

6.2. 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 authorized 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 authorized to do so. The last part of new Rule 5, however, restricts agencies to those which are legally authorized to do so. This creates an inconsistency and differential standards for requests for information.

MIT/79/158

1. Points for Consideration

By increasing data-retention periods and granting unfettered discretion to public servants (Rule 8) and opening up encrypted communications and confidential communications (commercial and personal) to multiple players in the ICT industry as well as multiple governmental departments (Rule 9), the proposed Amendments:

a) Amount to arbitrary mass-surveillance (Rule 9)

b) Enable the creation of a Database and Potential Inter-linking of Data/Information within governmental agencies or private entities in the light of increased horizontal integration. The increased periods of data-retention make the database even more attractive for abuse in a global data economy by entities interested in commoditization of not just data but citizens.

c) Undermine encryption and cyber security in times of increased cyber-attacks. Additionally, no replacement proposal has been unveiled to ensure similar, if not greater, cyber security for common IT users in the absence of the limited built-in security

d) Cover all forms of information and data, suppressing the freedoms to speech and expression, to privacy including the right to be forgotten among others. Further, the requirement of some access or information does not *ipso facto* translate into all available information becoming liable to be accessed or processed.

The Amendments link a citizen's data with his or her identity in light of the government IDs or bio-metric IDs (linked to other databases) required for telecom (internet) connections and presents to all the intermediaries, information that an individual may not wish or may not have consented to share with anyone. Also, 'big-data analytics' may place financial, health and geographical information and data together in a manner not consented to by the users.

e) Cater for excessively broad paradigms of potential requirements of government or its agencies on the basis of ill-defined criteria that is highly subjective (Rule 5) while mandating quick essential compliance without

i) similar quick processes of resolution for the users;

ii) public disclosure of such requests, use and results of the same;

iii) legislative oversight;

iv) accountability on part of the government or its agencies;

v) any protection for the civil liberties of the users.

Additionally, surveillance requires criteria that meets judicially and Constitutionally limited benchmarks for narrow well defined and legitimate objectives met in the least intrusive manner possible. The Amendments do not provide a proportionate and stable aka predictable parameter to be enforced.

f) Do not clarify the proposals ensure that 'for-profit' and private organizations carrying out technology-assisted proactive surveillance on private communications-

i) Restricting present and future data mining in any form on such data access and storage across a field famous for horizontal integration.

ii) Processes, Procedures and Infrastructure to ensure compliance with point (a)

iii) Potential technological solutions with reference to point (a)

iv) Accountability and Transparency Measures from the 'Intermediaries' including involvement of external experts and other forms of oversight

v) Penalties to be imposed in case of violation, Guidelines for compensation to the victim(s), Suggested time-periods for remedial action.

g) Trade and Commerce require free communication. Surveillance as well as acquitision of information has potential harmful effects on economic gorwth and accept of technology.

h) Lack of clarity about burden of intimation of surveillance and acceidental exposure and processes and procedures to ensure that due compensation is awarded.

2. Suggestions

It does not appear to be pragmatic or backed by historical evidence (global, within the sub-continent and the Country – discussed below) that 'trust' is enough to assure Constitutionally protected rights of the citizens will be protected and the massive database of extraordinarily sensitive private information will not be utilized, now or in the future, by any unauthorized personnel, government or corporate without providing any substantial safeguards, independent oversight mechanism and economic and criminal penalties for the such violators.

The Rules ought to, regardless of the outcome of the proposed Amendments, to incorporate specific and binding provisions for transparency and accountability mechanism – provisions that ensure that any agency or department requesting information or data declare the same to the Legislature and provide data on the same to the public with the limited but essential exemptions in favor of the nation.

Given that the topic at hand has significantly consequences for the freedoms of Indian citizens, possibly fulfillment of their responsibilities under the Constitution and their participation in the democracy as well as the government's ability to effectively safeguard the citizens, it would be more appropriate to undertake wider-publicized public engagement.

Such public discourse and engagement could be made more meaningful by providing concrete information on:

a) Whether the government has given thought to the causal links of the problems it wishes to solve and anticipated consequences of the interconnections when dealt with only the medium of digital intervention?

b) What studies or analysis, if any, have been undertaken for the cost-benefit analysis in economic, social, political and cultural terms?

c) What studies or analysis, if any, have been undertaken that support implementation of these digital amendments first instead of alternative resolutions to the problems these amendments seek to resolve?

d) Results of a Privacy and Civil Liberties Impact Assessment, if any, conducted.

e) What are opinions of legal and technical experts, if any sought, upon the reliability, cost-effectiveness and non-infringement of the Indian Constitution by these Amendments in achieving their said objectives?

f) What measures and penalties, if any, are being considered to ensure Privacy and Civil Liberties Elements have a forceful and effective voice in the process with the government and private entities?

g) What standard of special legal and technical training and brief, if any, is intended to be imposed and upheld by the actors involved on both sides to ensure compliance with International Law and the Indian Constitution?

3. Human Rights – Protected Online

Without repeating information about national and international laws protecting human rights such as freedom of speech and expression or right to privacy that are well documented and well known, I submit that these 'physical world' human rights subsist with same force in the online world.

For instance, in 2013, UN members got together to observe that "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments."[1]

In December 2013, the UN General Assembly adopted **Resolution 68/167**, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights.[2] ***Privacy*** was reaffirmed as a ***mechanism*** for ***'realization of the right to freedom of expression***'.[3]

Similarly, the UN General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.[4]

The 2014 UN General Assembly Resolution 69/166, 'The Right to Privacy in the Digital Age' follows the Report of the High Commissioner for Human Rights requested in Resolution 68/167.[5] The concerned ***OHCHR Report*** notes that technology can also facilitate violations of human rights via mass surveillance, interception of communications and data collection and expressed concern that mass surveillance 'technologies are now entering the global market, raising the ***risk that digital surveillance will escape governmental controls'***.[6]

---

[1] UN General Assembly Report, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013) - Findings of 15 governmental experts were adopted unanimously by the UN General Assembly.

[2] The Resolution acknowledges the duality of ICT

[3] Resolution 68/167, UN Doc A/Res/68/167, Preamble para 5. - Joyce, Daniel. "PRIVACY IN THE DIGITAL ERA: HUMAN RIGHTS ONLINE?" *Melbourne Journal of International Law*, vol. 16, no. 1, 2015, pp. 270-285.

[4] Resolution 68/167, United Nations High Commissioner for Human Rights, '*The Right to Privacy in the Digital Age'* <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>; Human Rights Council Res. 26/13 U.N. Doc. A/HRC/RES/26/13 (June 20 2014)

[5] The Right to Privacy in the Digital Age, GA Res 69/166, UN GAOR, 3rd Comm, 69th sess, 73rd plen mtg, Agenda Item 68(b), UN Doc A/RES/69/166 (10 February 2015, adopted 18 December 2014) ('Resolution 69/166').

[6] OHCHR Report, UN Doc A/HRC/27/37, 3[3]. - Joyce, Daniel. "PRIVACY IN THE DIGITAL ERA: HUMAN RIGHTS ONLINE?" *Melbourne Journal of International Law*, vol. 16, no. 1, 2015, pp. 270-285.

A potential networked database open for abuse views both 'public and private entities as privacy transgressors' and highlights 'their mutual complicity' though the pressurizing tactics may be employed from one side or the other. However, the eventual victim is always individual freedoms and thus, societal well-being. The OHCHR Report further notes that: [7]

The ***resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating Article 17*** of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.

It may be further noted that compliance with Article 17 (integrity and confidentiality of correspondence) requires that correspondence be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.[8] Correspondence here extends to digital correspondence and communication and expression such as emails, text messages and other forms of messaging online.

4. Freedom of Speech and Expression, Right to Privacy and Surveillance

Cyber communication is the dominant mode of expression of this century – "More and more people express their views not by speaking on a soap box at a Speakers' Corner, but by blogging, tweeting, commenting, or posting videos and commentaries."[9]

Freedom of speech and expression is not a stand-alone right. It is the ***key to other Fundamental and Human Rights***. The protection awarded to a citizen's speech, expression, thought and beliefs or even his privacy is essential to ensure that the public need not fear their conversations and activities are being watched, monitored, questioned and in the present age, monetized.

Right to Privacy, recently recognized as a fundamental right by the Hon'ble Supreme Court,[10] also includes the right to have one's data protected. Digital privacy is a subset of the right to

[7] OHCHR Report, UN Doc A/HRC/27/37, 9 [27]. - Joyce, Daniel. "PRIVACY IN THE DIGITAL ERA: HUMAN RIGHTS ONLINE?" *Melbourne Journal of International Law*, vol. 16, no. 1, 2015, pp. 270-285

[8] General Comment No 16, UN Doc HRI/GEN/1/Rev.9 (Vol. I), [8]. - Joyce, Daniel. "PRIVACY IN THE DIGITAL ERA: HUMAN RIGHTS ONLINE?" *Melbourne Journal of International Law*, vol. 16, no. 1, 2015, pp. 270-285.

[9] Harold Hongju Koh, Legal Advisor to the U.S. Dep't of State, Prepared Remarks before the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) <http://www.state.gov/s/l/releases/remarks/197924.htm. >

privacy. The rights-based approach creates a safety net wherein citizens can exercise control over their data – mandating consent for any kind of usage, processing, sharing with third parties, entitlement to seek removal of data as well as the 'right to be forgotten'.

The right to privacy includes the right to respect for ***digital communications***.[11] And if the Government (or any other entity) infringes the right of privacy, the ***injury spreads far beyond the particular citizens targeted, it intimidates many more***. Collection as well as retention of the communication/content along with the meta-data or other 'physical' links is an infringement of the right to privacy, regardless of whether it is utilized for a purpose of not.

Additionally, the right to a conducive environment for development is also infringed, because people may ***alter their behavior*** if they are under surveillance. The factum of collection of data can cause an individual to ***self-censor*** and affect an individual's ***right to freely seek and impart information.***[12]

For example, the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, asserted that the practice of 'surveillance and intelligence databases undeniably has a ***chilling effect on protestors*** who fear to hold further protests',[13] thus, undermining their freedom of expression as well as ***effective participation in a democracy***.

European Protection Against Monitoring

The European Court of Human Rights has reiterated that the mere existence of legislation which allows for the secret monitoring of communications amounts to an interference with the right to privacy, irrespective of any measures actually taken against individuals.[14]

---

[10] *Justice K S Puttaswamy and Ors v Union of India and Ors*, MANU/SC/1044/2017

[11] See G.A. Res. 68/167 (Dec. 18, 2013); Rep. of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 16-18, U.N. Doc. A/69/397 (Sept. 23, 2014); see also Copland v. United Kingdom, 45 Eur. Ct. H.R. 37 (2007); Weber and Saravia v. Germany, 46 Eur. Ct. H.R. 47, 77 (2006).

[12] Manon Oostveen and Kristina Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' 2016 Amsterdam Law School (Legal Studies Research Paper No 68) 11

[13] Rona, Gabor, and Lauren Aarons. "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace." *Journal of National Security Law & Policy*, vol. 8, no. 3, 2016, pp. 1-33.

[14] See Weber and Saravia, 46 Eur. Ct. H.R. at 78. Rona, Gabor, and Lauren Aarons. "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace." *Journal of National Security Law & Policy*, vol. 8, no. 3, 2016, pp. 1-33.

5. Absence of Proportionality Encourages Abuse: The 2014 NSA Report - Overreach is Likely?

While it is admitted that reconciling seemingly contradictory priorities is a difficult task in itself, historically overreaction and overreach are more likely.[15] Reference may be made to 'The NSA Report' 2014 (result of the US PRISM program) wherein the leading global cyber experts noted that whenever charged with keeping nation or national ideals safe, programs and policies often gone beyond what is necessary and appropriate to protect the nation, and instead take steps that unnecessarily and at times, dangerous jeopardize individual freedom.

The Report presents a well-known fact that US Presidents Johnson and Nixon encouraged government intelligence agencies to investigate 'subversives' for which extensive surveillance and information collection was undertaken. It covered over 3 million people in an attempt to investigate critics as well as expose, disrupt and neutralize their efforts to affect public opinion.[16] When the matter was investigated by the Legislature subsequently, a committee member noted that:[17]

> The government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts…The Government, operating primarily through secret informants, …has swept in vast amounts of information about the personal lives, views, and associations of American citizens.

