January 31, 2019

Via Electronic Mail: gccyberlaw@meity.gov.in; pkumar@meity.gov.in; dhawal@gov.in

Ministry of Electronics and Information Technology
Government of India
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003

Re: Information Technology (Intermediary Guidelines) Rules 2018

Dear Cyber-Laws and E-Security Group:

The Computer & Communications Industry Association (CCIA) respectfully submits these comments regarding the Ministry of Electronics & Information Technology (MeitY)'s draft Intermediaries Guidelines (Amendment) Rules 2018 ("Draft Guidelines").[1] CCIA appreciates the opportunity to provide its views on the proposed changes to intermediary liability laws in India, and raise concerns about the projected impact to the Internet ecosystem.

CCIA is an international, nonprofit association representing a broad cross section of large, medium, and small companies in the high technology products and services sectors, including Internet products and services, electronic commerce, computer hardware and software, and telecommunications.[2] For over 40 years, CCIA has advocated for promoting innovation and preserving full, fair, and open competition.

India has been identified as a market ripe for growth with a rapidly evolving digital economy.[3] As a quickly emerging player in the global Internet economy, the creation of a regulatory framework in India that further enables innovation is critical.[4] The Government of India has set

[1] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, *available at* http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

[2] A list of CCIA members is available at https://www.ccianet.org/members.

[3] Bhaskar Chakravorti, Ajay Bhalla, & Ravi Shankar Chaturvedi, *60 Countries' Digital Competitiveness, Indexed*, HARVARD BUSINESS REV. (July 12, 2017), https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed; Associated Chambers of Commerce and Industry of India & Ernst & Young, *Propelling India to a Trillion Dollar Digital Economy: Implementation Roadmap to NDCP 2018* (Nov. 2018), https://www.ey.com/Publication/vwLUAssets/ey-propelling-india-to-a-trillion-dollar-digital-economy/$FILE/ey-propelling-india-to-a-trillion-dollar-digital-economy.pdf.

[4] THE BOSTON CONSULTING GROUP, *The $250 Billion Digital Volcano: Dormant No More* (2017), *available at* https://media-publications.bcg.com/BCG-TiE-Digital-Volcano-Apr2017.pdf (mentioning that by 2020, India's Internet Industry is expected to comprise of 7.5% of its GDP).

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

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

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

Comments on Amendments

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(8) The intermediary upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency under section 79(3)(b) of Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorized.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

Respectfully submitted,

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

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