CUTS International

RESPONSE PAPER

FOR

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

ON 'THE INFORMATION TECHNOLOGY INTERMEDIARY GUIDELINES (AMENDMENT) RULES, 2018'

BACKGROUND

Consumer Unity and Trust Society (CUTS)[1] expresses its gratitude to the Ministry of Electronics and Information Technology (MeitY), for inviting comments and suggestions on The Information Technology Intermediary Guidelines (Amendment) Rules, 2018 (hereinafter as 'Draft rules').

ABOUT CUTS

In its 36 years of existence, CUTS has come a long way from being a grassroot consumer-centric organisation based in Jaipur, to opening overseas Resource Centres in Hanoi,[2] Nairobi,[3] Lusaka,[4] Accra,[5] Geneva[6] and most recently in Washington DC[7]. It continues to remain an independent, non-partisan and not for profit economic policy think tank, while opening various programme centres, namely: Centre for International Trade, Economics & Environment (CITEE);[8] Centre for Consumer Action, Research & Training (CART);[9] Centre for Human Development (CHD);[10] and Centre for Competition, Investment & Economic Regulation (CCIER).[11] It has been working towards enhancing the regulatory environment through evidence-backed policy and governance related interventions across various sectors and national boundaries.[12]

CUTS has been working on the issues related to privacy, data protection and digital economy from the perspective of safeguarding the interests of consumers. It has implemented several evidence-based research led advocacy and capacity building initiatives in this regard. It has published several papers, research publications, op-eds on the area of privacy and data protection and has also engaged with law makers, and policy influencers on the subject.

CUTS' USER PERCEPTION SURVEYS

Recently, CUTS commissioned a survey on privacy, data protection and user welfare in India. The objective was to understand perception and experience of users with respect to

[1] http://cuts-international.org/
[2] http://cuts-hrc.org/en/
[3] http://www.cuts-international.org/ARC/Nairobi/
[4] http://www.cuts-international.org/ARC/Lusaka/
[5] http://www.cuts-international.org/ARC/Accra/
[6] http://www.cuts-geneva.org/
[7] http://www.cuts-wdc.org/
[8] http://www.cuts-citee.org/
[9] http://www.cuts-international.org/CART/
[10] http://www.cuts-international.org/CHD/
[11] http://www.cuts-ccier.org/
[12] http://cuts-international.org/pdf/About-CUTS-2018.pdf

privacy; purpose of data collection; trust and confidence in data sharing; use of data collected; strategies for data protection, safety and security; data breach, among others, in relation to data collected by online and offline service providers, and the government. The survey was conducted in six states (Uttar Pradesh, West Bengal, Punjab, Assam, Andhra Pradesh and Maharashtra) with 2,400 respondents (10 percent of whom were non-internet users). The sample was distributed between urban, peri-urban and rural areas, with adequate representation of respondents from different education levels, occupations, genders and age groups (CUTS Privacy Survey)

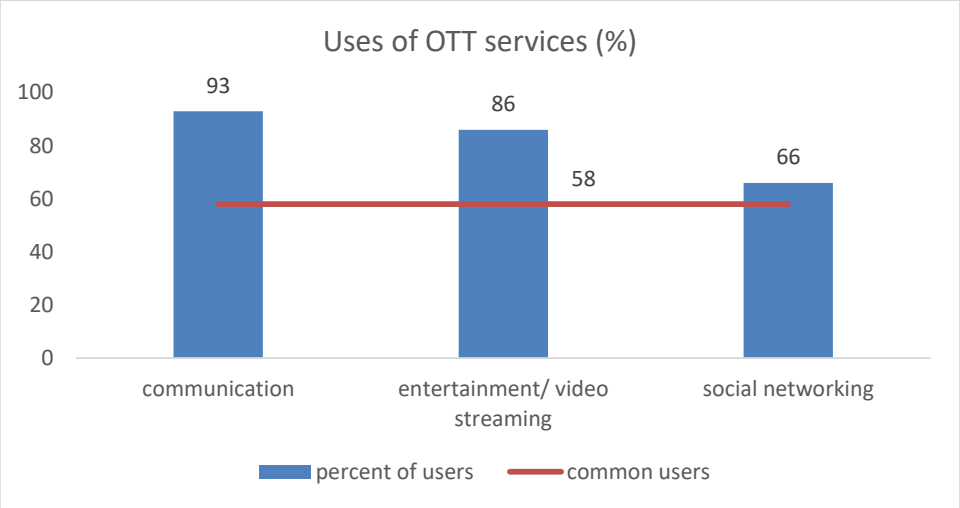
In addition, CUTS also commissioned a survey on benefits and challenges of over-the-top (OTT) services. The objective was to understand perceived benefits and challenges of OTT services on users' economic and social lives. The survey was conducted on 600 OTT users, out of which 496 were end consumers, and 104 were business owners. It covered 5 districts of Rajasthan, namely: Alwar, Kota, Jaipur, Jhunjhunu and Jodhpur (CUTS OTT Survey). Some of the key findings of these surveys have been used in this submission.

