॥न्यायस्तत्र प्रमाणं स्यात्॥

NATIONAL LAW UNIVERSITY DELHI

Prof. (Dr.) Ranbir Singh
Vice-Chancellor

January 31, 2019

Shri Ajay Prakash Sawhney
Secretary
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan,
6, CGO Complex,
Lodhi Road, New Delhi - 110003

Subject: Submission of Comments on the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018

Dear Mr. Sawhney,

The *National Law University Delhi* (NLU Delhi) instituted by Act No. 1 of 2008 of National Capital Territory of Delhi is a public funded university established by the Government of NCT of Delhi on the initiative of the High Court of Delhi. The University established the *Centre for Communication Governance* (CCG) in 2013 to ensure that Indian legal education establishments engage more meaningfully with information law and policy, and contribute to improved governance and policymaking. CCG is the only academic research centre dedicated to working on the information law and policy in India and in a short period has become a leading centre on information policy in the region.

Through its *Civil Liberties* team, CCG seeks to embed human rights and good governance within information policy and examine the evolution of existing rights frameworks to accommodate new media and emerging technology. It seeks to protect and expand freedom of speech, right to assembly and association, the right to dignity, and the right to privacy in the digital age, through rigorous academic research, policy intervention, capacity building, and supporting strategic litigation. The *Technology and National Security* team looks at the role of international and domestic law in India's national security matters from a legal and policy perspective, with a particular focus on

(A University of Law Established in 2008 by Act No. 1 of 2008 of Delhi)
Sector-14, Dwarka, New Delhi - 110 078 ☎ :+91 11 2803 4253 🖷:+91 11 2803 4256
: ranbirsingh2107@gmail.com, vc@nludelhi.ac.in website: www.nludelhi.ac.in

cybersecurity and cyber conflict. It aims to build a better understanding of national security issues in a manner that identifies legal and policy solutions that balance the legitimate security interests and national security choices with the constitutional liberties and the rule of law.

We regularly engage with government ministries and commissions such as the Ministries of External Affairs, Law & Justice, Information Technology, and Communications, and the Competition Commission of India, and work actively to provide the executive and judiciary with useful research in the course of their decision-making on issues relating to information policy.

As part of our work, and given how critical it is to provide policymakers with well researched and useful material, we are submitting our response to the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018. We welcome the opportunity to comment on these draft rules and commend MeitY for adopting a public and consultative approach to the whole process.

We hope that the response is of assistance to MeitY. My colleague Mr. Sarvjeet Singh (sarvjeet.singh@nludelhi.ac.in) can provide any additional material required, and we are happy to offer any further support to MeitY.

With warm regards,
Yours sincerely,

Ranbir Singh

Encl: Comments on the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018.

cc:

(i) Shri Rakesh Maheshwari, Scientist G & Group Coordinator, Cyber- Laws and E- Security Group, MeitY
(ii) Shri Prafulla Kumar, Scientist G, Cyber- Laws and E- Security Group, MeitY
(iii) Dr. Dhawal Gupta, Scientist E, Cyber- Laws and E- Security Group, MeitY

(A University of Law Established in 2008 by Act No. 1 of 2008 of Delhi)
Sector-14, Dwarka, New Delhi - 110 078 ☎ :+91 11 2803 4253 🖷:+91 11 2803 4256
: ranbirsingh2107@gmail.com, vc@nludelhi.ac.in website: www.nludelhi.ac.in

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA (MEITY) ON THE DRAFT INFORMATION TECHNOLOGY [INTERMEDIARY GUIDELINES (AMENDMENT) RULES], 2018[1]

INTRODUCTION

We appreciate the government's concern regarding the misuse of social media, the resultant harm, and the challenges that it has brought for the law enforcement Agencies *(LEA)*[2]. We support the need to consider various efforts to make the Internet a safer space, and also to update the laws governing cyberspace in order to bring them in consonance with the technological advances, and global best practices, and to deal with illegal speech online.

However, the draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 *(Draft Rules)* if passed in the current form will not achieve their intended outcomes. The draft rules violate the fundamental rights to freedom of speech and expression, and privacy of Indian citizens as enshrined in the Constitution of India,[3] to which this government has declared its commitment[4].

---

[1] *Authored by* ***Sarvjeet Singh*** *with assistance from* ***Yesha Tshering Paul*** *and inputs from* ***Shrutanjaya Bhardwaj***, ***Smitha Krishna Prasad*** and ***Ujwala Uppaluri***.

[2] Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770, ¶ 4.

[3] *See* Chinmayi Arun, *The 'Purdah' amendment: Proposed changes to the IT Act could draw a veil over the Indian internet*, SCROLL (Jan. 24, 2019), https://scroll.in/article/910601/the-purdah-amendment-proposed-changes-to-the-it-act-could-draw-a-veil-over-the-indian-internet.