The NSA Report of 2014 also refers to the Church Committee which noted that looking back years 'too often…intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression. This danger is inherent in very essence of government intelligence programs because '***the natural tendency of the Government is towards abuse of power***' and because men '***entrusted with power, even those aware of its dangers, tend, particularly when pressured, to slight liberty***.'[18] The Committee also noted encourages the natural '***tendency of intelligence agencies to expand beyond their scope***' and to generate ever-increasing demands for new data'. Apprehensions were also expressed about

[15] President's, Review Group on Intelligence and Communications Technologies Staff, et al. The NSA Report : Liberty and Security in a Changing World (Princeton University Press, 2014)
[16] The NSA Report : Liberty and Security in a Changing World (n 15)
[17] The NSA Report : Liberty and Security in a Changing World (n 15) 40
[18] The NSA Report : Liberty and Security in a Changing World (n 15) P 42

the fact that once the intelligence (information and data within the present context) has been collected, there are ***strong pressure to use it***.[19] The Committee cautioned that 'in an era where the technological capability of Government relentlessly increases, we must be wary about the drift towards 'big brother government' and instead put special emphasis on restraints for even future abuse.[20]

Global Application

The rationale behind such repetition of abuse of power is not to cast aspersions but to state a well-documented fact that massive collections of data are often used to the detriment of citizens and their fundamental rights. Examples can be found across the globe. For instance, Thai citizens have found their freedoms and rights impacted by three interconnected elements - mass surveillance, surveillance by the masses, and normalization of surveillance.[21] The use of Cyber-Scouts (form of government-backed cyber vigilantism) and Cyber Witch Hunts (that punish even non-conformity with the majoritarian views and sometimes) is not unique to Thailand.[22]

Similarly, a writer argues that in Ethiopia, the extent of surveillance abuse – perceived and real, has impacted the range of communication and self-expression along economic growth. [23] He contends that 'State incursions also obstruct the flows of domestic and global information exchange, accelerate social divisions among citizens, and ultimately restrict the full capacity of sustainable development.

European Denial of Retention of Data/Information

In 2014 the European Court of Justice determined that a requirement that providers of publicly available electronic communications services or of public communications networks

[19] The NSA Report : Liberty and Security in a Changing World (n 15) P 42
[20] The NSA Report : Liberty and Security in a Changing World (n 15) 43
[21] Laungaramsri, Pinkaew. "Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand 1." *Austrian Journal of South - East Asian Studies*, vol. 9, no. 2, 2016, pp. 195-213.
[22] Pinkaew (n 21). It also finds a parallel in the Chinese government-backed '50-cent bloggers' used to promote pro-regime information and detect as well as file complaint(s) for action against expressions deemed unfit. Katrien Jacobs, People's Pornography: Sex and Surveillance on the Chinese Internet (Intellect Books Ltd, 2012) 50. The same author also quotes a Chinese student as observing that 'If we restrict our internet and we Chinese cannot protect our voices, then the whole world will only hear those other voices'. Though made within a specific context distinct from the present discussion, the essence of the statement is still important – freedom of expression must be protected, and non-proportionate measures that have been documented to adversely impact the same are Constitutionally invalid.
[23] Grinberg, Daniel. "Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia." *Surveillance & Society*, vol. 15, no. 3, 2017, pp. 432-438.

retain, for a certain period, data relating to a person's private life and to his communications, for the purpose of possible access to them by the competent national authorities, directly and specifically affects private life and consequently, violates relevant articles of the EU Charter of Fundamental Rights.[24]

Dangers of Mass Surveillance

In a 2013 meeting of the UN Human Rights Council, the High Commissioner noted that the threat which mass surveillance poses to human rights is among the most pressing global human rights situations today.[25]

A 2015 survey (though small in scale) found that "Levels of concern about government surveillance in democratic countries are now nearly as high as in non-democratic states with long legacies of pervasive state surveillance", resulting in erosion of faith that the government will respect their freedom of expression or rights to privacy.[26] Almost one-third of the respondents admitted to avoiding particular topics and some expressed apprehensions about even researching certain topics or expressing certain views publically due to fear of negative consequences.

To quote US Supreme Court Justice Robert H Jackson - without clear limitation(s), "a federal investigative agency would 'have enough on enough people' so that 'even if it does not elect to prosecute them, the government would…still 'find no opposition to its policies' 'even those who are supposed to supervise are likely to fear them".[27]

[24] See Case C-293/12, Digital Rights Ireland, 43, at 29-34. Rona, Gabor, and Lauren Aarons. "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace." *Journal of National Security Law & Policy*, vol. 8, no. 3, 2016, pp. 1-33.
[25] Guild, Elspeth. "What does Mass Surveillance do to Human Rights?" *OpenDemocracy*, May 12, 2014
[26] "US Mass Surveillance Curtails International Freedom of Expression: Watchdog." *The Philippines News Agency (PNA)*, Jan 06, 2015.
[27] The NSA Report : Liberty and Security in a Changing World (n 15) 43

Background

At the outset, The Dialogue would like to thank the Ministry of Electronics and Information Technology (MeitY) for holding a public consultation on the Draft of *The Information Technology [Intermediary Guidelines (Amendment) Rules], 2018*. We commend MeitY for adopting a multi-stakeholder consultative approach.

The Internet is a pioneer human invention that enables free speech and sharing of information. Intermediaries are platforms that use capabilities of the web to act as platforms where information is shared. This includes messaging platforms, social media sites, payment companies, online marketplaces, blogs and video sharing sites [1]. These platforms themselves are not 'publishers of content', but rather serve as the place where user content is shared. This raises the question of whether these intermediaries should be held accountable for the content that is shared on their platforms, and what responsibilities and protections come with hosting Indian user content.

The amendments to the draft IT Intermediary Guidelines, 2018, is a new phase in this debate. Trying to regulate advancements in technology is not an envious job. Regardless of the stance taken by any regulator, there are bound to be differences in opinion with industry and civil society. This applies to the current IT Intermediary Guidelines as well. To that extent, The Dialogue appreciates MeitY's call for comments[2] on the issue as a step towards developing a progressive discourse on the same.

The Dialogue's position on the recent amendments is summarised in the points below and will be elaborated in the following sections. As an organization, The Dialogue hopes that our comments will add value to the debate on the issue. Being involved in the intersection between technology and policy, the policy issue related to intermediary liability is of great interest to us. We hope that the dialogues between relevant stakeholders should continue to evolve as progress in discourse is instrumental for how technology is incorporated in a Digital India.

[1] "A serious and imminent threat to the open Internet in India - MediaNama." 22 Jan. 2019, https://www.medianama.com/2019/01/223-a-serious-and-imminent-threat-to-the-open-internet-in-india/. Accessed 28 Jan. 2019.

[2] "Comments/suggestions invited on Draft of "The Information ... - MeitY." 10 Jan. 2019, http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9C-information-technology-intermediary-guidelines. Accessed 28 Jan. 2019.

Whether the amendments should have been brought through Section 79 of the IT Act, 2000?

Excessive Delegation: The proposed draft rules have gone beyond scope of the provisions of the parent act and erodes the safe harbour protection available to intermediaries under section 79 of the IT Act. As noted in the landmark judgement of *Shreya Singhal v. Union of India,* the intermediary is called upon to exercise its own judgment under Rule 3 sub-rule (4) and then disable information, when intermediaries by their very definition are only persons who offer a neutral platform through which persons may interact with each other over the internet. Thus, it then solely depends upon the intermediaries subjective sense, to take down content, which has a chilling effect on freedom of speech and expression. The requirement for intermediaries to subjectively determine the legality of an expression should be replaced with an objective test. The objective test should be such that it does not create an obligation for the intermediary to go into the adjudication of a legal claim or into the investigation of facts and circumstances.[3]

Lack of procedural safeguards: The Rules are procedurally flawed as they ignore elements of principles of natural justice and lacks safeguards. Under the rules, the third party provider of information whose expression is censored is not informed or made aware about the takedown, let alone given an opportunity to be heard before or after the takedown. There is no redressal mechanism for the aggrieved user or third party uploading or providing the content, to appeal the decision of the Government agency in the courts.

Lack of transparency and accountability: The intermediary is under no obligation to provide a reasoned decision for rejecting or accepting a takedown notice. There is also no requirement for disclosure or transparency in the takedown process. The Rules do not prescribe any recourse for an intermediary even if such intermediary knows that the takedown notice is frivolous and that the process is being abused. The results demonstrate that the Rules do not establish sufficient safeguards to prevent misuse and abuse of the takedown process

[3] Rishabh Dara, 2011, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, The Centre for Internet and Society, Available at https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf.

to suppress legitimate expressions. This clearly induces the complainant to abuse the takedown process to suppress free expression without worrying about the repercussions. Specifically, in *Union of India v. Tulsiram Patel*[4], the Supreme Court held that the principle of natural justice required the satisfaction of the audi alteram partem rule, which consisted of several requirements, including the requirement that a person against whose detriment an action is taken be informed of the case against him and be afforded a full and fair opportunity to respond. In, *M.C. Mehta v. Union of India*[5] the Supreme Court held that the absence of due notice and a reasonable opportunity to respond would vitiate any holding to the right holder's detriment.

[4] AIR 1985 SC 1416
[5] AIR 1999 SC 2583

Rule 3(2) - Privacy Policy

"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 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."

The amended rules hereinabove risk misinterpretation as the draft rules have not identified any proposed metrics to determine how such online content may harm public safety and critical information infrastructure, which is also in contravention to the ruling Supreme Court gave in the Shreya Singhal judgment.

Moreover, Rule 3 (2) of the Intermediary Guidelines, which lists the grounds for censorship, is not compliant with Article 19(2). Many of the grounds mentioned have no constitutional basis whatsoever. Rule 3 (2) prohibits, *inter alia*, content which is "grossly harmful", "harassing", "invasive of another's privacy", "hateful", "disparaging", "grossly offensive" or "menacing". Since the whole scheme of the Intermediary Guidelines is premised on these extra-constitutional grounds, they are, subject to being to being struck down. In *Romesh Thappar v. State of Madras*,[6] the Supreme Court held very narrow and stringent limits govern the permissibility of legislative abridgment of the right of free speech. Ordinarily, any abridgement of free speech by means of censorship must be compatible with one or more of the grounds provided for under Article 19 (2), and the Supreme Court held in *Express Newspapers (Private) Ltd. v. Union of India*, [7] that limitations on the exercise of the Article 19(1)(a) right which do not fall within Article 19(2) cannot be upheld.

In addition to the proposed amendments to Rule 3(2) are over-broad and vague. In *Kartar Singh v. State of Punjab*[8],at para 130-131, it was held:
"It is the basic principle of legal jurisprudence that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several

[6] AIR 1950 SC 124
[7] AIR 1958 SC 578
[8] (1994) 3 SCC 569

important values. It is insisted or emphasized that laws should 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. Such a law impermissibly delegates basic policy matters to policemen and also judges for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. More so uncertain and undefined words deployed inevitably lead citizens to "steer far wider of the unlawful zone ... than if the boundaries of the forbidden areas were clearly marked."

Therefore it is recommended that the amendments are reconsidered as it is in violation of basic principles of legal jurisprudence.

Rule 3(4) - Reminders

"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."

In today's hyper connected age, first it must be noted that intermediaries already provide such information as part of their standard operating procedures and any additional requirement to enhance accountability may in fact end up increasing compliance cost to the intermediaries Second, it is important to note that an average mobile user subscribes to services provided by multiple intermediaries and such monthly reminders would lead to notification fatigue.

Separately, research has shown that users do not generally read the terms of service of the platform and click through them. It is recommended that the obligation should be voluntary and intermediaries should explore innovative means to build user awareness about their platform's policies.

Rule 3(5) - Traceability and Request for Information

"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 Guidelines have a provision that requires intermediaries to trace out the originator of information on its platform should the Government require so for the purpose of law enforcement as well as provide such information and any such assistance required by legally authorized government agencies within 72 hours of communications.

One of the biggest consequence of enabling this tracing mechanism is a challenge to end to end encryption. In simple terms, for intermediaries to monitor content, they would have to know what the content is, which may threaten what end to end encryption stands for. It is important to note that there are openly available open source technologies which are openly available which can be used for anonymous communication. For example, the onion router (TOR) can be used to conceal identity. Therefore, it is important to further examine this issue and hold a larger consultation on traceability. Access to data for law enforcement purpose is justified, but it cannot go without transparency and due process of law.

This provision has broader implications in terms of rights and legal principles in India. Firstly, this goes directly against the precedent set by the *Shreya Singhal* judgment which clarified in 2015 that companies would only be expected to remove content when directed by a court order to do so[9]. The other principal that the provision will break is the right to privacy. In today's world, the digital communication that we have is akin to actual conversations and

[9] "Mozilla List 5 Concerns on New Draft Rules on Intermediary Liability in ...." 3 Jan. 2019, https://www.dqindia.com/mozilla-list-5-concerns-new-draft-rules-intermediary-liability-india/. Accessed 29 Jan. 2019.

tracing 'who said what' is a clear digital infringement on the consumer-citizens fundamental right to privacy.