SUBMISSION

Rule 3(2) (j) and Rule 3(2)(k) Prohibited information

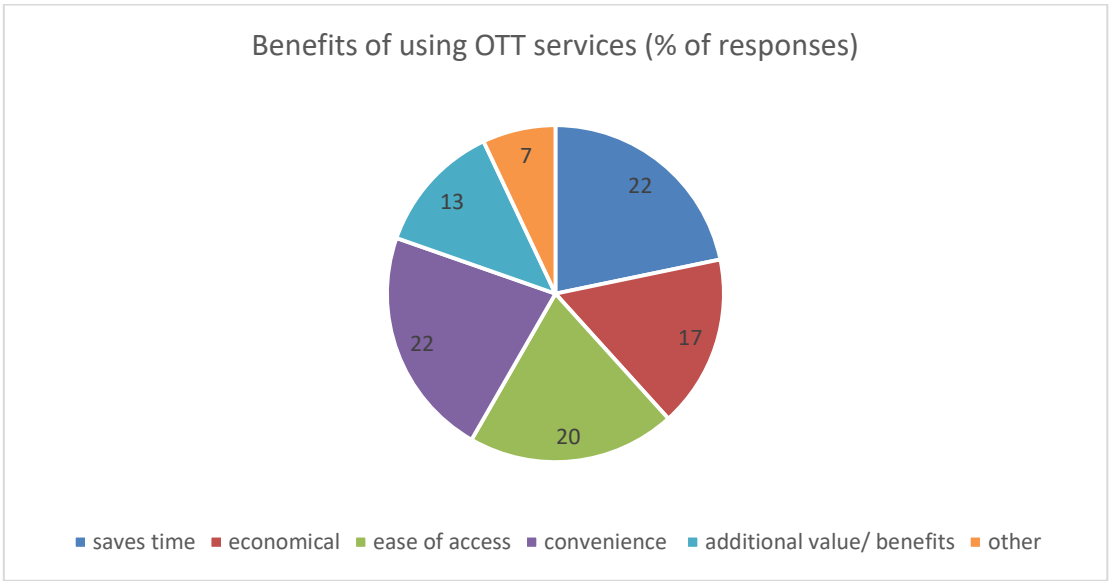
Rule 3 mentions due diligence to be observed by the intermediaries. Rule 3(2) provides that intermediaries are required to informs users not to host, display, upload, modify, publish, transmit, update or share certain prohibited information by way of privacy policies and terms and user agreements. The draft rules add sub rules (j) and (k) to Rule 3(2) and expand the list of prohibitions to include information: threatening public health and safety, promoting cigarettes, or threatening critical information infrastructure. The draft rules primarily wish to address and contain the nuisance on social media platforms while securing the privacy and freedom of speech of its citizens.[13]

CUTS OTT survey highlighted that intermediary services have now become part of lives of users and were most commonly used for communication, entertainment and social networking. Moreover, most users were using services of multiple intermediaries.



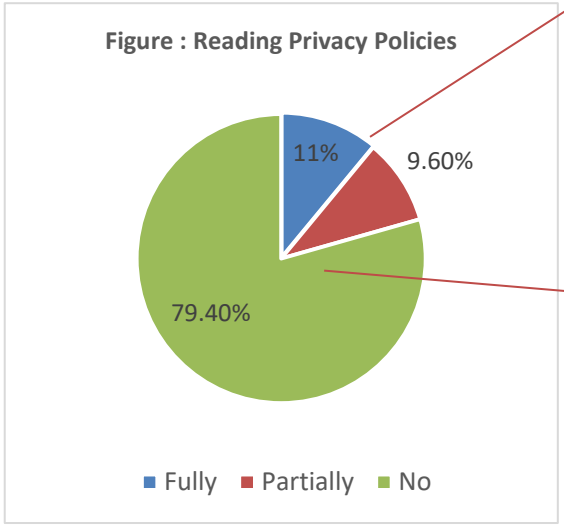
[13] 'Draft IT rules issued for public consultation' by the Ministry of Electronics & IT, Government of India, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770