The draft rules, if enacted will privatize censorship, which has thus far been a power of the state, discharged primarily by the executive arm and subject to review for compatibility with constitutional bounds by the judiciary. Privatizing this power has an adverse effect on our core fundamental rights. Moreover, the censorship of the degree envisaged by Rule 3(2) read with Rule 3(9) of the draft rules will effectively guarantee unchecked surveillance and will violated the fundamental right to privacy.

As per the press note released with the draft rules, the object of the proposed amendment appears to tackle the menace of fake news/ misinformation and the circulation of obscene content,[5] and to make the social media platforms accountable under the law.[6] However, the proposed rules apply to all intermediaries[7] irrespective of their specific role or nature[8].

"Intermediaries" according to the Information Technology Act, 2000 (IT Act) with respect to any particular electronic records is defined as:

any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes.[9]

The amended definition of "intermediaries" after the 2008 amendment of the IT Act was hailed by some for its clear definition and extensive scope, expanding the type of entities that can claim safe harbor protection.[10] However, others have

---

[4] Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770, ¶ 3.

[5] Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770, ¶ 4.

[6] Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770, ¶ 5.

[7] The Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018, r. 2(k).

[8] *See* Chinmayi Arun and Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASES STUDIES 67 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

[9] The Information Technology Act, 2000, s. 2(1)(w).

[10] Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).

criticized it for failing to make allowances for functional differences between various intermediaries.[11]

The scope of this clause is extremely wide and includes everything ranging from social media services and communication platforms to ride hailing applications and cyber cafes. Moreover, this is not an exhaustive list and may include services not mentioned in the section.

In case of the draft rules there is no nexus between the object of the amendments[12] and the actual regulations in case of most of the entities which fall under the definition of intermediaries. For these entities, the obligations under the proposed amendment seem "entirely misplaced and inapplicable".[13] It is necessary for MeitY to identify the relevant intermediaries, based on reasoned and valid categorization, which have a nexus to the concerns that are sought to be remedied, and draft appropriate regulations (if permissible)[14] for such intermediaries.

PROBLEM OF EXCESSIVE DELEGATION

According to the doctrine of excessive delegation, delegation of essential legislative functions by a legislature to any other authority is unconstitutional.[15] The power to make changes in policy is an essential function and cannot be delegated.

---

[11] Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

[12] Draft IT rules issued for public consultation, PRESS INFORMATION BUREAU (Dec. 24, 2018), http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770, ¶¶ 4-5.

[13] Amba Kak, *Move fast and break things: Government's new rules on internet regulation could kill innovation and privacy*, TIMES OF INDIA (Jan. 4, 2019), https://timesofindia.indiatimes.com/blogs/toi-edit-page/move-fast-and-break-things-governments-new-rules-on-internet-regulation-could-kill-innovation-and-privacy/.

[14] While the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 were promulgated on April 11, 2011, on a bare reading of Sections 79 and 87(2)(zg) of the Information Technology Act, 2000 it is not apparent that the Act provides the government authority to make such distinctions between intermediaries. Section 79(2)(c) of the Information Technology Act, 2000 does state that "the intermediary observes…[and] also observes such other guidelines as the Central Government may prescribe in this behalf." However, a bare perusal of the act, it probably means that such guidelines (in addition to the due diligence requirement) apply to any and all intermediaries. Moreover, unlike cyber-cafe, it will be very problematic to define a set of intermediaries (without it being over or under inclusive).

[15] *See In Re Delhi Laws Act*, (1951) S.C.J. 527; *Harakchand v. India*, (1970) 1 S.C.J. 479. *See also* STANDING COMMITTEE ON SUBORDINATE LEGISLATION, PRACTICE & PROCEDURE-ABSTRACT SERIES (Feb. 2005), *available at* https://rajyasabha.nic.in/rsnew/practice_procedure/book13.asp.

The legislature is the master of legislative policy and if the delegate is free to switch policy it will lead to usurpation of legislative power itself.[16]

The authority which is the delegate is not allowed to widen or reduce the scope of the Act, and cannot legislate in the garb of making rules.[17] Moreover, delegated legislation should conform to the parent statue and cannot exceed the scope of enabling act.[18]

While determining a case of excessive delegation a court should take into account the subject-matter and the scheme of the statute, the provisions of the statute including its Preamble and the facts and circumstances and the background on which the statute is enacted.[19]

It is also a settled principle that the rule making power cannot be sub-delegated by the executive, unless such power is clearly granted by the enabling act. Such sub-delegation without being expressly granted by the parent act will be void.[20]

Many rules of the proposed guidelines fall outside the permissible limit of the enabling statute, which is the IT Act. These include Rules 3(5) and 3(7), and specific issues with these rules have been discussed below.