An adverse impact in terms of rights and principles does not occur in a vacuum. Requiring traceability and breaking end to end encryption can have real economic consequences for India. Should companies fail to offer privacy to their customers, it may serve as a deterrent to the entry of new intermediaries in India. A slew of apps pride themselves in providing their consumers with encrypted messaging services ensuring their privacy. .Any intermediaries that stand by their policies on maintaining encryption would also be deterred by the precedent that their technology can be used as a mechanism to to trace its consumers and spy on them.

For firms that are already competing in Indian app stores, these provisions might trigger a rethink on their investments in India going forward, as well as rolling out any new technologies that they have already come up with. There are already examples of this with apps such as Messenger dealing with regulation in different spheres. In the UK, the popular messaging service recently rolled out a payments feature that allows consumers to make and receive payments in the app[10]. However, the same technology is yet to come to India. This is a concern because in-app payments have the potential to increase the number of cashless transactions in India, however, this potential is yet to be harnessed because of data regulations. At the same time, mandating intermediaries to provide information within 72 hours of notification is a challenge to the principles of 'due process of law', which requires any request for data disclosure to be clear, transparent, and open to review or challenge.

[10] "Facebook Messenger payments comes to UK - BBC News." 6 Nov. 2017, https://www.bbc.co.uk/news/technology-41894014. Accessed 29 Jan. 2019.

Rule 3(7) User Base and Incorporation

"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 new amendments suggested by MeitY apply to any intermediary with a user base of 50 lakh. Companies with a user base at or above this number will have to have a permanent registered office in India with a physical address. The entity will also have to appoint a nodal person to facilitate interactions with the Indian government to work towards compliance with legal provisions. Before we begin to question the problems with the implementation of this provision, it is important to question the methodology used to devise this 50 lakh benchmark and the kind of users it is referring to.

India today has ~350 million internet users[11] so 50 lakh would cover ~1.4% of the country's user base. A large number of intermediaries will have a user base of 50 lakh. However, the guidelines are not clear about the kind of users they are referring to, daily active users, monthly active users or registered users. If left undefined, it will create a sense of arbitrarily imposed ambiguity which will give the government perennial benefit of the doubt over any legal cases that may involve this amendment.

This brings us to concerns regarding the implementation of this measure. Any intermediary with a 50 lakh user base will need to have a physical office in India. At the same time, we need greater understanding on how this will be enforced.

So if the government was to come up with a category of users (daily/monthly active), how would they plan on getting these numbers from possibly thousands of intermediaries which may have this large a base? Secondly, the current scenario on top level intermediaries is well cut out in terms

[11] "India's internet user base crosses 350 million: IAMAI - Times of India." 2 Sep. 2015, https://timesofindia.indiatimes.com/tech-news/indias-internet-user-base-crosses-350-million-iamai/articleshow/48773098.cms?from=mdr. Accessed 28 Jan. 2019.

of big players, but considering smaller players will the government ban an app from the Play Store/App Store that doesn't set up a physical office in India? Apps do not fill out government forms and seek public approval when they are rolled out, instead, they appear on app stores. Going forward, what mechanism does the government intend to use when new(er) apps are rolled out and reach 5 million users? We believe that there has to be a standard process in place for how it will cope up with advancements.

In addition to this, such a requirement would also outlaw important global services which do not have a local presence or do not have the resources to set up such an entity. For example, Wikipedia is run by a non-profit NGO Wikimedia Foundation. Wikipedia, an intermediary, which is one of the most visited websites in the world would be in violation of the law if the requirement for local incorporation is enforced.

Should the government set up an implementation process that addresses these concerns, we also have to consider what that might mean for the influx of new intermediaries in the Indian market. Successful regulation might mean a lack or absence of desire for said intermediaries to set up shop in India by acting as a deterrent.

Rule 3(8) - Take Down Requests

"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 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."

The draft rules mandate intermediaries to disable access to 'unlawful' content without the requisite procedural safeguards. Such requests can only be made under Section 69 (A) of the IT Act. Similarly, the provision for retention of data should come under Section 67 (A) of the IT Act.

Additionally, the usage of the word 'associated records' is vague and arbitrary, which violates Right to Privacy. There is no clarity as to what or how much information precisely must be held in the form of "associated records". The Intermediary Guidelines though include limits on the scope of disclosures that government agencies can demand or expect to retain in accordance with Article 19(2), however, do not define what type of data to be retained which is in contravention of Article 21. The vagueness in the data retention provision violates the obiter dictum of *PUCL v. Union of India*[12] too.

[12] AIR 1997 SC 568

Rule 3(9) - Proactive Monitoring of Content using automated tools

"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 intermediary guidelines of 2018 serve as a clampdown on 'unlawful' content. The issue with proactively trying to censor content is that its effects can spill over into over-censorship and impact the freedom of speech, internet is supposed to enhance and enable. There are multiple categories on basis of which intermediaries are supposed to regulate the content that is displayed on their website. According to the guidelines, intermediaries can be asked to remove 'unlawful' content if it is:

1. In violation of decency and morality
2. Public Order
3. Impacts the Sovereignty and Integrity of India
4. Security of State
5. Friendly Relations with the Foreign States
6. In Relation to Contempt of Court
7. Defamation or Incitement to Offence
8. Grossly Harmful
9. Harassing
10. Blasphemous
11. Defamatory
12. Obscene
13. Pornographic
14. Paedophilic
15. Libelous
16. Racially or Ethnically Objectionable
17. Invasive of Another's Privacy
18. Hateful
19. Disparaging
20. Relating or Encouraging Money Laundering or Gambling
21. Otherwise Unlawful in Any Manner Whatsoever

There are concerns over some of the terms used here to determine what content will be removed from intermediary platforms. While some categories, such as pornography and pedophilia can be identified and removed, terms such as 'Otherwise Unlawful in Any Manner Whatsoever', 'In violation of decency and morality' are ambiguous and can be used as a basis to over-extend scope of regulation and 'chill' freedom of speech[13]. The Rules are erroneous in nature about the requirement to proactively

[13] "Mozilla List 5 Concerns on New Draft Rules on Intermediary Liability in ...." 3 Jan. 2019, https://www.dqindia.com/mozilla-list-5-concerns-new-draft-rules-intermediary-liability-india/. Accessed 28 Jan. 2019.

identify 'unlawful information or content'. The phrase is vague and may lead to excessive censorship. It should be understood that these rules are made in context of Section 79 of the IT Act which is an enabling provision. Again, it should be remembered that these draft rules do not create new offences but only provide conditions for immunities from offences that are defined in other laws such as the IPC. The phrase 'unlawful information or content' goes beyond the limits of expressions used in Article 19(2) of the Indian Constitution.

So while there are categories that are easily justified as grounds to remove content from intermediaries, there are also terms that overextend the reach of censorship and regulation. These vague parameters can have an adverse impact on people's freedom of speech and do not specify whether it applies to content that is shared by foreign nationals but might appear on Indian feeds. For better and more specific implementation of the guidelines, it is best to narrow down such ambiguous definitions and instead use a standards-based approach to defining unlawful content. This would provide the state with more credibility and companies with a framework to operate within.

The Rules focus on earlier proposed idea[14] of pre-censorship of online content. This imposes an obligation on intermediaries to take down content rather taking on liability. Due to the emergence of technologies, intermediaries also deploy Artificial Intelligence to eradicate 'unlawful' content. However, there are several incidences where AI has proved to be inaccurate.[15] The draft intermediary rules have implications for free speech rights of users with requirements for automated content removal and an array of ambiguous terms used to categorise content deemed unlawful. While it is true in light of the Supreme Court's holdings in *Prakash Jha Productions v. Union of India*,[16] that pre-censorship is permissible within the Indian constitutional scheme, this permissibility is qualified. For example, prior censorship may be undertaken only within closely regulated circumstances, such as under the grounds in the Cinematograph Act, 1952, and even then, only by an

[14] https://india.blogs.nytimes.com/2011/12/06/any-normal-human-being-would-be-offended/

[15] Facebook, using its automated tools deleted a post by Norwegian Prime Minister, Erna Solberg. The post showed Pulitzer Prize winning photograph, "napalm girl" from the vietnam war. The photo was used to showcase that how history has changed the warfare, but, AI tools saw it as a pornographic content and removed it. Available at https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row.

[16] (2011) 8 SCC 372

appropriately empowered governmental entity. Herein, the Intermediary Guidelines create mechanisms for the abridgement of the freedom of speech which amount to indirect and unjustifiable prior censorship, contrary to Article 19 (2)

Therefore, there should be a balanced approach, and, when Intermediaries platform is abused for transmission of allegedly obscene and objectionable contents, the intermediaries/service providers should not be absolved of responsibility. A definite obligation should be casted 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 cyberspace 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.

Recommendations and Way Forward

There is currently raging debate on the amount of responsibility intermediaries have over the content and information that is shared on their platforms. The Dialogue recommends that the following policy actions be taken for the sake of progressive discourse on the issue:

Outlining a System for Implementation

The Guidelines set out certain provisions for intermediaries with a user base of more than 5 million. Any intermediary meeting these requirements is to have a physical office in India and should also appoint a nodal official in charge of interactions with the Indian government. As of today, this legislation can easily target big companies under these laws. However, there is no mention of how these requirements will be implemented on intermediaries that are smaller but still significant in the Indian market? Does the government plan to ban any intermediary that has 5 million users but does not set up a physical office in India? More fundamentally, how does the Government plan to determine whether or not an intermediary has 5 million users? Will all new intermediaries appearing on the App Store/Play store be continuously required to share their user numbers to implement the measure? There are several questions regarding the implementation of this provision that need to be answered. The Dialogue recommends coming out with a mechanism that addresses these queries.

The Need for a Problem Statement

There have been a number of tech policy announcements by the government in recent memory that have proven to be contentious. There was the call for data localization presented in the Justice Srikrishna-led committee on data protection, the notification by RBI that called for the same in the financial sector, and the MHA notification that empowered 10 agencies to intercept data. A common theme across all of these measures, as with the revised intermediary guidelines, is the lack of a problem statement and how the proposed measures are expected to act as a solution in achieving the same. Providing the world with well-defined goals that the state wants to accomplish can also serve as an important indicator to the private sector on what the government wants to accomplish and how they have planned on getting there. This would lay a better foundation for the facilitation of a public-private partnership

and also ensure that the two entities collaborate more to reach a common goal instead of competing without knowing what the other is trying to achieve. In this case, providing a concept note on what intermediary liability is supposed to accomplish and discussing the same in a multi-stakeholder meeting could lead to representing more diverse interests and also possible multilateral solutions to a common goal.

Eliminating Ambiguity and Establishing Standards on Definitions of Unlawful Content

A point of contention in the intermediary guidelines is that some of the parameters set for intermediaries to remove unlawful content (by automated means or manually after receiving 'actual knowledge') are vague. For instance, consider the two phrases that were cited as reasons among the total 21 causes, 'in violation of decency or morality' and 'unlawful in any manner whatsoever'. The problem with such vague provisions is that they can be seen as the equivalent of handling the government a blank cheque. So while an intermediary does not have control over what a user may post on its platform, it can be asked to take down that content if it is arbitrarily deemed as unlawful by senior government officials. Frequent usage of this provision can have consequences on the trust users place on the platform. It would be better for all parties if the government sets clearly defined standards, backed with rationale on what content it deems to be (un)lawful. This would help maintain consumer trust and also allow intermediaries with a defined framework to function within.

Complying with Article 14 of the Constitution

Reasoned state action must recognize that their liabilities must necessarily vary with the specific type of service that each provides. The Intermediary Guidelines fail to do so, and are consequently incompatible with Article 14. There needs to be a classification made with respect to the type of intermediaries. A singular watertight formula cannot be applied to all intermediaries. There needs to be a tactical separation between User Generated Content space and Curated Content providers. The guarantee of "equal protection of laws" requires equality of treatment of persons who are similarly situated, without discrimination *inter se*. It is a corollary that

that people differently situated cannot be treated alike.[17]

Once the government recognises different types of intermediaries, a differential regulation needs to be established as well. Intermediaries can be classified into: 1) ISPs, 2) Data processing and web hosting providers, 3) Internet search engines and portals, 4) E-commerce intermediaries and online aggregators, 5) Social Media and Messaging Platforms /Participative Networking Platforms. Distinct classes of intermediaries should be created and due diligence requirements be assigned as per the functions performed by each of intermediaries.

[17] E.P. Royappa v. State of Tamil Nadu, AIR 1974 SC 555. See also, M/S Sharma Transport v. State of Andhra Pradesh, AIR 2002 SC 322, Mahesh Chandra v. Regional Manager U.P. Finance Corporation, AIR 1993 SC 935.

MIT/79/160

We present the following demands for consideration in addition to the request.