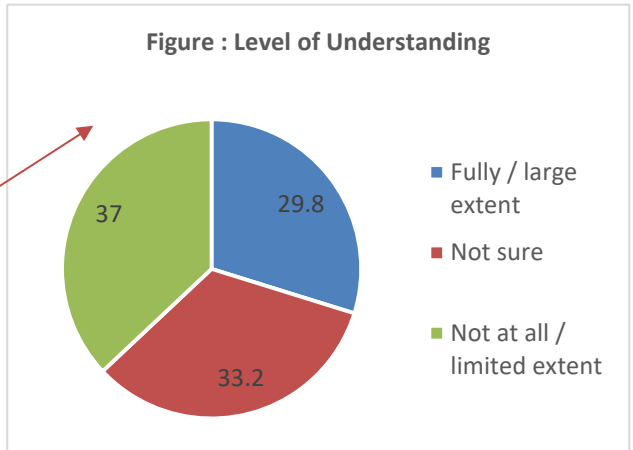
Key benefits to users of intermediary services include: time and cost savings, and ease of access. These services have enabled small businesses to grow in India.

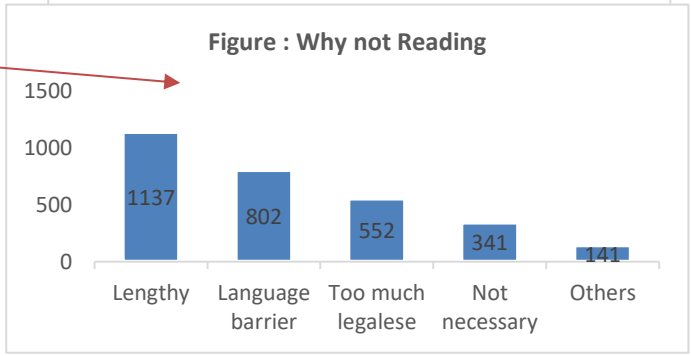


Given the benefits of intermediary services to users, any potential restriction must be carefully thought through in terms of implementability and potential costs of such restrictions must be weighed against potential benefits.

The key assumption of draft rules is that users of intermediaries would read terms and conditions and user agreements. In this regard, CUTS' privacy survey heighted that only 11% users read privacy policies, although 90% were aware of their right to privacy. Length, language barrier and legalese were noted as two main issues for not reading.[14]







[14] In addition to their inaccessibility and length, privacy policies also omit important information. Berkley Technology Law Journal, 'The "Nutrition Label" Approach to Privacy Policies' available at http://btlj.org/2016/06/the-nutrition-label-approach-to-privacy-policies/ (June, 2016)

Therefore, it appears that intermediary services offer several benefits to users and users are unlikely to read lengthy terms and conditions and privacy policies, which are full of legalese. As a result, the objective of informing users of additional prohibitions, as envisaged under the draft rules, may not be met.

Clearly, there is disconnect among commercial practices, user beliefs, and regulatory assumptions. The root of this mismatch probably lies in how user privacy regulation is conceptualised. Privacy policies are based on the "notice and choice" model, which purports that 'informed' users will choose the policy (and consequently the service provider) they like best, when all competing suppliers disclose their data practices.[15] Unfortunately in the Indian context, neither of the situation is true- the consumers are not aware or informed, and nor does the service provider follow a transparent format.[16]

Recommendation

Given this backdrop, the draft rules must be read and understood along with the India's first umbrella framework for data protection and privacy as envisioned in the draft Personal Data Protection Bill, 2018 (hereinafter as 'PDPB'). PDPB seeks to correct the broken notice and consent mechanism by laying down granular rules. Thenceforth, for consent to be valid and meaningful, it has to be free, specific, informed, clear and capable of being withdrawn. However, there may be several challenges in implementing such provision.