SPECIFIC CLAUSES

RULES 3(1) AND 3(2)

One of the conditions to receive immunity under Section 79 of the IT Act is the observance of due diligence by the intermediary.[21] The current due diligence

[16] *Avinder Singh v. Punjab*, (1979) 1 S.C.C. 137.
[17] *Agriculture Market Committee v. Shalimar Chemical Works Ltd.*, (1977) 5 S.C.C. 516.
[18] *See India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C .641; *State of Karnatak v. Ganesh Kamath*, (1983) 2 S.C.C. 40. *See also* Ujwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011* (July 16, 2012), https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules.
[19] *K.T. Plantation Pvt. Ltd. v. State of Karnataka, (2011) 9 S.C.C. 1*.
[20] *See India v. M/s Bhanamal Gulzarimal*, A.I.R. (1960) S.C. 475; *Bhagwati Saran v. Uttar Pradesh*, A.I.R. (1961) S.C. 928.
[21] For a detailed discussion of the various requirements for an intermediary to claim immunity under Section 79, Information Technology Act, 2000, *see* Chinmayi Arun and Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF

requirements were introduced by the government in the intermediary guidelines which were notified by the Central Government on April 11, 2011, in exercise of the powers conferred by Section 87(2)(zg) read with section 79(2) of the Act.

Under the proposed guidelines rule 3(1) require intermediaries to publish rules and regulations, privacy policies, and user agreements. Subsequently, Rule 3(2) require intermediaries to inform users to not make available or circulate a range on content provided in Rules 3(2)(a) to 3(2)(j). While the draft rules add Rules 3(2)(j) and (k), we believe that most of the provisions under Rule 3(2) should be removed from the guidelines, especially after the *Shreya Singhal* judgment.

The constitutionality of Rule 3(2) was challenged in the *Shreya Singhal* case.[22] This has been cursorily noted in the judgment, but there is no substantive discussion on the same and the conclusion refers only to Rule 3(4). Any future challenge to these rules will be upheld based on the principles laid down in *Shreya Singhal* and discussed below.

- ***BEYOND THE REMIT OF ARTICLE 19(2)***

The *Shreya Singhal* judgment categorically states that Section 79 and *by implication the guidelines framed under it* cannot be used to regulate unlawful acts which are not relatable to Article 19(2) of the Constitution.[23] This builds on the Court's reasoning by a five-judge constitution bench which held that any limitation on Article 19(1)(a) which does not fall within the purview of Article 19(2) cannot be upheld.[24]

In the draft rules, as well as the existing guidelines, numerous grounds under Rule 3(2) are not even legal standards, but merely subjective terms with no constitutional basis.

NATIONAL CASES STUDIES 71-74 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

[22] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 119.

[23] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 122 and 124.3.

[24] *Express Newspaper (Private) Ltd. v. Union of India*, (1959) S.C.R. 12.

Apart from Rules 3(2) (e), (i), and the terms "defamatory", "obscene", "pornographic", and "pedophilic" under Rule 3(2)(b), and in certain contexts Rule 3(2)(c), and arguably Rule 3(2)(k) and part of Rule 3(j) pertaining to "threatens public health or safety", none of the other grounds are cognizable under Article 19(2).[25] However, even certain terms which may fall within the ambit of Article 19(2), as used in the proposed rules are vague and overboard.

- ***VAGUE AND OVERBROAD TERMS***

The Supreme Court has repeatedly held that vague provisions must be struck down as being arbitrary and unreasonable.[26] Many of the terms listed under Rule 3(2) are subjective and not defined either in the current version or the proposed rules or the IT Act itself. These include terms like "grossly harmful", "harassing", "blasphemous", "hateful", "racially", "ethnically objectionable", "invasive of another's privacy", "disparaging", "harms minors in any way", "grossly offensive", "menacing" and "insulting any other nation".

Many of these terms were declared vague by the Supreme Court in *Shreya Singhal*.[27] Majority of the remaining terms are nebulous in nature[28] and provide no opportunity to know what is prohibited.[29] The *Committee on Subordinate Legislation* as far back as 2013 stated that these terms are ambiguous and asked MeitY to incorporate the definition of all these terms within the guidelines itself, and also ensure that no new category of offences are created by these guidelines.[30]

---

[25] *See* Ujwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011* (July 16, 2012), https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules.

[26] *State of Madhya Pradesh v. Baldeo Prasad*, (1961) 1 S.C.R. 970; *A.K. Roy & Ors. v. Union of India & Ors.*, (1982) 2 S.C.R. 272; *See Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 67-79.

[27] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 85.

[28] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 79.

[29] *Kartar Singh v. State of Punjab*, (1994) 3 S.C.C. 569, ¶¶ 130-131.

[30] STANDING COMMITTEE ON SUBORDINATE LEGISLATION, THIRTY FIRST REPORT ON THE INFORMATION TECHNOLOGY RULES (March 21, 2013), ¶ 25-26, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.