1. **Kindly wait for a strong data privacy law before permitting wider use of Personally Identifiable Information.**

India doesn't have a data protection law. We have seen numerous reports of data leaks which are cases of malicious intent and criminal behaviour, we don't have a stringent data protection bill which has a framework for Govt, Private & Intermediaries. A data privacy law is required to facilitate the lawful use of Personally Identifiable Information given by due consent by an Indian citizen to 'appropriate government' or an 'intermediary'. Such a law would also bring in safety measures, checks, accountability, due procedure to be followed when requesting data and what punishment should be given in case of non compliance by the government and the intermediaries.

2. **Only courts orders should empower data requests or termination of services by the Intermediary.**

The amendment in Section 8 empowers any 'appropriate government' issuing a 'lawful order' to request Personally Identifiable Information or terminate access to services by Intermediaries, however the time to respond to such a request is only 72 hours in case of data requisition or 24 hours in case of termination of service. There is no scope for the Intermediary to challenge the lawful validity of an order at appropriate judicial courts. There are numerous instances of government departments and agencies continuing to use antiquated laws which has been changed / improved by newer regulations, laws or court orders / judgements. Thus lawful validity of orders can only be ensured when courts are approve data requisition.

3. **No automatic measures as it would legalize mass surveillance & mass censorship while being ineffective to restrict fake news, hate speech or misinformation.**

Corporations like Google, Facebook, Whatsapp are being investigated by various governments across the worlds for their mass surveillance and misuse of Personally Identifiable Information. The proposed amendments through its

mandate in Section 9 legalizes the harvesting of data by Intermediaries. The technological tools employed are unequipped to handle the complexity of data. This is evident by the numerous amounts of accounts blocked by Youtube due to misidentification of uploaded content. A similar mandate by the European Union named 'Article 13' was opposed by the general public and the Intermediaries as it is not accurate. The mandate also requires the Intermediaries to proactively block content and disable public access to the same. This is a responsibility of the government which should not be offloaded to the Intermediary.

MIT/79/161

ASSOCHAM Suggestions on

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

The Associated Chambers of Commerce and Industry of India ("ASSOCHAM") is the oldest Apex Chamber of India representing the interests of trade and commerce in India, and acts as an interface between issues and initiatives. The goal of ASSOCHAM is to promote both domestic and international trade, and reduce trade barriers while fostering conducive environment for the growth of trade and industry of India. Several of ASSOCHAM's members are key constituents of the digital ecosystem and are committed to working with the government to realise the vision of a Digital India.

Some of our members are telecom and online service providers who are classified as "intermediaries" under the Information Technology Act ("IT Act"), acting as channels of communication and trade among others. Intermediaries now constitute a core part of the digital economy and have transformed the way Internet users consume content, communicate with others, and conduct business online. In this regard, the regulatory framework governing them is key to the continued role of the Internet in providing platforms for communication, business and sharing content to the Internet users in India.

The ability of intermediaries to innovate and operate responsibly has been made possible through carefully designed legal frameworks regarding liability for illegal third-party content. Also known as safe harbours, these laws guarantee that as long as the intermediaries meets certain conditions, they are not liable for the third party information, data, or communications links which is generated by its users. These laws treat intermediaries differently from the author or publisher of the content served, linked, or hosted and exempts them from liability in case their role is limited to providing access to a communication system, or where the intermediary has neither initiated the transmission nor selected the receiver nor modified the information contained in the transmission and where the intermediary has observed due diligence/ guidelines issued by the Government from time to time.

The Ministry of Electronics and Information Technology ("MeitY") had in this regard, notified the Information Technology (Intermediaries Guidelines) Rules, 2011 ("Intermediary Guidelines") under the IT Act.

MeiTY has now taken an initiative to engage with the stakeholders on the changes occurring in the areas of information technology in recent times by introducing the draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 ("Draft Rules") which amend the Information Technology (Intermediaries Guidelines) Rules, 2011 ("Intermediary Guidelines") under the IT Act.

We welcome this engagement, however, as representatives of several intermediaries which provide services in India, we believe that several of these proposed amendments are out of step with the need of the hour.

We also believe that the proposed data protection framework as recommended by the expert committee headed by Hon'ble Justice B.N. Srikrishna (Retd.), will have an important bearing on the Intermediary guidelines and therefore, it may be desirable that the data protection framework is finalized before any amendments are introduced in the Intermediary Guidelines.

We also believe that any changes in this framework relating to Intermediaries should not create an onerous or impractical burden and should also keep in mind the need to facilitate the intermediaries in performing their functions in order to enable the digital economy to grow in line with global trends. It may be appreciated that overly restrictive obligations will stifle the Internet user's experience, curtail the growth of the digital sector, and affect business of all the players in this economy. We also believe that intermediaries should not be held liable for any third party information, data or disputes as provided in the safe harbour provisions under Section 79 of the IT Act.

In this context, ASSOCHAM would like to take this opportunity to highlight certain concerns with respect to the Draft Rules, as some aspects of the proposed amendments are likely to have a suppressive effect on the digital arena in India and are even contradictory to some existing positions of law and policy in India. ASSOCHAM is grateful to have the opportunity to engage with the MeitY on the Draft Rules and would like to recommend that any amendment to the Intermediary Guidelines be considered after the proposed data protection framework is in place.

Our specific concerns in relation to the provisions of the Draft Rules are set out below.

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.

1. Rule 3(2)

Existing Provision	Proposed Amendment
(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,	(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 —	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; (k) threatens critical information infrastructure.

The existing Rule 3(2) of the Intermediary Guidelines prescribes that intermediaries must inform their users that certain types of content should not be hosted, displayed, uploaded, modified, published, transmitted, updated or shared on the platform provided by the intermediary – failing which [under Rule 3(4)]such content could be removed and the user's access to the platform could be terminated.

The Draft Rules add two additional types of content that cannot be hosted, displayed, uploaded, modified, published, transmitted, updated or shared: (i) content that threatens public health or safety (promotion of cigarettes and other tobacco products, and intoxicants including alcohol and Electronic Nicotine Delivery Systems); (ii) content that threatens critical information infrastructure.

Our concerns with regard to the proposed amendment are as below:

a) *Vagueness*: We would like to submit that these two clauses of the Draft Rules have been drafted very broadly and do not identify the particular kind of content that are meant to be restricted from publication. There is no guidance in the Draft Rules as to what would be considered to be 'threatening' to public health or safety and critical information infrastructure, or what would be considered to be 'promoting' intoxicants.

b) *Constitutionality*: In this respect, we would like to submit that terms such as 'threaten' and 'promotion' suffer from the same kind of vagueness that caused Section 66A of the IT Act to fall afoul of the right to freedom of speech and expression guaranteed under Article 19 (1) (a) the Constitution of India. In the case of *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act, which restricted speech on the grounds of being 'menacing', 'causing annoyance, inconvenience, danger', 'grossly offensive' etc. for being 'unconstitutionally vague'.

c) *Exceeds Applicable Law:* On tobacco related content: the prohibition on tobacco is captured in Section 5 of The Cigarettes and other Tobacco Products (Prohibition of Advertisement and Regulation of Trade and Commerce, Production, Supply and Distribution) Act, 2003 which only prohibits 'advertisements' of tobacco related products and not 'promotion' of any and all content. A distinction must be drawn between advertisements that are paid for, and all other forms of content. Therefore, Rule 3 (j) is beyond the scope of the Cigarette Prohibition Act.

d) *Distinction between Advertising and Content:* 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.

e) *Out of Scope Governing Laws:* The proposed sub-rule relies on the Drugs and Cosmetics Act which is not the governing statute for the subject matter sought to be covered in this sub-rule, at least insofar as cigarettes and alcohol are concerned. At best it only covers use of 'nicotine.' In any case even the Drugs and Cosmetics Act only prohibits advertisements and is content neutral, therefore it cannot be the overarching legislation to determine the scope of these subject matters. Restrictions on alcohol advertising are specifically provided for under The Cable Television Networks (Regulation) Act 1995 *("*CTNA") and Cable Television Networks Rules, 1994 *(*"CTNR") - which is limited in its scope and coverage to the electronic media. By this rule, there is an attempt to legislate for the online world - that can only be done through the parliamentary process. Even otherwise, even the Cable Television Networks Act only restricts ads and not all forms of content which relates to cigarettes or alcohol.

f) *Sufficient Laws Already Exist:* Critical Information infrastructure is defined in the IT Act as "*...the computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety*." There are separate provisions within the IT Act that address the issue of threatening critical information infrastructure (e.g. Sec 70), and have framed detailed Rules for their implementation [Under Sec 70A(3), the Information Technology (National Critical Information Infrastructure Protection Center and Manner of Performing Functions and Duties) Rules, 2013]. Existing rules, therefore, cover for various aspects of protecting critical information infrastructure and there is a complete code both in terms of statutory provisions and enabling rules. Further, Sec 70B provides for the establishment of CERT and its functions and roles, which include handling cyber security incidents. The scope of CERT's powers as laid down in the Act and in the Information Technology (The India

Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 would cover what is intended to be covered under the proposed sub-rule (k). Further, Sec 70B(7) of the Act provides for penal provisions that not only provide for substantive steps to be taken, but more importantly also lay down the penalties to which intermediaries will be subject for non-compliance with such provisions.

g) *Double Jeopardy:* This sub-rule that would operate as a condition precedent for intermediaries to avail of the safe harbour protection is untenable and overreaching. It may also amount to double jeopardy for intermediaries that as they be liable for penal provisions under sec 70B(7) and additionally, will risk the loss of their safe harbour protection.

Broadly worded restrictions are against the spirit of providing a safe harbour for intermediaries, and are also challenging to enforce. From the perspective of users, ambiguous restrictions on the types of content that can be shared will have a chilling effect on the freedom of speech and expression, which is safeguarded by the Indian Constitution.

2. Rule 3(4)

Existing Provision	**Proposed Amendment**
(5) The Intermediary shall inform its users 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 lights of the users to the computer resource of Intermediary and remove non-compliant information.	(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 existing provision prescribes that intermediaries 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 that intermediaries inform their users regarding the above at least once every month.

This provision creates a highly onerous burden on intermediaries without any corresponding public benefit. Users of any service can access its Terms of Use at any

time, which are published by intermediaries in accordance with Rule 1 of the Intermediary Guidelines. Monthly reminders are more likely to create warning fatigue and dissatisfaction among users, instead of increasing their awareness of this provision. Collective industry experience shows that repeated display of caution notices or warnings results in user fatigue and they reach a point when they no longer pay any attention to such notices. Users will end up receiving a deluge of such messages from all the service providers whose services they have signed up to - thereby completely defeating the purpose.The manner of doing this needs to be clear given that accessibility of these terms is the main objective here. Therefore, these should be limited to displaying them by publishing on the website (other modes may be a bit intrusive)

Additionally, the Government also needs to play an equal role by framing policies and taking necessary measures to educate citizens at grassroot level and creating awareness amongst people. The Government is in the strongest position to take proactive measures to educate the people in this regard.

3. Rule 3(5)

Existing Provision	Proposed Amendment
(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. 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.	(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 existing Rule of the Intermediary Guidelines requires intermediaries to provide information or assistance when required by lawful order. The Draft Rules amend this rule significantly. The problems in this regard are as follows:

a) *Time limit of 72 hours*: The Draft Rules mandate a time limit of 72 hours within which intermediaries will be required to provide the information or assistance. This time limit

is entirely arbitrary and may be very difficult to comply with in terms of practical implementation. This duration does not allow the intermediaries the time to analyse the request, respond appropriately or request a hearing. It is also important to note that these guidelines a bit wide and are open to diverse interpretations, at all places they need to be qualified to clearly state as when and in what situations these obligations come into play e.g. in the case of Public order/Crimes involving threat to life/security the response within 72 hours may be vital, however to extend it to all scenarios is a bit overarching.

The time limit is also extremely onerous, given the complexity of issues, the wide nature of products and services that may be provided by intermediaries, the vast scope of incoming requests, the availability of content in different Indian languages and dialects, and the likely contextual background. Having an aggressive response time line for all content categories may result in that requests with genuinely urgent needs are pushed down the queue and are not dealt with the priority that they deserve to be dealt with, especially with players that have fewer resources to dedicate to enforcement efforts. In general, imposing short turnaround times inhibit companies from carefully considering the merits of each supposed investigation/request. The risk of excessive requests runs counter to the fundamental rights of citizens in India. Requests for basic subscriber information and content data are governed quite differently by foreign data protection and data sharing laws, making the same 72 hour threshold for both kinds of requests unrealistic and often infeasible.

