31st January, 2019

To,
The Ministry of Electronics and Information Technology,
Government of India

CC:
Group Coordinator, Cyber Law and eSecurity Group

Subject: ARTICLE 19 comments on Draft of Intermediary Guidelines 2018

Dear Madam/Sir,

ARTICLE 19 welcomes the opportunity to participate in this public consultation on the Draft of Intermediary Guidelines 2018.

As a global freedom of expression organisation, we share MeitY's concerns surrounding disinformation and propaganda on social media, and actively engage with issues of content regulation, disinformation, online anonymity, hate speech, and the role of social media platforms in democracies. We offer our comments below keeping in mind that the Indian State is bound by fundamental rights in Part III of the Constitution, and by her obligations under international human rights law.

In case you have questions about our submission, or if we can provide any further assistance in this process, please feel free to contact ARTICLE 19's Digital Programme Officer, Vidushi Marda, at vidushi@article19.org.

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA

T +44 20 7324 2500 F +44 20 7490 0566 E expression@article19.org W www.article19.org

Rule - wise feedback

1. **Draft Rule 3(5)** of the Guidelines contemplates that intermediaries shall enable tracing of originators of information on platforms as may be required by government agencies who are legally authorised.

By requiring intermediaries to trace originators of information, there is an implicit expectation for users of platforms to be known, and for data on these users to be collected. It is submitted that this draft rule is **technically infeasible** in case of some intermediaries like Signal, Telegram, banking applications and other end-to-end encrypted platforms that do not collect or retain metadata required for the purposes of traceability. Further, even in the case of platforms that do collect metadata, the draft rule implies that encryption will need to be weakened through 'back-doors' in order to understand the payload of user communication. The draft rule further implies a general monitoring obligation, which can lead to **unwarranted censorship**. All of these implicit requirements translate to a **significant dilution of privacy, freedom of expression and security of users online**. The language of the draft rule only exacerbates these concerns - it does not shed light on what constitutes a "legally authorised government agency", nor does it lay out the circumstances, checks, or balances under which the requirement of traceability may arise.

ARTICLE 19 submits that this draft rule is violative of the fundamental right to privacy (including informational privacy) recognised by the nine-judge Constitutional bench in *Justice K.S. Puttaswamy v. Union of India* (2017)[1] and the right to privacy under international law. The bench in *Puttaswamy* laid down the test for "**proportionality and legitimacy**"[2] that any interference with the right to privacy must meet, which the draft rule does not satisfy. We further submit that Draft Rule 3(5) does not meet the requirements under the International Principles on the Applications of Human Rights to Communications Surveillance[3] ("**Necessary and Proportionate Principles**") which was cited by Justice R.F. Nariman in *Puttaswamy*. We also note that this draft rule is in direct tension with the principle of **data minimisation** which has been recognised and implemented by the Srikrishna Committee on data protection.[4]

Anonymity and encryption are fundamental concepts in the protection of freedom of expression and the right to privacy.[5] In May 2015, the UN Special Rapporteur on the promotion

[1] Justice K. S. Puttaswamy (Retd) & Another v. Union of India & Ors (2017), Writ Petition (Civil) 494 of 2012.
[2] Concurring opinion of Justice Sanjay Kishan Kaul, Paragraph 71, Page 37, *ibid.*
[3] International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/principles.
[4] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Page 52 - 27, available from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf. Also see the Personal Data Protection Bill, Sections 5 & 6, available from http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
[5] ARTICLE 19, Right to Online Anonymity, June 2015. Available from https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.

and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) released a report[6] on online anonymity and encryption, which made clear that **attempts by governments to gain backdoor access to people's communications or intentionally weaken encryption standards are a violation of international law**. In light of these observations, we urge reconsideration of this rule.

2. **Draft rule 3(7)** of the Guidelines requires an intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India to be incorporated as a company in India with a permanent registered office, and appoint a nodal person of contact for coordination with law enforcement agencies.

ARTICLE 19 submits that this draft rule imposes obligations on intermediaries in a manner that may **disproportionately and significantly affect small and medium enterprises**. The threshold of fifty lakh users is not significant given the nature of the information flows on internet, and the requirement of setting up physical offices in India, hiring a full time employee for coordination with law enforcement is **thoroughly impractical** for most intermediaries. These onerous compliance costs would mean that information from small and medium enterprises would not be accessible in India. Further, the draft rule does not lay down the grounds on which the government can notify intermediaries, or on what parameters, making the obligation on intermediaries **uncertain and vague**.

This is legally significant for two reasons. First, it violates the **right to receive information under Article 19(1)(a) of the Indian Constitution** by precluding internet users in India from accessing information from around the world. It also violates freedom of expression and information as contemplated under **international human rights law**, which recognises that the freedom of expression includes the freedom to "*seek, receive and impart information and ideas of all kinds*".[7] Second, it has implications for **competition in the market**, as it risks encouraging larger players to become gatekeepers of information on the internet. The high compliance costs of the draft rule perpetuates dominant players' position in Indian markets by making it impractical for smaller players and newer entrants to compete.

3. **Draft Rule 3(8)** requires intermediaries to take down content upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency within 24 hours. Further, the draft rule requires intermediaries to retain such data for a minimum of 180 days, or for any such longer period as may be required by a court or by government agencies.