Some terms under Rule (2) arguably fall within the scope of Article 19(2) including terms from Rule 3(2)(b) - "defamatory"[31], "obscene"[32], "pornographic"[33], and "pedophilic"[34], Rule 3(2)(i) – "threatens the integrity, defense, security or sovereignty and of India"[35], "friendly relations with foreign states"[36], "public order"[37], "incitement to commission of any cognizable offence"[38], Rule 3(2)(j) – "threatens public health"[39] and "safety"[40] and Rule 3(2)(k) – "threatens critical information infrastructure" [41]. However, since these terms have been lifted from Article 19(2) of the Constitution, the body making the determination of whether a piece of content falls within the purview of Article 19(2), has to follow the judicial interpretation and the legal jurisprudence which has developed and provides the scope of these grounds.

For example, for a piece of content to be a threat to public safety, it must meet the public order standard[42] and a threat to critical information infrastructure must meet the very high threshold of the security of state standard.

---

[31] Will fall under the "defamation" ground, the Constitution of India, 1950, art. 19(2).
[32] Will fall under the "decency or morality" ground, the Constitution of India, 1950, art. 19(2).
[33] Will fall under the "decency or morality" ground, the Constitution of India, 1950, art. 19(2).
[34] Will fall under the "decency or morality" ground, the Constitution of India, 1950, art. 19(2).
[35] Will fall under the "interests of the sovereignty and integrity of India" and "the security of the State" grounds, the Constitution of India, 1950, art. 19(2).
[36] Will fall under the "friendly relations with foreign States" ground, the Constitution of India, 1950, art. 19(2).
[37] Will fall under the "public order" ground, the Constitution of India, 1950, art. 19(2).
[38] Will fall under the "incitement to an offence" ground, the Constitution of India, 1950, art. 19(2).
[39] Will arguably fall under the "public order" ground, the Constitution of India, 1950, art. 19(2). *See Romesh Thappar v. State of Madras*, (1950) S.C.R. 594. However, according to the Supreme Court in *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶ 45, "Public order is not the same thing as public safety and hence no restrictions can be placed on the right to freedom of speech and expression on the ground that public safety is endangered".
[40] Will arguably fall under the "public order" ground, the Constitution of India, 1950, art. 19(2). *See Romesh Thappar v. State of Madras*, (1950) S.C.R. 594. However, according to the Supreme Court in *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶ 45, "Public order is not the same thing as public safety and hence no restrictions can be placed on the right to freedom of speech and expression on the ground that public safety is endangered".
[41] Will fall under the "the security of the State" or presumably "public order" grounds, the Constitution of India, 1950, art. 19(2).
[42] *See* CHINMAYI ARUN, ARPITA BISWAS AND PARUL SHARMA, HATE SPEECH LAWS IN INDIA 14-16 (2018); Sarvjeet Singh, Parul Sharma and Kritika Bhardwaj, *Public Order, Hate Speech and the Indian*

The constraint on promotion of cigarettes, tobacco products, consumption of alcohol and electronic nicotine delivery system (ENDS) is also vague and overbroad[43], since promotion is not defined.

Rule 3(2) in the present form regulates protected speech and because of its overbreadth has a chilling effect on the freedom of expression.

RULE 3(4)

Under rule 3(4) an intermediary is obligated to inform all its users "at least once every month" that noncompliance with rules and regulations and other agreements and policies may lead to termination of services being provided by the intermediary.

The proposed provision is paternalistic and will lead to notice/ consent fatigue. However, there is no apparent violation of users' fundamental rights.

The draft rule lumps all intermediaries together, while possibly being aimed at intermediaries where the users have to register or sign-up or actively generate or communicate content.

The provision does not define what a "user" is in this context. It will be technically unfeasible for a large number of intermediaries to undertake this task. For instance, users may not regularly use services such as search engines (when not signed in), cyber-cafes or provide any contact information to the service provider, creating a situation where it is difficult to effectively communicate these terms to the user in a regular manner, or identify how often each user has been informed of the terms and record actual implementation of the rule.

Constitution, XXXV (4) Common Cause India Journal 5-11 (2016). However, according to the Supreme Court in *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶ 45, "Public order is not the same thing as public safety and hence no restrictions can be placed on the right to freedom of speech and expression on the ground that public safety is endangered".

[43] *See* Yesha Tshering Paul, *Fake News: Misguided Policymaking To Counter Misinformation*, BLOOMBERGQUINT (Jan. 14, 2019), https://www.bloombergquint.com/opinion/fake-news-misguided-policymaking-to-counter-misinformation.

Moreover, if the owner of the intermediary is an Indian citizen, she can raise a potential claim (albeit a bit weak) of violation of Article 19(1)(g) of the Constitution.