It is thus recommended that the 72 hour response timeline should be dropped, as it can be technically unfeasible, and also procedurally impossible to comply with. Alternatively, this requirement should be confined to such narrowly but clearly defined emergency/urgent action 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.

b) *Vagueness*: The Draft Rules specify that the 'information or assistance' can be asked for by *any* government agency. It further states that assistance can also be requested in respect of "security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security". This portion of the Rule is highly unclear, as there is no guidance or system of checks and balances as far as the following are concerned:

    - The meaning of 'information and assistance', which may be interpreted broadly by government agencies;

- Whether *any* government agency can seek information or assistance by lawful order, or there are limitations and procedural safeguards in respect of this power;
- Any procedural safeguards to maintain transparency.

It is recommended that any such requests should only be made by lawfully authorized and duly designated Government agencies or through judicial orders.

c) *Increased Scope and Contradictions:* 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 and duly designated to do so.

Further, the last part of new Rule 5, however, is restricted to agencies to those which are legally authorised to do so. This creates an inconsistency and differential standards for requests for information.

d) *Mode of communication of data requests*: The proposed amendment includes requests made by electronic means. This addition casts the net of the law too wide, as even WhatsApp messages have been recently seen to be an adequate means of communication for legal processes, such as summons. This provision should clearly specify the procedures that can be used by lawfully 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 specifically state that requests for restrictions of content must be clear, be unambiguous, and follow due process.

e) *Tracing obligation*: The Draft Rules also impose an obligation on the intermediaries to enable tracing of originators of information, as required by government agencies who are legally authorised. This requirement may not be practically possible to implement, since 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.

Apart from being practically difficult to implement, such obligation may also require significant investment to bring about major technological changes in relation to traceability of content.

We would also like to highlight the right to privacy articulated in the case of *KS Puttaswamy v. Union of India*, in which the Supreme Court emphasised the criticality of judicial scrutiny in relation to data requests. In accordance with this judgment, the tracing provision is required to meet the triple test of legality, necessity and proportionality – of which it fails to satisfy the test of necessity and proportionality.

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. Further, the criteria by which an intermediary can gauge their compliance with rule is also absent, which will add to the uncertainty of operating in India as an online service provider. Finally, 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. Thus, this provision may be considered to be violative of the fundamental right of privacy.

f) *Applicability and Conflict with Foreign Laws:* Rule 5 casts an obligation of traceability requirement which means that in encrypted services, an intermediary may be required to break the same and provide details. Such obligation cannot be cast on the telecom operators who are merely providing the communication link. Further, 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*"

g) In addition to this the manner in which this obligation is cast upon the intermediaries appears as if they have been asked to step into the shoes of an investigation agency, without them being entitled to the immunities that are otherwise enjoyed by state actors. Not aiding an investigation is one thing and actively performing an investigation is quite another.

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. An appropriate proviso in this regard could be added to the provision.

4. Rule 3(7)

Existing Provision	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.

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.

Our member telecom operators have no comments to offer on this proposed amendment. The concerns of our other members are highlighted below:

a) *Arbitrary and onerous obligations*: An incorporation requirement is likely to hinder several intermediaries from being able to offer their services if it is not feasible for them to incorporate in India. This requirement will also act as a barrier to entry into the Indian market and cause an anti-competitive impact on the digital economy, which is not in line with other initiatives of the Government to induct more foreign investment by projecting India as a premier investment destination In the longer run, it may also deny Indian users from accessing the services that are available to the rest of the world, and fragment Internet access available within India.

b) *Excessive delegation of powers*: The present iteration of this sub-rule provides no guidance on the factors based on which intermediaries can be notified by the Central Government. With this lack of criteria, any intermediary can be required to fulfil the requirements under this rule. This is a case of excessive delegation that could lead to non-uniform application of this already onerous requirement. This is also likely to lead to an environment of uncertainty amongst Intermediaries as the Government is empowered to notify entities that must conform to this requirement.

c) *Substantial Economic Impact:* Pursuant to the current scope under the IT Act, there are multiple intermediaries who provide IT services in India and comply with the requirements of the IT Act but are not registered or established in India. 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.

d) *Disproportionate Impact on Startups/Micro, Small and Medium Enterprises (MSMEs):* The eligibility criteria of fifty lakh users is quite 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 threshold currently seems to be an arbitrarily fixed number and should ideally be backed by statistical analysis of usage patterns.

e) *Metric Determination and Enforceability:* There is a need for clarity on how this provision will be implemented. Some of these aspects include: 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.

5. Rule 3(8)

Existing Provision	**Proposed Amendment**
(4) 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	(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 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

contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,	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.

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 of India. Our concerns with this are highlighted below:

a) *Lack of safeguards*: This rule contains a process for the removal or disabling of content. However, unlike the procedure under Section 69A of the IT Act and the IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("Blocking Rules"), the proposed Rule 3(8) does not incorporate any safeguards while creating this new process. Presently Rule 3(8) of the Draft Rules does not specify who can pass the orders, does not require reasons for such orders, and provides an unreasonable window of 24 hours to implement such orders.

b) *Infeasibility:* The prescribed timeline of 24 hours is a particularly stringent requirement, with no concrete justification or rationale. Further, there can be significant implementation challenges (e.g., for a company with only a few employees working daytime shifts) without commensurate benefits.

c) *Lack of Proportionality and Contradiction with Shreya Singal v/s Union of India:* The Shreya Singal ruling is based on an understanding of reasonableness and proportionality of approach and the 24 hour time period goes beyond the letter and spirit of the decision. There have been innumerable instances, where intermediaries have had reason to review the court order or removal requests and to seek clarification on the scope of the same, which have been well received by courts and other authorised authorities and had led to appropriate modification of the orders in certain cases. This process will definitely require a time period that is more than 24 hours, otherwise, the understanding is that content will be removed without any exercise of discretion/ review, which may pose a threat to legitimate speech or for that reason any protected speech as well. We strongly urge that the rules are framed in a manner that the healthy trend of intermediaries and courts/ regulators/ government authorities

working in tandem to maintain a balance between user interests with the need to observe legal obligation is not only preserved but also strengthened.

d) *Period of storage of data*: Rule 3(8) of the Draft Rules also extends the period of time that the information and associated records must be stored for (from at least ninety (90) days, as required at present, to at least one hundred eighty (180) days). Moreover, it authorises Courts or government agencies to extend it further. When requiring service providers to preserve content for an undefined period lawmakers risk imposing new data retention requirements on service providers. This would increase legal uncertainty and confront companies with new financial, logistical and technical challenges. It should be clarified that the storage is required for a maximum of 180 days and a longer period will be only if required by Court Order or lawfully authorized Government agencies.

e) Thus, sub-rule 3(8) extends many powers to government agencies without prescribing any procedural safeguards, which is highly detrimental to freedom of speech and expression, and a matter of critical concern for all governments seeking to regulate speech in the digital arena. In this context, it is worthwhile to note that UN Special Rapporteur Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/38/35 2018), in which it has been noted that:

> "*66. .... 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.*
>
> *68. States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.*"

6. Rule 3(9)

Existing Provision	**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

Rule 3(9) of the Draft Rules mandates that intermediaries deploy 'technology based automated tools' for 'proactively identifying and removing or disabling public access to unlawful information or content'. By placing the burden on intermediaries to identify and remove unlawful information and content, the rule seeks to change the nature of intermediaries and transform them into censorship bodies in lieu of the Government. By

doing so, it also goes against the *Shreya Singhal* judgment, in which 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 government agency. The Supreme Court observed that:

> *"122. 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."*

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 entities that are neither the Court nor government agencies, which is contrary to what is envisaged by the IT Act, *Shreya Singhal*, and the Manila Principles. In addition to the above, it alters the inherent characteristic of an intermediary that entitles them to the safe harbour envisaged under the IT Act, i.e. that Intermediaries cannot *inter alia* "*select or modify the information contained in the transmission*." In a way the amendment is suggesting that intermediaries ought to deploy filters which is a unreasonable obligation on them. In this regard the Delhi High Court in the case of Kent RO v. Amit Kotak (2017) has noted the following in paragraph 42 of the judgement.:

"to require an intermediary to do such screening would be an unreasonable interference with the rights of the intermediary to carry on its business."

Violation of International Law: This proposed amendment 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.

Private Parties Determining Unlawful Content: Rule 9 casts an obligation of proactive monitoring on an intermediary to disable "unlawful information/ content", which is not tenable. Firstly, an intermediary is a platform provider and not in a position to identify or determine whether a content is unlawful or illegal, which is the prima facie role of the Courts and not of an intermediary. Additionally, there is no definition of "unlawful information/ content". Also the proposed changes shifts the onus and duty of the State to private party and is against the Shreya Singhal case.

Further telecom operators who are also classified as intermediaries, are as per the license granted to them, required/permitted to block Internet sites/Uniform Resource Locators (URLs)/Uniform Resource Identifiers (URIs) and / or individual subscribers, as identified and directed by the Licensor from time to time.

Implementation challenges: 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 will be an extremely high burden and may even result in killing innovation and investment in the sector, especially if it is linked to their ability to avail of the statutory immunity to which they are entitled.

Violation of Right to Privacy: Proactively identifying content may also entail monitoring of content, which would lead to invasion of right to privacy. For example, cloud service providers, who fall within the scope of Section 2(w) of the IT Act, 2000, would have to deploy technology which would impinge on privacy of the enterprise customers, and will have an adverse impact on cloud service providers catering to both Indian and international customers. As a result this will decrease trust and confidence in business opportunities in India. In addition to that, the proposed rules, if implemented, may be in violation of the other laws of the land.

In conclusion, we would like to submit that the interests of the Indian Internet users would not be met by imposing onerous and impractical obligations on intermediaries who provide a variety of services, in the manner envisaged in the Draft Rules. We hope that our submissions above will merit your kind consideration and support.

In addition, we suggest strengthening international avenues of law enforcement access, such as the MLAT mechanism. The Government may also consider participating in the Budapest Convention on Cybercrime. With becoming a member, India will be part of an international network that will enable it to use information exchanges as well as the assistance of law enforcement agencies abroad in the investigation of cybercrimes. India's integration into the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) regime will also facilitate international cooperation in the region.

(7) Intermediary liability with respect to consumer grievances for products/ services sold over the intermediary's platform

Under the IT Act, 2000, 'intermediaries' include 'online marketplaces', and are afforded certain protections if they fulfil the requirements of being an intermediary. Therefore, only an entity providing the goods or services is responsible to a consumer for services rendered by it. This principle is a universally accepted one since an intermediary performs services as a middle layer and is not directly liable for the actual services or goods/products offered on its platform, unless it accepts certain additional responsibilities

such as delivery, order fulfillment or customer care services. While it cannot be denied that strong enforcement of consumer laws is the need of the hour, it would not be possible for intermediaries to function under a regime that imposes additional responsibilities on them similar to those generally fulfilled by an end-service provider or the original manufacturer/retailer of goods/products/services, especially given the emphasis on independence of the manufacturer/retailer of goods/products/services and statutorily prescribed inability of the intermediary to influence them. In line with the current position, we recommend that no further changes be made under the Intermediary Guidelines or any other laws to ensure that intermediaries are not held responsible for third party goods and services.

In conclusion, we would like to submit that the interests of the Indian Internet users would not be met by enhancing the obligations of the intermediaries who provide a variety of services, in the manner envisaged in the Draft Rules. We believe that the interests of the law enforcement agencies with respect to data requests and blocking requests would be better met by existing channels under the IT Act and Indian Penal Code, and by strengthening international avenues of law enforcement access, such as the MLAT mechanism. The Government may also consider participating in the Budapest Convention on Cybercrime. With becoming a member, India will be part of an international network that will enable it to use information exchanges as well as the assistance of law enforcement agencies abroad in the investigation of cybercrimes. India's integration into the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) regime will also facilitate international cooperation in the region.

MIT/79/163

U.S. INDIA STRATEGIC PARTNERSHIP FORUM

SUBMISSION ON THE DRAFT AMENDMENT TO THE INTERMEDIARY GUIDELINES, INDIA

Introduction

The U.S.-India Strategic Partnership Forum ("**USISPF**") is committed to fostering strategic partnership between the U.S. and India. We seek to enable business and government to come together to engage in critical policy issues to achieve our shared goals of driving economic growth, job creation, innovation, inclusion, and entrepreneurship. Our work also includes engaging on legal and policy issues that impact digital trade, which is crucial to the development of both countries.

In this context, we would like to offer our comments on the Draft Information Technology (Intermediaries Guidelines) Amendment Rules, 2018 ("**Draft Amendment**") under the Information Technology Act, 2000 ("**IT Act**") issued by the Ministry of Information and Technology ("**MEITY**"), Government of India. We believe that several of the legal provisions in the Draft Amendment will result in barriers to full participation in the digital economy as they may result in inhibiting the free flow of data across borders. The Draft Amendment would deprive Indian users from the benefits of global connectivity, and place undue restrictions on technological leaders seeking to provide services in the country.