The grounds on which content can be considered unlawful are found, for the purposes of this draft rule only, in Article 19(2) of the Indian Constitution. Some of the grounds listed are

[6] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, 29 May 2015, Available from https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx.
[7] Article 19 of the International Covenant on Civil and Political Rights. Available from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

extremely vague and could be interpreted to include even legitimate speech. Some of these grounds include, "*in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality..* ". The term **"appropriate government" also does not find definition in the draft rules**, further broadening the scope of this draft rule.

Further, draft rule 3(8) contemplates a **data retention requirement** of a minimum of 180 days, or "*for such longer period as may be required by the court or by government agencies who are lawfully authorised.*" Specificity in periods for data retention, is a fundamental aspect of progressive data protection practices, as it imbibes the **principles of collection limitation, data minimisation, and purpose limitation**. All three principles have been recognised and adopted by the Srikrishna Committee of Experts on data protection in India and to this extent, this draft rule is in **direct conflict with the Personal Data Protection Bill, 2018.**

4. **Draft Rule 3(9)** requires intermediaries to deploy technology based automated tools for proactively identifying and removing or disabling public access to unlawful content.

ARTICLE 19 notes that this draft rule embeds the assumption that automated content moderation is part of the answer to problems like disinformation, hate speech, election manipulation and terrorist propaganda. We believe the draft rule's approach to proactively identify, remove or disable access to content using automated tools can have **dangerous unintended consequences taking into account technical limitations of automated systems, and additionally has the proclivity to violate fundamental rights under the Indian Constitution and international human rights law.**

The draft rule does not define what is meant by "unlawful information and content", making the scope of this rule **vague and open to arbitrary interpretation**. The standard to which these automated tools are expected to adhere to are nebulous at best, which **incentivises intermediaries to err on the side of caution** to avoid liability, thus resulting in over-censorship and restriction on legitimate speech. This is particularly worrying as the **draft rule does not stipulate an appeal mechanism** for users whose content has been taken down, nor does it contemplate the importance of **accountability, transparency, or scrutability** of these systems. Instead, it imposes a blanket obligation on intermediaries to deploy these tools.

In *Shreya Singhal v. Union of India* (2015),[8] the Supreme Court reaffirmed India's tradition of free speech in the technological age, and emphasized the limits of **reasonable restrictions** that can be used to limit free speech under the Indian Constitution. This is in line with international human rights law[9] with contemplates freedom of expression as a human right with **narrowly tailored restrictions** that must (i) be provided by law, (ii) in pursuit of a legitimate aim, and (iii) be necessary and proportionate to the aim pursued. **The intended use of automated tools under this draft rule does not satisfy these tests.**

[8] Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012.
[9] Article 19, Paragraph 3 of the International Covenant on Civil and Political Rights. For a detailed explanation and interpretation, see General Comment No 34, CCPR/C/GC/3, para. 21, 22.

Specifically on the question of intermediaries, in *Shreya Singhal*, the Supreme Court held that private companies could not be tasked with ascertaining the legality of content themselves, and should rely on a court order or notification by the appropriate government to have 'actual knowledge" of unlawful content, "*for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.*" **This draft rule, by requiring private intermediaries to proactively identify, remove or disable public access to unlawful content, is thus, in direct conflict with the precedent laid down by the Supreme Court in *Shreya Singhal*.**

Further, the definitions of hate speech, disinformation, terrorist propaganda are extremely subjective and complicated even for the human eye. The assumption that automated tools have the ability to moderate content efficiently and accurately is deeply flawed. **Even the most sophisticated machine learning systems today are not equipped to understand context and nuance in speech**, social intricacies, let alone complicated constructs like hate speech and fake news. While machine learning systems can carry out rudimentary sentiment analysis, the ability of these systems to understand key aspects of speech - tone, context, sarcasm and irony - is extremely limited at present.[10]

Finally, and most importantly, the draft rule assumes that automated tools are the appropriate mechanism to proactively monitor content and tackle problems like hate speech and election manipulation. **This trust in automated systems should be demonstrated and earned, but the growing global tendency has been instead to assume their appropriateness, which this draft rule does.** Even once these systems reach greater levels of sophistication in re: context and nuance, ongoing research in the field indicates that automated tools embed and potentially exacerbate existing biases, that these systems rely on models which perform in opaque and unfair ways, with the tendency to disadvantage vulnerable communities.[11] These tools are far from being neutral, and in fact encode societal discrimination and unfairness into inscrutable systems.[12] As we have shown through previous research,[13] this has **significant implications in jurisdictions like India**, and thus, we would urge MEITY to tread with extreme caution in this regard, and to reconsider this rule entirely.

[10] ARTICLE 19, Facebook Congressional testimony: Why "AI tools" are not the panacea, April 2018. Available from https://www.article19.org/resources/facebook-congressional-testimony-ai-tools-not-panacea/.
[11] Safiyah Umoja Noble, Algorithms of Oppression: How search engines reinforce racism, 2018. *New York University Press, New York.*
[12] Virginia Eubanks, Automating Inequality: How high tech tools profile, police, and punish the poor, Page 190, January 2018. *St. Martin's Press, New York.*
[13] Vidushi Marda, Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making, October 2018. 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences.* Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240384.