Consequently, to help users better understand prohibitions and other conditions mentioned in privacy policies and terms and conditions of intermediaries and make an informed choice, we suggest the draft rules encourage intermediaries to adopt a **"Nutrition Label for Privacy"** (hereinafter as 'privacy label'). A privacy label has been an area of interest in many developed nations[17] for some time now, whereby the consent form and privacy policy can be presented in a

[15]In addition to their inaccessibility and length, privacy policies also omit important information. The notice and choice model treats privacy as a commodity that consumers demand from suppliers. Consumers are expected to trade their privacy for the convenience offered by the goods or services offered by the suppliers. The failure of the notice and choice model is partly because there is no privacy left for consumers to choose and because of the "tradeoff fallacy," the condition of consumers having become so powerless that they think it is futile to try to control their data. See, Berkley Technology Law Journal, 'The "Nutrition Label" Approach to Privacy Policies' available at http://btlj.org/2016/06/the-nutrition-label-approach-to-privacy-policies/ (June, 2016)

[16] Ranking Digital Rights in India — The Centre for Internet and Society (2017). The report is an attempt to evaluate the practices and policies of companies which provide internet infrastructure or internet services, and are integral intermediaries to the everyday experience of the internet in India. Some findings and recommendations:

1. While compliance with these regulations also varies from company to company, there are barely any instances of companies taking initiative to ensure better privacy procedures than mandated by law, or to go beyond human rights reporting requirements as detailed in corporate social responsibility regulations.
2. Most companies take very little effort in obtaining meaningful user consent towards their policies, including efforts towards educating users about the import of their policies.
3. Most companies do not take much effort in maintaining robust or meaningful terms and conditions or privacy policies, which include an explanation of how the service could potentially affect a user's privacy or freedom of Expression.

[17] (a) Our results show that standardized privacy policy presentations can have significant positive effects on accuracy and speed of information finding and on reader enjoyment of privacy policies. Patrick Gage Kelley, Lorrie Cranor, 'Standardizing privacy notices: an online study of the nutrition label approach' available at https://www.researchgate.net/publication/221515415_Standardizing_privacy_notices_an_online_study_of_the_nutrition_label_approach (b) In 2010, the privacy nutrition label idea started becoming popular when the Federal Trade Commission recommended a privacy nutrition label approach. The CUPS lab, Carnegie Mellon University, USA has been developing a "privacy nutrition label" to make privacy policies easy to understand and compare. https://cups.cs.cmu.edu/privacyLabel/

readily intelligible format for users. The privacy labels do not depart from the notice and choice model of privacy regulation; they only address the flaws regarding the length and complexity of privacy policies.[18] They will be constructive in presenting the information in a simple and standardised format that is actually understandable, and allow users to quickly and efficiently find information, and help them make their own decisions about what services to use, and to trust. It will also make comparisons easy, while making the experience of reading a privacy policy more enjoyable. An initiative made in this direction will help empower users and enable them to exercise more agency over their data.

But the label use alone is not expected to be sufficient in modifying behaviour, ultimately leading to improved outcomes.[19] Some researchers have found that the co-relation is probably bi-directional,[20] which means that the users must be aware of the privacy harms and actively engage in taking measures to secure and protect their privacy and data. Designing policies with attributes which allow people to gain awareness and give meaningful consent is an elementary step in that direction.[21] The privacy survey recorded only 2% users reporting privacy violations. The fact suggests that most users are unaware of privacy violations and harms. And most users denied taking measures to protect their privacy. Additionally, 70% users felt the need for more awareness, and less than 40% considered the laws to be adequate in this regard.

Consequently, we suggest **creating mass awareness** for not just users but intermediaries, government and all the key stakeholders involved with respect to use and potential abuse of intermediary platforms.

Further, the Draft Rule 3(2)(j) proposes that ENDS can be promoted through an intermediary to the extent that is approved under the Drugs and Cosmetics Act, 1940 (***DC Act***). However, the Drugs Consultative Committee (***DCC***) in its 48th Meeting held on 24 July 2015, held that "*E-cigarettes are not covered under the definition of the term 'drug' and therefore do not come under the purview of Drugs and Cosmetics Act, 1940. E-cigarettes therefore cannot be regulated under the provisions of the said Act.*"[22] In 2018, the Central Government issued an Advisory which also acknowledged that ENDS are not, as of now, regulated under the DC Act. There is, therefore, an inconsistency in expecting regulation for ENDS products under the DC Act, when ENDS products lie outside the scope of regulation of the said Act. Should Rule 3(2)(j) be enforced, it would create an absurdity in the law by prescribing an impossible event. To that extent, Rule 3(2)(j) is not sound in law and must be suitably amended.