The key issues we would like to draw your attention, in light of their potential detrimental impact on global trade and business, are as follows:

(i) The Proposed Amendments are ultra vires the scope of Section 79 of the Act
(ii) Lack of Procedural Safeguards
(iii) Proactive Monitoring of Content and Tracing Requirements
(iv) Mandatory Incorporation
(v) Repeated Alerting Requirements
(vi) Specific Concerns w.r.t Due Diligence to be observed by Intermediary

The Proposed Amendments are *ultra vires* to the scope of Section 79 of the Act

The proposed amendments are *ultra vires* Section 79 of the IT Act. The Intermediary Guidelines are framed under section 87(2)(zg) read with section 79(2) of the Act. These provisions empower the government to make guidelines relating to an intermediary's obligation to observe due diligence in discharging its obligations under the Act in order to retain its safe harbour. It is within these contours that the Intermediary Guidelines have been formulated and it is important that the amendments do not result in extending the scope of the guidelines beyond this statutory obligation.

Section 79 of the IT Act is an exemption provision and this has been noted by the Supreme Court in *Shreya Singhal v. Union of India*[1]. Therefore, the rules under Section 79 cannot serve the role of creating additionally onerous obligations on intermediaries that go beyond the due diligence to be observed to preserve their safe harbour. Such an extension of scope might be challenged as *ultra vires* and struck down.

The Draft Amendment Lacks Procedural Safeguards

Technology-based businesses have made significant investments in building systems to secure user data from unauthorised access except where this access is as per procedure established by law. Where the law itself is vague or unclear, not only does it undermine these security systems and processes, it also puts user data at risk. This would also be detrimental to the government's commitment to improving Ease of Doing Business in India.

To provide examples:

(i) Proposed Rule 3(5)[2] provides that intermediaries, when required by lawful order, must provide, within 72 hours, "*information and assistance*" to *any* government agency. The proposed language leaves undefined relevant government agencies compared to the 2011 rules, which gave standing to only agencies "who are lawfully authorized." (in Proposed Rule 3 (7)), thus significantly broadening the rules. There is no clarity on what constitutes assistance, whether there are purpose limitations to the orders that may be considered lawful, and a clear legal process through which it must be served upon the intermediaries in order to be complied with.

In addition, Section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (the "Blocking Rules") already govern the issuance of government directions for removal of content. Therefore, Section 79 does not authorise the government to issue similar directions, as this could lead to the creation of conflicting processes dealing with very similar issues. The Blocking Rules contain a set of procedural safeguards, which this process should not seek to bypass. Significantly, in comparison to Section 69A, the procedural safeguards in the proposed amendments are drastically lacking.

[1] AIR 2015 SC 1523

[2] Proposed 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 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) Proposed Rule 3(5) also requires "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." There is no clarity on the circumstances under which such intrusive and potentially privacy endangering requests can be made, and who can make such requests. There is an obvious potential for misuse when any government agency could request tracing of any user for any purpose. For instance, a junior officer in a government agency could send a request to trace all originators of content that is in disagreement with their political views, and the intermediary would be obligated to comply. It is clear that this could turn into a dangerous tool of surveillance if not reined in with appropriate procedural safeguards and regulatory justification. We further note that with the expansive definition of "intermediary" made in 2008 and technical advances made in the past ten years, tracing the origins and route of the data in question has now become an exponentially more difficult procedure. The degree of difficulty also has bearing on the revised timelines found in the Proposed Rule 3 (8). In addition to this there is lack of clarity as to what constitutes tracing. It also put an onerous and technically infeasible obligation on intermediaries. It is submitted that there can be multiple circumstances where it is not possible to trace the originators due to technical considerations such as use of VPNs, free and open-source software enabling anonymous communication, end to end encryption, etc.

(iii) The proposed timeline of 72 hours also appears arbitrary and there are no clear reasons for selection of 72 hours as a response time. It does not consider time that may be required to seek clarifications from the issuing 'government agency'. Companies have had past experiences where assistance had to be provided to government agencies who do not consider genuine commercial structures or business challenges. The timeline also ignores the time any intermediary may require to authenticate the request. There have been instances where entities were issuing requests for removal of content in the form of fake government requests. This is especially pertinent as there have been past instances of fake communications being issued by persons claiming to be law enforcement officers, etc. Additionally, often government servants will issue communication not through an official government email ID, but through their personal email ID, which leads to time spent on verification. Thus, it is necessary that intermediaries are allowed adequate response time to appropriately address issues of inauthentic requests under the proposed amendment, failing which there is significant risk to freedom of speech and ensuring privacy of user data.

(iv) Often human intervention is required to comply with such requests, which may not be possible to comply with within 72 hours. There is no scope / time for delay on account of external factors beyond the control of intermediaries such as technical glitches, public holidays, etc.

What is equally concerning is that the above provisions are accompanied by extremely strict and short time limits for *direct compliance* while there is not even a reference to procedures and timelines for response, review and challenge. This provides the intermediary with no opportunity to address unlawful requests. In this context, it is important to note the recent Supreme Court judgement on the Aadhaar (Targeted Delivery of Financial Benefits and Other Subsidies, Benefits, and Services) Act, 2016 ("Aadhaar Act, 2016"), which struck down Section 33(2) of the Aadhaar Act as it allowed access to citizen data on national security grounds, without adequate safeguards. The Supreme Court pointed out that unfettered access to citizen data under Section 33(2) would not be permitted even if data was sought for national security purposes. In striking this provision down in its entirety, the Supreme Court delineated a clear and a high standard of needing due process safeguards such as prior judicial authorisation, and seniority of officials who can issue data access requests, in addition to purpose limitations such as national security. Some of these safeguards already exist in frameworks such as the Telegraph Act, and there is no reason for the Draft Amendment to seek to establish a lower, more challengeable threshold. The amended provisions of Proposed Rule 3 highlighted above can all be challenged and struck down given the strong precedent that now exists for striking down legal provisions that permit access to data without due process.

It is important that India does not undertake legal changes that are open to easy constitutional challenges. Such changes to law only fail to serve the legitimate statutory purpose, but also create an unstable legal regime for businesses to operate in. We would therefore strongly urge the MEITY not to undertake these proposed amendments.

The Draft Amendment Mandates Proactive Monitoring of Content

Proposed Rule 3(9) of the Draft Amendment states that intermediaries "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."

Proactive monitoring can be feasible for certain intermediaries, such as those who actively curate content, and in respect of particular categories of unlawful content such as direct copyright infringement. However, where the range of content covered is very broad, and much of it is not susceptible to easy identification without the assistance of regulators or courts, there are several problematic aspects of this requirement, as highlighted below:

Proactive monitoring on such a broad scale, particularly as it relates to intermediaries that are neutral information channels has flaws: Many intermediaries covered by the IT Act are merely neutral channels for conveying information. In many cases, an intermediary cannot be held liable for any third party information made available or hosted by it, as long as certain

'safe harbour' conditions are fulfilled – which includes removing or disabling content when having notice of the same through appropriate legal channels. It is technically and legally infeasible to require intermediaries like telephone service providers, network service providers, web-hosting services, online payment sites, just to name a few, to surveil disparate and unrelated points in the digital ecosystem.

Given the often impermanent nature of content and the rapidly increasing volume of data, technological solutions may also not be feasible for certain types of intermediaries. Furthermore, in many cases, intermediaries are not in a position to be the judge and arbiter of what content is lawful as per the relevant country's laws. While several key intermediary platforms have formulated internal policy in this regard, this is a matter of self-regulation. With many intermediaries providing services across multiple jurisdictions, the determinations of the legality of content in each segment of the ecosystem, several of which could reside in different countries, can be exceedingly complex.

This is also particularly difficult for cloud service providers ("CSPs") given how it requires them to enforce content monitoring and control requirements and take down certain kinds of unlawful content resulting in the inadvertent removal or blocking of legal content as well.[3] Unlike social media platforms, CSPs do not access their customers' data that is stored on their infrastructure[4], and have little to no insight into the nature of data that is stored or processed using their services.[5] They cannot distinguish between different kinds of data and may be forced to take down entire websites.[6]

Monitoring requirements conflict with Indian law: The position of law in India as spelled out through various court decisions, is perfectly clear on the point that neutral intermediaries should not be made to assess the legality of content. In ***Shreya Singhal v. Union of India*** it was held under various provisions of the IT Act and rules thereunder, that the intermediary in that case could not be required to proactively monitor its platform for unlawful content, and its

[3] 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)
[4] 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).
[5] Amazon, Comments on the draft Personal Data Protection Bill, Page 13.
[6] 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).

responsibility was limited to taking down content when notified by court orders or authorized government agencies.

Monitoring In Many Cases Is Not Technically Feasible: The Draft Amendment also seems to assume that it is an easily achievable task to develop algorithms and solutions that would proactively filter out all of the identified types of content that is unlawful in India. In reality, this is an extremely difficult balance to achieve, as this entails global service providers having to develop tools to perform the following functions: (a) accurately identifying content that is unlawful as per the laws of the specific country they are operating in (even when the laws are as vague as content being "threatening" or "promoting" something); (b) potentially identify content in the many languages in India; (c) maintaining the balance of respecting the freedom of speech and expression of users; (d) ensuring the ability to provide these tools at scale.

This submission is supported by the pornography instituted by the Government of India. Despite efforts at full compliance, the wrongdoers have repeatedly helped users circumvent these bans by setting up mirrors, the usage of VPNs, web browsers and extensions that use proxies, and so on.

This, and other examples, demonstrate the challenges to the technical feasibility of active monitoring. If the inability to develop such algorithms could potentially lead to businesses losing legal immunity, this is a significant disincentive for several service providers from providing services in the first place.

Free speech related concerns: As pointed out above, the Draft Amendment appears to overestimate the ease with which unlawful content can be identified through deploying technology, and taken down without inadvertently removing content that is a legitimate exercise of the constitutionally protected freedom of speech and expression of users. This effectively incentivizes the deployment of broad censoring tools on the part of private entities, in order to enable them to stay on the safe side of the law. Given the practical impossibility of fine tuning such automated tools to the point where they can assess content correctly in various formats, numerous languages and under various laws, it is likely that overbroad tools may be deployed for this purpose which could result in content being taken down and user accounts being deactivated arbitrarily, having a chilling impact on free speech.

Broad list of unlawful content: As noted above, the proactive monitoring obligation in the Draft Amendment must be seen in light of the broad list of unlawful content that the intermediary should warn the users not to upload, as part of Proposed Rule 3(2). The Draft Amendment expands an already broad list by adding two broad and undefined content types: (i) content that threatens public health; and (ii) content that threatens critical information infrastructure. Given the extremely unclear implication of a term as vague as "threatens", it is extremely difficult to determine what kind of content should be filtered by the intermediary.

In this regard, it is useful to note that vague restrictions on free speech, phrased in similar language, have already been struck down by the Supreme Court of India in litigation against Section 66A of the IT Act (*Shreya Singhal vs. Union of India).* Similar issues will arise in regard to these additional requirements in Proposed Rule 3(2).

Monitoring goes against international best practices: The best practices for a regulatory regime governing intermediary liability are enshrined in the Manila Principles on Intermediary Liability, which globally inform government regulation. [7]

The first principle is that intermediaries should be shielded from liability for third-party content, and never be made to proactively monitor content. This is elaborated upon as follows:

(i) Any rules governing intermediary liability must be provided by laws, which must be precise, clear, and accessible.
(ii) Intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in modifying that content.
(iii) Intermediaries must not be held liable for failing to restrict lawful content.
(iv) Intermediaries must never be made strictly liable for hosting unlawful third-party content, nor should they ever be required to monitor content proactively as part of an intermediary liability regime.

Clearly, the Draft Amendment falls short of this principle and is out of step with global best practices, by making proactive monitoring a part of the intermediary's obligations.

This proposed amendment also goes against India's commitments under various international covenants, which include:

(i) 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)
(ii) Joint Declaration on Freedom of Expression and the Internet (2011) issued inter alia by the UN Special Rapporteur on Freedom of Opinion and Expression

Recommendation: In light of the above discussion, we recommend limiting the scope of content monitoring to only those specific intermediaries who function as curated content providers, pursuant to an adequate definition of such a platform being provided. The scope of monitoring should be limited only to copyright-infringing content that is easily identifiable through the deployment of content recognition technology that is presently available.

[7] https://www.manilaprinciples.org/organization-signatories?page=1

Draft Amendment Mandates Tracing of Originator

The Draft Amendment also imposes requirements on intermediaries to assist law enforcement in tracing the originator of content. While several key intermediaries are already in conversation with the government to find the best way to address legitimate concerns of fake news, etc. this requirement appears to subvert those efforts by imposing a uniform obligation on all intermediaries across the board.