RULE 3(5)

Rule 3(5) require intermediaries to provide assistance or information concerning state security to a government agency within a period of 72 hours of being asked by such agency. The rule also requires them to provide traceability of the originator[44] of certain information.

This rule is a substantive amendment of Rule 3(2)(7) of the existing guidelines. The current rule provides that only a lawfully authorized government agency can ask an intermediary for certain information or assistance. However, the proposed rule expands the nature of agencies to "any government agency". Any agency will include among others any ministry, department, commission, board, authority, municipal and other local authority, and statutory body.

The proposed language provides unbridled power to thousands of government agencies to request information and assistance from the intermediary. This will be violative of the right to privacy. The rule should retain the language from the current guidelines and allow only lawfully authorized government agencies to seek such information and assistance.

There is also a need to define/ clarify as to what is meant by lawful order in this instance. Unlike Sections 69 and 69B of the Act and rules framed under those sections[45], there are no safeguards provided in the instant case. Without any safeguards, the proposed rule and even the existing rule will fall foul of the tests laid down in the *Puttaswamy* judgment[46] for infringing the right to privacy.

The proposed rule is also ambiguous. The first part of the rule states that "*when required by lawful order, the intermediary shall, within 72 hours of*

[44] The Information Technology Act, 2000, s. 2(1)(za).

[45] The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

[46] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.

communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto."

While "security of state" is a term found is the Constitution, "cybersecurity" needs to be defined or at least the gravity of threat to cybersecurity after which the intermediary has to undertake these obligations. The phrase "protective or cyber security*"* is not clear and leads to ambiguity. The phrase should be *"*protective of cyber security*"*. However, that is unnecessary since this is covered by the phrase *"*concerning security of the State or cybersecurity*"*. Additionally, an expansive reading of "and matters connected with or incidental thereto" will allow the state an unfettered access to data which would violate the right to privacy.

- ***TRACEABILITY AND ENCRYPTION***

The second part of the rule mandates an intermediary to provide traceability to find the originator[47] of certain information. Traceability needs to be defined and it should be specified as to what exactly the government requires when it requires the intermediary to trace the originator. This will help to pre-empt the claim that it may be technically impossible to provide the kind of traceability that the state expects. Even in case an intermediary is not end-to-end encrypted, an originator may be using a VPN to browse the Internet or Tor to connect to it. In such instances there is only very limited information that an intermediary will be able to provide.

There are conflicting opinions whether the provision of traceability (as generally understood) can be introduced without breaking encryption.[48]

The U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated that encryption and anonymity are

[47] The Information Technology Act, 2000, s. 2(1)(za).

[48] *See* Press Trust of India, *Building traceability will undermine end-to-end encryption: WhatsApp*, INDIAN EXPRESS (Aug. 23, 2018), https://indianexpress.com/article/technology/tech-news-technology/building-traceability-will-undermine-end-to-end-encryption-whatsapp-5321806/; Himanshu Gupta and Harsh Taneja, *WhatsApp has a fake news problem—that can be fixed without breaking encryption*, COLUMBIA JOURNALISM REVIEW (Aug. 23, 2018), https://www.cjr.org/tow_center/whatsapp-doesnt-have-to-break-encryption-to-beat-fake-news.php.

essential to protect the rights of privacy and freedom of expression online, and any limitations on them should be narrow.[49]

The freedom of speech and expression across the whole of the internet as a medium is seriously and disproportionately undermined by this requirement, if it requires breaking encryption. Where speakers in the offline context were assured a limited degree of secrecy and obscurity in their communications, the proposed measure renders encrypted and therefore secret communication impossible.

In *Puttaswamy*[50], it was recognized that a right to cognitive privacy – that is the right to think and work through one's thoughts and beliefs and develop opinions and positions without interference – was a part of the right to privacy. Without the opportunity for this right to reflect, a key object of Article 19(1)(a) which is to lay the foundations for a vibrant and deliberative electorate and democracy whose citizens are genuinely informed and aware,[51] is seriously impaired.

By creating the capacity for surveillance at will and with neither the opportunity for speakers to be served any notice nor any opportunity for them to contest improper uses of the capacity, such a provision expands the state's capacity for invisible and unaccountable surveillance.