[18] The FDA's updated nutrition labels could improve your health—if you know how to read them, available at https://www.popsci.com/new-nutrition-labels-fda#page-3 (Oct, 2018)

[19] The FDA's updated nutrition labels could improve your health—if you know how to read them, available at, https://www.popsci.com/new-nutrition-labels-fda#page-3 (Oct, 2018)

[20] bi-directional meaning that both factors have an influence on one another. Nutrition labels may promote healthier eating, whereas individuals with healthier diets are more likely to seek out nutritional labels in the first place. The FDA's updated nutrition labels could improve your health—if you know how to read them, available at, https://www.popsci.com/new-nutrition-labels-fda#page-3 (Oct, 2018)

[21] The Good Notice Project by Stanford University brings together groups working on the challenges of presenting complex legal information in usable, comprehensible ways to lay people. http://legaltechdesign.com/GoodNoticeProject/2014/01/22/privacy-icons-alpha-release-mozilla-aza-raskin/

[22] Please find the report of the 48th DCC Meeting here.

Rule 3(4) Due diligence to be observed by intermediary

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. Monthly reminders are more likely to create warning fatigue and dissatisfaction among users, instead of increasing their awareness of this provision.

Recommendation

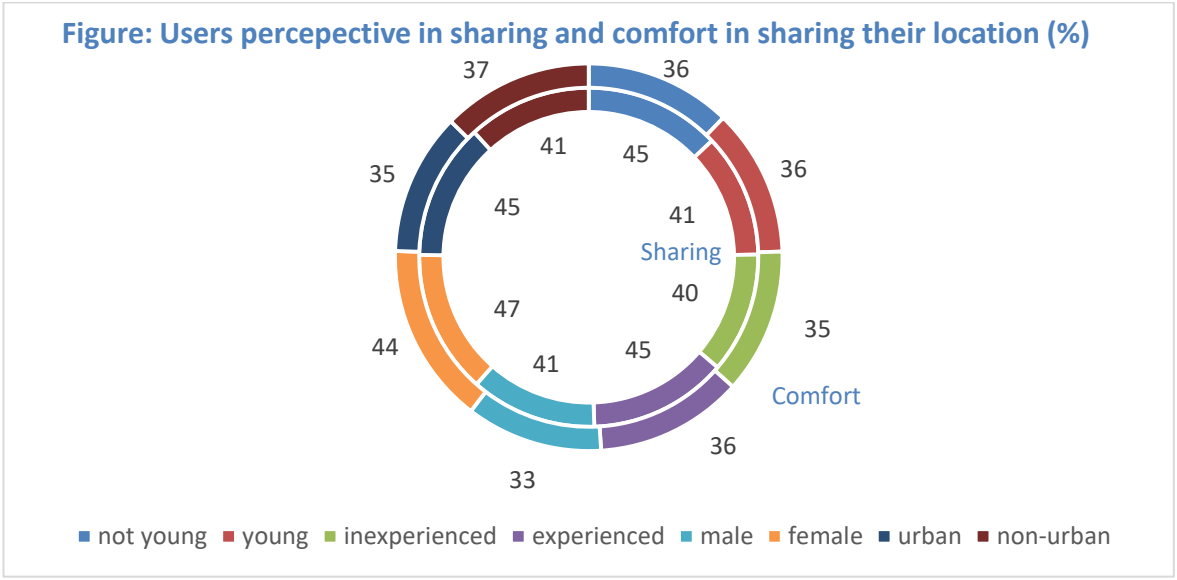
The manner of doing this needs to be clear given that accessibility of these terms is the key objective. Therefore, these should be limited to displaying them by publishing on the website (other modes may be a bit intrusive). Additionally, the Government also needs to play an equal role by framing policies and taking necessary measures to educate/sensitise citizens at grassroot level with support from civil society organisations.

Rule 3(5) Tracking of originators

The draft rules propose to amend rule 3(5) to require intermediaries to enable tracing of such originator of information on its platform as maybe required by government agencies who are legally authorised.