This gives rise to several concerns:

Right to Privacy: The right to privacy has been recently upheld by the Supreme Court of India as a facet of the right to life and liberty.[8] While this obligation is not specifically enforceable against a private party, it is clear that in the present political climate, users consider this to be a key civil right that they value and wish to have safeguarded. One of the key commitments that several intermediaries bring to users is that their privacy is valued and safeguarded by the products and processes offered by the intermediary. The imposition of a vaguely worded tracing obligation could potentially require a change in fundamental business practices and underlying technology of such intermediaries, and give rise to legitimate concerns among users that their privacy is violated through the tracing of all their communications.

Existence of processes under criminal law: Furthermore, to the extent that intermediaries are able to provide information, this can already be requested under existing mechanisms in Indian criminal law, and most intermediary platforms are willing to comply with legitimate law enforcement requests in this regard. These intermediaries work with governments across the world to identify ways to balance these concerns with other concerns of freedom of business of companies, and right to privacy of users. Existing processes also have due process requirements built in which the Draft Amendment seeks to do away with, and there is no apparent legal justification for this.

In the interest of creating a predictable legal regime that enables co-operation between law enforcement and intermediaries, we recommend not undertaking these changes. However, if MEITY still wishes to introduce changes, we request that these be kept in the nature of best effort clauses, and not attract strict liability. We also recommend focusing on strengthening existing criminal law procedures with due safeguards instead of creating parallel processes.

The Draft Amendment Introduces Mandatory Incorporation Requirements

Sub-rule 3(7) of the Draft Amendment states that the intermediary who has more than fifty lakh users in India, or is in the list of intermediaries specifically notified by the government,

[8] *K S Puttaswamy vs. Union of India,* Writ Petition (Civil) No 494 Of 2012

shall incorporate as a company in India, have a permanent registered office in India with physical address, and appoint contact persons in India for "*round the clock coordination with law enforcement agencies and officers to ensure compliance with their orders and requisitions*."

Incorporation is a trading barrier: At the outset, a requirement of incorporation cannot be included in a law that is designed to provide conditions for exemption from intermediary liability. This is effectively a pre-condition to provide certain services in India, and functions as a trade barrier across the various service sectors in which intermediaries provide services. This may also have implications on India's WTO commitments for trade in services, based on the specific service sectors in which commitments have been undertaken. A legal framework for providing safe harbour cannot be a channel through which trade barriers are addressed or sought to be introduced. Any discussion of trade barriers should be redirected through the appropriate channels, and informed by a holistic understanding of the industry interests of India's trading partners.

While incorporation can be made an eligibility criteria for receiving certain benefits as permitted by India's trading commitments, it is unprecedented to make it a precondition to operating as in intermediary. This is particularly problematic as a broad based obligation which operates across different sectors with varying FDI commitments, as it seeks to undermine sectoral regulations / exemptions and sectoral commitments in one broad sweep.

Increased regulatory and taxation exposure may be commercially unviable: Incorporation in every country of operation involves complying with a host of regulatory issues and increased incidence of tax – including immediate exposure to corporate taxation regimes which would serve as an enormous disincentive against doing business in India. Undertaking such regulatory and taxation exposure may not be commercially viable for most global players, and it is likely that Indian users would be deprived of several services that are accessible to the rest of the world, and experience the internet very differently.

Further, foreign companies doing business in India (which have a place of business in India, and conduct business activities within India) are already regulated under the Companies Act, FDI Policy and many other laws. As such there is no need for additional regulatory exposure through mandatory incorporation.

Limiting Consumer Access to Technology: 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 scalability and 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 by increasing costs to an extent that offering services / technologies to consumers in India becomes financially unviable.

Metric Determination and Enforceability: 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 that can fall afoul of these requirements.

Reciprocal measures by other states could balkanise the internet: The rapid development of key intermediary platforms on the internet over the last decade has allowed cross border flow of information at a scale that is unprecedented in the trading history of most countries. Free flow of data across borders has led to important innovations and allowed global companies to contribute to India's digital economy and allowed Indian companies to access global markets by providing several key services on a cross border basis. At this point, the regulatory focus should be designed to make it easier for companies to provide such services across borders, without compromising on user experience. However, a mandatory incorporation requirement could lead to a fragmentation of the internet, as only companies incorporated in India can provide services to the Indian population at a large scale. It should be borne in mind that if other countries were to enact similar measures, it would be very difficult for Indian companies to operate in global markets, thereby subverting some of the key advantages of a free and open internet for Indian service providers as well.

In light of the above factors, we *strongly* recommend that the incorporation requirement be done away with.

The Draft Amendment Introduces Repeated Alerting Requirements

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

The requirement to inform users of this one specific aspect of the usage conditions and not any other aspect is highly arbitrary. This may require commercial and technical changes to be undertaken by intermediaries, which is onerous without a corresponding benefit – as users are already able to see these requirements in the terms and conditions that are easily accessible. If intermediaries repeatedly provide this information to their users, this might in fact result in warning fatigue, defeating the purpose of the requirement. Therefore, we recommend that this additional obligation of monthly notice should not be introduced.

Specific Concerns w.r.t due diligence to be observed by Intermediary

Rule 3 (2) (j)

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".

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 should not be regulated under the provisions of the said Act." In 2018, the Central Government issued an Advisory which also acknowledged that ENDS are not, as of now, regulated under the DC Act.

To that extent, Rule 3(2)(j) is not sound in law and must be suitably amended to remove references to ENDS entirely.

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 need 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.

Conclusion

Given India's commitment to improving ease of doing business, and fulfilling the promise of Digital India, it is crucial to recognise the role played by online intermediaries to further these causes. Any regulatory regime that is unduly prescriptive, unpredictable and onerous could

prevent the Indian economy from reaping the many benefits promised by an open Internet that prioritises cross border flow of data. USISPF therefore urges the government to reconsider these proposed amendments.

MIT/79/164

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 concernd 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.

MIT/79/166

The Information Technology
[Intermediaries Guidelines (Amendment) Rules]
2018

Given below are Microsoft comments on the proposed amendments to the Intermediary Guidelines. Our comments (whereever we felt necessary) are given on the main text and highlighted in Green.

Covering Note of MEITY

Comments / suggestions invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

The Information Technology Act (IT Act), 2000 was enacted with a view to give a fillip to electronic transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures. The Act came into force on 17th October, 2000.

Section 79 of the IT Act elaborates on the exemption from liabilities of intermediaries in certain cases. Section 79(2)(c) mentions that intermediaries must observe due diligence while discharging their duties, and also observe such other guidelines as prescribed by the Central Government. Accordingly, the Information Technology (Intermediaries Guidelines) Rules, 2011 were notified in April 2011.

Comments:

(a) MEITYs intent to attempt these modifications are well understood and appreciated. Technology has vastly evolved since the time the IT Act was first notified. There was no such thing as the social media at that time, nor were there smart phones, there was no ubiquitous Wifi and no easy access to the internet content. It is but natural that in some cases Laws haven't been able to keep pace with technology. Hence the need to reexamine and harmonize Laws with current realities. However Laws have to be kept generic so that they are technology neutral. Else there will

be a need to have a major recasting of Laws every few years. New technologies like IOT platforms, AI platforms, blockchain platforms etc will make it impossible for the Law to keep pace. Hence what MEITY should consider doing is, to keep the bare Law generic and broad based, so that it can cope with the upheavals of time, technology and business models. And consider bringing out specific guidelines for different types of intermediaries keeping in mind their operating model, technology used and reach.

(a) Intermediaries by their very nature have a limited control over the content passing through them. Keeping these inherent limitations in mind, certain safeguards have been provided under Law. Diluting these safeguards will make it difficult for intermediaries to operate and will make the amendments open to legal challenge. This will also drive away innovation and new products from India.

(b) Intermediaries come in various hues: Telcos, ISPs, Content Hosting Platforms, Social Media, WiFi hotspots, Cable providers etc. MEITY is attempting the solve for all types of intermediaries disregarding the fact that each class has a different role, uses different technology and has different level of access to the content, different type of content and different level of impact on end consumers.

(c) In trying to solve for everything, every type of intermediary and every type of technology, MEITY is attempting to amend the regulation. However the filter is becoming so fine, that everyone and everything is getting stuck. This will make compliance impossible from the process, Legal and technology point of view for **ALL** the intermediaries.

(d) Many social media platforms and content hosting platforms are transnational. Regulations have to keep these realities in mind. These platforms have a difficult task of operating in different geographies while balancing local regulatory concerns.

A calling attention motion on "Misuse of Socal Media platforms and spreading of fake News" was admitted in the Parliament (Rajya Sabha) in 2018 (Monsoon session). Hon'ble Minister for Electronics and IT, responding to the calling attention motion on 26/07/2018, made a detailed statement where he *inter alia* conveyed to the House the resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law.

Comments: Please see Parliament observation above. The problem that MEITY is addressing is Social Media platforms and fake news. The solution should be focused on addressing these as had been done in the Prajwala case. Existing regulations provide for enough powers for Government to work with social media platforms. There may be a case for MEITY to bring out additional guidelines (not change in Law) for certain types of intermediaries like social media platforms in consultation with them. There may also be a case to strengthen other laws and enact Laws which makes the punishment of fake news and misuse of social media stringent. The focus should be on the perpetrators of the crime rather than the intermediaries.

Subsequently, MeitY has prepared the draft Information Technology (Intermediary Guidelines) Rules 2018 to replace the rules notified in 2011.

Overall Comments: There are four core issues that the proposed amendments seek to address:

(i) Notice to users: MEITY should guard against notice fatigue and also consider that this be difficult to implement for most intermediaries. There can be short/sharp notices of not more than once in 90 days frequency

(ii) Establishment in India: For more than 50 lakh users: Such entities will automatically open their establishments in India

for furtherance of business.This should be dictated by business imperatives, rather than a Law. There could be scenarios like IOT, weather apps etc, where number of users could be more than 50 lakhs, but there is no requirement to open an office here. Such apps and services will have no option but to leave India.

(iii) Response to Law Enforcement requests: Home Ministry (MHA) has already laid down 72 hours response time. Harmonize with this.

(iv) Tracing of originator/ content: There are technical and legal limitations

(v) Deploying automated tools to monitor content: Technical infeasible, Legally untenable. Please follow Prajwala guidelines.

Government needs to create a clearing house to adjudicate requests from various Law Enforcement agencies.Otherwise all the good intent will not come to fruition.

==========

1. 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.

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; No Comments
(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;

(Communication link is not referred to anywhere else in the document. So we could examine if this is superfluous)

(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;

(It maybe necessary to define this more sharply. Section 70 of the Act defines this in terms of protected systems. For example a database of suspected criminals or a Defense

computer would qualify to be a protected system, but will not qualify as Critical Information Infrastructure).

(f) "Cyber security incident" means any real or suspected adverse event in relation to cyber security or privacy 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 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;

(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.

3. Due diligence to be observed by intermediary — 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 ~~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 —

This is difficult to implement. This cannot be done by many types of intermediaries like Wifi service provider, where usage by the user could be only for a few minutes. No one will read such a long notice. Also in case of TSPs and ISPs, the user agreement would have so much fine print that no one will pay attention.

(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;

Gambling is allowed in some states (Casinos etc). There are many e-Gambling and gaming sites on the internet. Difficult to implement.

(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;~~

[It is better to keep this open ended instead of making it prescriptive and giving examples. Requirements may change from time to time] .

(k) (k) threatens critical information infrastructure.

(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):

(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;

(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;

~~(4) 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 ninety days for investigation purposes,~~[1]

(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.

(Once in a month will lead to notice fatigue. If notice is too long or too frequent, it will lead to users ignoring it. This will defeat the intent of the Government. Short notices in the frequency of not more that once every three calendar months is recommended)

(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 invoking the relevant provision of Law. 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, to the extent technically feasible.

Comments: MEITY and MHA must have a clearing house of such requests. The field formations of Law Enforcement do not have an appreciation of the finer aspects of Law or of Technology. Their requests could be technically infeasible to comply with or could be in gross violation of the Law or Fundamental Rights. Lower levels of the Law Enforcement put pressure on companies without understanding the nuances. This could lead to escalations like the Shreya Singhal case.

(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.

(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:

[1] This sub-rule has been modified as per Supreme Court Judgment in the matter of Shreya Singhal Vs UOI dated 24.03.2015.

(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.

Most intermediaries have international operations. They cannot designate a senior functionary only for acting as a nodal officer. It should suffice ass long as there is a person appointed by such intermediaries for handling this requirement. This is also inline with the requirements laid down by MHA in the Prajwala case.

(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~~ (this has to be 72 hours in sync with the rules framed by MHA after the Prajwala case) 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.