This measure is problematic in three respects. *First*, as explained above, unlike in respect of the processes under Sections 69 and 69B of the IT Act[52], not even a minimally rights respecting procedure for the exercise of this sweeping power is specified. *Second,* this measure amounts to shifting the natural presumption from one of innocence to one of guilt. It is ordinarily understood that ordinary citizens will be left untouched in the enjoyment of their rights – including the rights to speak, to associate and to privacy – until the state demonstrates some reasonable justification for limiting their rights. By the proposed measure, the expressive capacity of citizens

[49] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 56, A/HRC/29/32 (May 22, 2015) (David Kaye).
[50] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (Bobde, J., sep. op.).
[51] *Union of India v. Association for Democratic Reforms*, 2002 (3) S.C.R. 294.
[52] For an analysis of safeguards under Section 69 and Section 69B of the Information Technology Act, 2000 *see* Chinmayi Arun and Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASES STUDIES 75-79 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

is diminished without the showing of any cause sufficient under constitutional law. *Third*, by applying this inverted presumption to all citizens and all speech online, this proposed draft rule assures its unconstitutionality under any standard of review – whether rigorous or minimal. In contrast to a basis in targeted suspicion, generalized suspicion would neither satisfy the classic test in *V.G. Row*[53], nor would it meet the new standard of proportionality adopted in respect of privacy in *Puttaswamy*[54].

- ***EXCESSIVE DELEGATION***

Sections 69 and 69B of the Act read with their respective subordinate legislations[55] provide the procedure for access by law enforcement agencies to information available with the intermediary.

A delegated legislation apart from being challenged on the ground that it exceeds the parent statue, can also be challenged for being contrary to other statutory provisions.[56] In the present case, parts of the proposed Rule 3(5) that are in conflict with Sections 69 and 69B and rules framed under those. Rule 3(5) is beyond the mandate of the parent provision i.e. Section 79(2) and thus void.

RULE 3(7)

The proposed rule requires that any intermediary with more than 50 lakh users in India or who is in a list notified by the government, needs to incorporate in India, have permanent office in India and appoint a nodal officer in India.

The rule, like a lot of other proposed rules is vague and ambiguous. It does not define/ explain what a "user" is for the purposes of this rule. India has over 560

[53] *State of Madras v. V.G. Row*, (1952) S.C.R. 597.
[54] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (Chandrachud, J.) and (Kaul, J., sep. op.) whose opinions represent a majority of 5 judges of the 9 on the bench in this case).
[55] The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
[56] *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C. 641. *See* Ujwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011* (July 16, 2012), https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules.

million Internet subscribers as of September 2018[57], and this number is probably over 600 million currently[58]. There is no rational given as to why this number is chosen. MeitY should also clarify how it will determine the number of users, once the term is defined. Otherwise it will be impossible to implement this rule.

- ***POTENTIAL VIOLATION OF ARTICLE 19(1)(A)***

If the burden of incorporation and maintaining an office in India proves to be too onerous certain intermediaries will probably stop providing services in India. Such a situation will give rise to a potential violation of the right to freedom of expression.[59] The right to freedom of speech and expression includes the right to receive information[60], and the court has held the right to a diverse media environment as an integral part of Article 19(1)(a) of the Constitution.[61] This interpretation is consistent with the internationally recognized principle of freedom of expression codified in Article 19 of the International Covenant on Civil and Political Rights[62] to which India is a signatory.

- ***EXCESSIVE DELEGATION***

Rule 3(2)(7)(i) and (ii) are beyond the scope of Section 79(2) of the IT Act. The executive in the garb of rulemaking is legislating and widening the scope of the

[57] Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators: July – September 2018*, ii (Jan. 8, 2019), available at https://main.trai.gov.in/sites/default/files/PIR08012019.pdf.

[58] India is adding 10 million active internet users per month: Google, BUSINESS STANDARD (June 27, 2018), https://www.business-standard.com/article/current-affairs/india-is-adding-10-million-active-internet-users-per-month-google-118062700882_1.html.

[59] *See* Chinmayi Arun, *The 'Purdah' amendment: Proposed changes to the IT Act could draw a veil over the Indian internet*, SCROLL (Jan. 24, 2019), https://scroll.in/article/910601/the-purdah-amendment-proposed-changes-to-the-it-act-could-draw-a-veil-over-the-indian-internet.

[60] *Bennett Coleman v. Union of India*, (1972) 2 S.C.C. 788 (Mathews, J., dissenting); *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C .641; *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161; *Sahara India Real Estate Corporation Ltd. & Ors. v. SEBI & Anr.*, (2012) 10 S.C.C. 603; *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 21.

[61] *Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, (1995) 2 S.C.C. 161, ¶¶ 201(3)(a)-(b).

[62] International Covenant on Civil and Political Rights, art. 19, (Dec. 16, 1966), 999 U.N.T.S. 171.

Act. Moreover, since section 79(2) does not expressly allow the executive to sub-delegate, any list of specific intermediaries prepared will be void.[63]

RULE 3(8)

The proposed rule 3(8) is an amendment to Rule 3(4) of the current guidelines. It incorporates the changes laid down in the *Shreya Singhal* judgment regarding the actual knowledge standard and the scope of content that can be taken down.