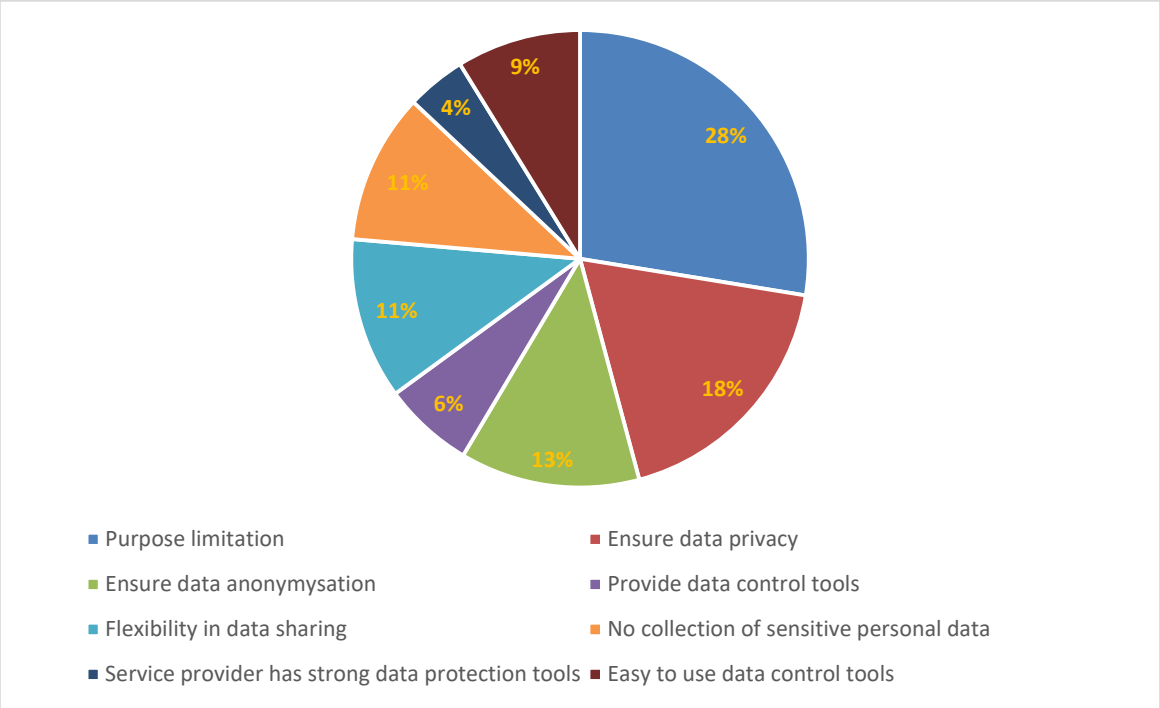
CUTS privacy survey revealed that some users may be sharing their personal information, and details like browsing history and location with online service providers despite not being comfortable in doing so. Consequently, users are unlikely to be comfortable if such data is used by intermediaries to track them.

Figure: Users percepective in sharing and comfort in sharing their location (%)



The privacy survey also revealed that less than half users were of the opinion that the data shared by them should be used for user verification. Also, data anonymisation i.e. inability of to identify the users, is one of the key user expectations from online service providers.

Figure: User expectations from online service providers (response %)



Recommendation

Consequently, any misuse of proposed provision to trace users might result in breach of user trust and confidence. Thus, there is a need to ensure that appropriate safeguards are put in place to ensure the proposed provision is not misused. To this end, the government should be able to invoke the proposed provision only when it is not left with any other means but to ask the intermediary to trace originators of information. In other words, the government should have exhausted all other options at its disposal to track originators of information and recourse to intermediaries should be the last resort. Further, reasons for requiring intermediaries to trace the originator should be clearly mentioned in the request so made and should be authorised by officer not below an appropriate senior rank (preferably joint secretary). Also, intermediaries should be expected to deploy reasonable efforts only to track originators of information and should not be expected to alter their business model (such as end-to-end encryption) in order to track originators.

3(9) Deploy technology based automated tool to proactively identify unlawful information

The proposed Rule 3(9) requires intermediaries to deploy technology based automated tools for proactively identifying and removing or disabling public access to unlawful information or content. 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."

Identification of potentially unlawful information or content is a huge responsibility and must be accompanied with adequate accountability mechanisms for intermediaries. Such power should not be misused to supress freedom of speech and expression.

Intermediaries tend to formulate community guidelines for use of their platforms and deploy automated tools and artificial intelligence to identify information posted in violation of such guidelines. While such self-regulation is well intentioned, it might result in supressing genuine and lawful information.

Recommendation

Consequently, such guidelines and self-regulation codes must be designed after robust public consultation, incorporating diverse point of views and upon ratification by legislature. While automated tools are being used to identify potentially unlawful information, they could also be used to address grievances of users and empower consumers who might have been unfairly targeted by such use.[23]

****

[23] Mehta, The potential of AI in empowering consumers, 09 January 2019, at https://www.livemint.com/Opinion/ruTtZ4WxAMoWJyJdKJuOEJ/Opinion--The-potential-of-AI-in-empowering-consumers.html