(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 provision needs to be dropped. This is impossible to implement. As mentioned in the introduction, intermediaries are of all kinds. Does this mean that intermediaries like ISP and TSPs shall monitor all content passing through their systems ? Is the State giving them that right? What about this violating individual privacy, right to freedom of expression etc. Besides being technically infeasible due to the high cost of such technology, there are also severe limitations in technology. This will also drive out innovative new apps out of India as the cost of even attempting compliance will be prohibitive. The limitations of existing technology to even attempt this has been brought out by the Joint Working Group of the industry and Government constituted by MEITY to comply with an observation of the Hon'ble Supreme Court in the Prajwala case. Proactively monitoring of content by all intermediaries may make foreign countries stop outsourcing BPO work to India and move to other countries.

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

This is too broad a definition. What constitutes a security incident? A port scan, a ping by a Bot, a virus etc. What should be the frequency of such reporting, where should this be reported? In what format?

(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.

(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;

(13)The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

==========

The problem being sought to be addressed by MEITY is being faced by all countries around the world. Here is a snippet of what other jurisdictions are doing to address this.

- The EU has its (non-binding) Code of Conduct Against Illegal Hate Speech (to which MS is a signatory)
- The EU also has efforts afoot to address illegal terrorist content in terms of formal regulation (expected "soon")
- Australia has its Office of the eSafety Commissioner, which focuses on combatting cyberbullying and "revenge porn," and has recently expanded to so-called "image-based abuse" (which it calls another term for revenge porn; I believe it is broader)
- New Zealand has its Harmful Digital Communications Act, which was supposed to focus on cyberbullying, as well, but the name itself suggests a much broader surface area, and
- Germany has its social media law (this is a link to a news article).
- UK is coming out with an "Online Harms Whitepaper" in the next couple of months that is supposed to be the precursor to more comprehensive legislation, as well as appoint a designated regulator. Both illegal (i.e., child sexual abuse, terrorism) content and harmful/potentially harmful content (i.e., bullying, harassment, etc.) will be covered by the whitepaper.

MIT/79/166

MEDIANAMA

Sir/M'am,

Thank you for holding a public consultation to amendments to the IT Rules, and offering to publish comments and allowing for submission of counter comments. We would have appreciated a similar approach from MEITY to the process of finalising the Personal Data Protection Bill.

MediaNama is a publication that participates in government consultations, with the intent of helping build an open, fair and competitive digital ecosystem in India, with user and citizen interest in mind.

Before we get into substantive comments on these rules, we would like to remind you of the circumstances in which the Section 79 of the IT Act was forumated.

The importance of Safe Harbor for Internet businesses and users

On December 14th, 2004, Avnish Bajaj, now a co-founder at VC firm Matrix Partners, was arrested, and sent into judicial custody without bail until December 24 that year. Bajaj had gone to Delhi to meet the police, and help with an investigation related to the attempt at selling a copy of the infamous DPS MMS clip via Baazee.com. Baazee.com, which Bajaj had founded, and sold to eBay, was the precursor to eBay.in, and allowed users to buy and sell physical and digital products. The seller had put up a listing on Baazee, for the MMS clip, and offered to email users the clip, once the payment was done. Upon being informed about the clip, Baazee had removed it, and was assisting the police with the investigation.

It was Bajaj's arrest that led to the discussion on providing a safe harbor for intermediaries in India, which would allow them to facilitate communication, commerce and services between individual users, whether those users are corporations or independent individuals. The Internet does not differentiate between types of entities that transact online, and this principle is at the heart of the issue of Net Neutrality: ISPs, like any other intermediaries, are neutral, and should not discriminate between users.

When the IT Act was passed in 2008, despite its flaws, it brought in "safe harbor" for "intermediaries". Intermediaries – which include social networks, messaging platforms, e-commerce marketplaces, video sharing sites, blogs (when it comes to comments that you leave on them), payment companies who enable transactions, domain registrars – are merely seen as entities that allow sharing of information, and not as "publishers" in the traditional sense of the word. Just as you shouldn't be held liable for my comments, my video, platforms are protected from liability of how users use them. In the same vein, marketplaces are not

responsible for the actions of sellers and most importantly, ISPs are not responsible for what you access. This limitation of liability, known as “Intermediary Liability protections”, ensure that platforms can enable billions of users to communicate, message, publish, sell, and interact.

Safe harbor is fundamental to the growth of the Internet.

Why safe harbor was strengthened in 2015.

Prior to the Shreya Singhal judgment, for safe harbor, intermediaries, as per Section 79 of the IT Act, had to follow certain “due diligence” requirements. However, this wasn’t without its challenges: among the provisions of Section 79 was the requirement that in order to avoid liability, service providers have to take down certain content once the fact that it is of a certain type is brought to their “actual knowledge”. Intermediaries were acting on frivolous takedown notices, some of which chose to take down content instead of risking liability (read research). Content which conformed to vaguely defined terms, like “grossly harmful”, “obscene”,”racially, ethnically objectionable, disparaging,” or legal content such as “blasphemous” and “pornographic”, paedophilic, libellous, invasive of another’s privacy, hateful, or relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever. Section 79 was eventually written down by the Supreme Court as a part of the Shreya Singhal judgment in 2015, by defining “actual knowledge” as a court order and/or the notification by a government or its agency, and in conformity with reasonable restrictions on free speech, as per Article 19(2) of the Indian constitution.

While this didn’t incorporate a recourse to the entity whose content would be taken down, it was still an improvement. **What the judgment acknowledged was that the medium/enabler of free speech – the platforms – need to be protected in order to enable and protect free speech.**

Issues with amendments to the IT Rules

1. They don’t just affect content and fake news: Given the framing of changes to these rules by the government – in terms of the announcement, and subsequently on the basis of news reports based on limited understanding of issues, the assumption is that they will only impact WhatsApp. This is incorrect: the requirements, whether of proactive monitoring of “unlawful information” using automated tools, or requiring registration in India of platforms with more than 5 million Indian users, will also impact advertising networks, payment gateways, Wikipedia, Github, Pastebin, Stackoverflow, and several others.

Thus, MEITY’s attempt to look at IT Rules from the perspective of only Fake News is myopic and will have disastrous consequences for the internet ecosystem.

Recommendations: <u>Seek other solutions for addressing issues related to misinformation and fake news, including enhancing law enforcement capacity, using counter speech, and other mechanisms being researched. Do not amend the IT Rules or the IT Act without studying what the consequences of such a move will be.</u>

2. Proactive censorship will have a disproportionate impact on free speech: The rules call for "proactively identifying and removing or disabling public access to unlawful information or content".
Impact:

- **More than pre-censorship:** These changes even go beyond what Kapil Sibal had proposed in 2011 of precensorship of social media content, because they cover all sorts of information, including code. ISPs essentially would not be able to function. They might just end up blocking parts of the Internet, just to avoid taking the risk of unlawful content being accessed via India.
- **Disproportionate censorship:** This will force platforms to overcompensate so as not to take on liability, and they will be more likely to take down content, products, code and information, rather than take on liability. We saw that in 2009-2011, and there is evidence to that end from Rishabh Dara's research.
- **Breaking encryption:** This requirement for proactive monitoring will require the breaking of encryption for proactively identifying content, and checking of all the content and information that goes through the pipes.
- **AI is incapable of dealing with it:** Artificial Intelligence and Machine Learning have evolved, but they're still not good enough to accurately identify human context, and judge when something is illegal or not. We're not at Minority Report levels of advancement yet, and we're seeing that with how platforms are using AI to take down content, and messing up. We really cant leave the job of judgment to anyone but qualified judges here.

<u>We recommend that this provision be deleted completely. There should be NO proactive monitoring and censorship.</u>

3. Section 79 is an exemption section, not an enabling provision: the government of India is trying to bring in provisions like traceability of users on platforms, proactive monitoring of content (effectively surveillance), ensuring that assistance is provided to government agencies, informing users of terms and conditions once a month via amendments to this section, which it really doesn't have the remit to do. Section 79 is a section that is meant to ensure that platforms to basic due diligence, and nothing more.

Recommendation: <u>Do not use amendments to the IT Rules for enforcement purposes.</u>

4. Traceability will break end to end encryption: Forcing traceability upon platforms is it significantly impacts privacy: end to end encryption will have to be broken for bringing in traceability, and this ends up making users of end to end encryption more vulnerable. This is a disproportionate requirement specifically with WhatsApp in mind. It is also deeply problematic because the Internet also enables marginalised communities to communicate, interact, publish content, and maybe find love: Before Section 377 was decriminalised, imagine how these rules would have impacted apps like Grindr.

Recommendations: <u>Addressing encryption is essential, and we need surveillance reform and an encryption policy. This is a backdoor means of doing the same thing, and clearly beyond the remit of Section 79. The government should start a separate process for surveillance reform.</u>

5. The 50 lakh users limit is vague and will cover everyone: India has around 350 million Internet users, and over 500 million Internet connections. In this context, 50 Lakh, or 5 million, is 1.43% of India's Internet user base. Think of the number of apps that have 5 million Indian users. Every moderately large advertising network and every single ad exchange probably does. Each of these, under the amendments to the rules, will be required to:
(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 24×7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.

a. How many apps in the world will incorporate a company in India, or have a registered permanent office with a nodal person? What will the government do – block apps that don't set up an office in India? Or will the apps decide not to take on the liability and block out the Indian market itself? This is an underhanded, backdoor means of addressing challenges posed by significant intermediaries.
b. Secondly, what is not clear here is what the amendment means by 50 lakh users – does it mean daily active users, monthly active users, or registered users? There seems to be no objective rationale here for subjecting one intermediary to differential set of recommendations from another.

Secondly, subjecting significant intermediaries to a particular set of regulations essentially creates a regulatory barrier to market entry in favor of large intermediaries who can afford the cost of additional regulations.

Thirdly, regulating intermediaries by different types, such as social media, advertising networks, ecommerce marketplaces etc is problematic because several intermediaries have multiple roles: they allow users to network, but also provide payment services, or ecommerce platforms. Games incorporate messaging, and allow users to message or talk to each other. Google Maps

enables booking of cabs. The utility of the Internet lies in platforms evolving over time, and incorporating different elements of audio, visual, text and interactivity, and combining content and commerce in ways previously unimagined. Any attempt to create classifications will essentially impact the way the Internet functions.

Recommendations: Avoid any attempt to regulate intermediaries based on size or categorisation.

6. Vagueness in definition of "assistance": The draft amendment to the rules sat 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."

The phrase "assistance" here is not specific, and lends itself to the usage of a due diligence clause for the purpose of enforcement. The IT Rules are not the place for such a demand, and even if elsewhere, the phrase "assistance" should be specific and clear, and limited in its approach. Additionally, it should lend itself to mandating sharing of vast amounts of data in a manner that is disproportionate, and a form of mass surveillance.

Recommendations for improvements to IT Rules

1. Incorporate at Takedown and Appeals process: The IT Rules need to learn from DMCA is notice and takedown with appeal. It's not takedown and stay down.
2. Provide transparency to citizens in terms of number of takedowns ordered by the government and courts under Section 79 and the IT Rules
3. Remove vague phrases from the rules, including grossly harmful, blasphemous, obscene, hateful, or racially, ethnically objectionable, disparaging. Blasphemy is not a defined crime under the IPC.

Thanking you,
Nikhil Pahwa,
Founder, MediaNama.com

S.No	Ref. No.	Comments
162	MIT/79/162	I and all the people who were informed (about 90% of the students in my college) about this upcoming amendment, strongly oppose the enactment of such an amendment. As it makes the internet and primarily all information technology extremely insecure. By giving all intermediaries full access and power to monitor its every user and terminate their accounts automatically without proper investigation into the offense and parties involved. As a student and practitioner of law and commerce, I am fully aware of the unjust power given by this amendment to any government agency and intermediary to access anyone's private data without their consent. The internet is a great medium grapevine communication (the casual talks and interactions among peers unofficially) to flow, the government has to strengthen its methods of official communication rather than trying to control the internet. The grapevine system of communication is meant to flow from anywhere to anyone in a very short time. But its never a medium for official communication and needn't be considered as a source of reliable information. Literally 100% of the people (Puducherry) were unaware the coming of this amendment and the commencement of the public opinion period. MEITY and the government should make a lot more efforts in publicizing such upcoming changes before making decisions based on public opinions given by only 1% of the actual population.

S.No	Ref. No.	Comments
165	MIT/79/165	Sirs, In response to the invitation for comments and suggestion from all relevant stakeholders on the Draft of the Intermediary Guidelines 2018, we wish to submit the following: 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 problem of fake news or of accountability of social media platforms will be addressed, much less resolved. Thus, there is an urgent need to have wider consultations with as many stakeholders as possible on both these issues before bringing in any changes in the existing law.