The rule states that on receiving actual knowledge in form of a court order or on being notified by an appropriate government agency, an intermediary shall remove or disable access to content relating to unlawful acts within the scope of Article 19(2) within a period of 24 hours. It also requires the intermediary to preserve information relating to such take downs for a period of at least 180 days and maybe longer if required by a court or authorized agencies.

The proposed rule in accordance with *Shreya Singhal* incorporates the language of Article 19(2) to the guidelines. Therefore, any court or any other body determining whether a piece of content is unlawful and within the purview of Article 19(2) has to be very careful about the boundaries and judicial interpretation of these terms, and not to expand their scope. It may not be enough to state one of the grounds under Article 19(2), but will possibly require the exact unlawful act to be identified[64]. The phrase "appropriate Government" and "its agency" should be defined. This will limit the unfettered power to various government bodies and specify who can ask for the takedown of content.

Moreover, the new rule reduces the maximum time period available to the intermediary for removing or disabling content from 30 days[65] to 1 day. The

[63] *See India v. M/s Bhanamal Gulzarimal*, A.I.R. (1960) S.C. 475; *Bhagwati Saran v. Uttar Pradesh*, A.I.R. (1961) S.C. 928; S.P. SATHE, ADMINISTRATIVE LAW 56-57 (2008).

[64] *See* Shrutanjaya Bhardwaj, *Comments on the Draft Intermediary Guidelines (Amendment) Rules, 2018*, 1 (Jan. 4, 2019).

[65] Ministry of Electronics & Information Technology, Government of India, *Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000* (Mar. 18, 2013), *available at* http://meity.gov.in/sites/upload_files/dit/files/Clarification%2079rules(1).pdf. *See* Chinmayi Arun and

proposed rules should differentiate between content[66] and have different time period for different content.

Unlawful acts relating to "the sovereignty and integrity of India", "the security of the State", and potentially "public order", which require an urgent response can have a period of 24-48 hours. Unlawful acts relating to other grounds in Article 19(2) can have a time period of at least 14 days[67]. While the authority issuing the order will (presumably) apply its mind, this period will also allow the intermediary to review the content and decide its validity in relation to this rule.

If the time period remains 24 hours for all the content, to claim the immunity under Section 79, the intermediaries will err of the side of removing content and in most instances will take down the content without adequately examining it.[68] This will lead to censorship and takedown of lawful speech.[69]

The rule also requires retention of content that is disabled or taken down. However, it does not provide for conditions of such preservation, or describe what kind of investigation is permitted into such information. Where such data consists of personal information, the rules will need to ensure that data retention procedures, as well as the procedures to be followed at the time of investigation, or transfer of the information to the government agencies or courts for such investigation are respectful of the right to privacy and the principles of data protection in *Puttaswamy*

Sarvjeet Singh, *Online Intermediaries in India*, in GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASES STUDIES 74-75 (Urs Gasser and Wolfgang Schulz ed. 2015, Berkman Center Research Publication No. 2015-5).

[66] *See* Jens-Henrik Jeppesen, *The European Commission's draft regulation on 'terrorist content' requires significant revision*, CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 21, 2018), https://cdt.org/blog/the-european-commissions-draft-regulation-on-terrorist-content-requires-significant-revision/.

[67] Recent initiative in Europe have a different time periods ranging from 1 hour to

[68] *See* Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India*, 7 N.U.J.S. L. Rev. 73, 83 (2014).

[69] *See* Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET & SOCIETY, BANGALORE 20-23 (Apr. 10, 2012), https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf/view; Daphne Keller, *Empirical Evidence of "Over-Removal" by Internet Companies under Intermediary Liability Laws*, CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Oct. 12, 2015), http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

(in the absence of any specific data protection laws in India). The term "government agencies" also needs to be defined. The rule also lacks any outer time limit for retention of the data, and this will be violative of test laid down in *Puttaswamy*.

It is also useful to note that preservation and retention of information by intermediaries is already dealt under Section 67C of the IT Act, and ideally the issue of retention should be dealt under that section.

The proposed rule or the existing rule have no safeguards against misuse. To remedy that, it should be mandatory for the body asking for takedown to record its reasons in writing. In all cases except for those that fall within the 1-2 days takedown period, the intermediary and the originator (if identified) should be heard before passing an order.[70] In cases of 1-2 days takedown period, there should be an ex-post facto hearing, and the content should be enabled/ put-up again if the committee is satisfied that such content does not fall within the ambit of Article 19(2).

It may be useful to set up a dedicated body/ bodies in different states (like under Section 69A) to deal with these issues. However, to avoid misuse and adhere to the scope of restrictions in Article 19(2) it is necessary to have judicial oversight[71]. While the exact nature and scope of the body will require an in-depth examination, MeitY should start considering this option.

RULE 3(9)

This rule mandates the intermediary to use automated tools or other appropriate mechanisms to proactively identify and disable/ remove unlawful content.

Shreya Singhal has already held that an intermediary should not be made to judge the validity of any content.[72] Moreover, since the proposed rule does not define "unlawful information or content" it suffers from vagueness and is void. The rule also

[70] *See Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 115.
[71] *See Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) S.C.C. OnLine S.C. 1642, ¶ 447(4)(f).
[72] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 121-122.

does not define what is “appropriate mechanisms” which can be used in place of automated tools.

A programme for proactive monitoring and censorship, such as by using algorithms in order to detect and block content, raises several other concerns. These obligations will require encrypted intermediaries to break their encryption. The problems relating to this have already been discussed above. Additionally, since these rules apply to all the intermediaries it will be practically impossible for some like cyber-cafes to follow these rules and the rule will not be of relevance to several others like ride hailing platforms among others.

Further, at the threshold, any programme for automatic censorship and prior restraint by an intermediary, rests on the foundation of total prior surveillance.[73] Under this rule private entities (namely, the intermediary) are left in total control of users’ rights freedom of expression and to privacy online. As these entities are not ‘State’ for the purposes of Part III of the Constitution, they are under no legal obligation to respect or protect fundamental rights or even to apply basic requirements of natural justice, including the rights to notice and to a hearing when decisions adverse to a citizen’s rights are taken. The state under this rule is outsourcing the judicial function to private entities.

At a general level, the impulse to introduce technical measures to address problematic speech online is understandable, given the volume of communication on each online service at the content layer of the Internet. The Supreme Court has recognized this concern and noted the tremendous difficulties associated ensuring review and takedown of content on individualized basis.[74] Nevertheless, algorithmic blocking must be approached with circumspection and careful advance consideration.

[73] *See* Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism 9-10, OL OTH 71/2018 (Dec. 7, 2018) (David Kaye, Joseph Cannataci and Fionnuala Ní Aoláin).
[74] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 122.

There is a growing awareness of the limitations and pitfalls of algorithmic systems.[75] These technologies are inaccurate[76] and prone to both over inclusive and under inclusive outcomes.[77] Automated tools are a blunt instrument, with an incapacity to correctly register tone and context (which can vary across cultures, classes and other social dimensions) in the manner a human reader would be able to[78] and disproportionally affect marginalized speakers and communities[79].

Finally, over-censorship, by which a great deal of lawful content is disabled, is a near certainty.[80] The legal consequence of failing to screen content through these means is a lifting of the intermediary safe harbour under Section 79 of the parent act. Intermediaries acting rationally and in their ordinary best interests are offered no real incentive to preserve users' freedom of speech and a serious disincentive to the retention of problematic content on their services. The natural choice for any rational actor would be to over-censor and thus limit liability.[81]

---

[75] *See* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (Aug. 29, 2018) (David Kaye); EVAN ENGSTROM AND NICK FEAMSTER, THE LIMITS OF FILTERING: A LOOK AT THE FUNCTIONALITY & SHORTCOMINGS OF CONTENT DETECTION TOOLS (March 2017); NATASHA DUARTE, EMMA LLANSÓ AND ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS (November 2017).

[76] Daphne Keller, *Problem with Filters in the European Commission's Platforms Proposal*, CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Oct. 5, 2017), http://cyberlaw.stanford.edu/blog/2017/10/problems-filters-european-commissions-platforms-proposal.

[77] Jens-Henrik Jeppesen and Laura Blanco, *Taking 'Illegal' Content Online: The EC continues push for privatized law enforcement*, CENTER FOR DEMOCRACY & TECHNOLOGY (Oct. 7, 2017), https://cdt.org/blog/tackling-illegal-content-online-the-ec-continues-push-for-privatised-law-enforcement/.

[78] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 15, A/73/348 (Aug. 29, 2018) (David Kaye); NATASHA DUARTE, EMMA LLANSÓ AND ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 16, 19 (November 2017).

[79] NATASHA DUARTE, EMMA LLANSÓ AND ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 13-15 (November 2017).

[80] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET & SOCIETY, BANGALORE 20-23 (Apr. 10, 2012), https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf/view; Daphne Keller, *Empirical Evidence of "Over-Removal" by Internet Companies under Intermediary Liability Laws*, CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Oct. 12, 2015), http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

[81] *See* Chinmayi Arun*, Gatekeeper Liability and Article 19(1)(a) of the Constitution of India*, 7 N.U.J.S. L. Rev. 73, 83-86 (2014); Emma Llansó, German Proposal Threatens Censorship on Wide Array of

CONCLUSION

There is a need to make the Internet a safer space. However, the proposed guidelines do not fulfil that aim and will instead lead to prior restraint, chilling effect, complete loss of anonymity and surveillance. The proposed guidelines are vague and do not contain adequate safeguards against misuse, and in their current form violate a number of fundamental rights enshrined under the Constitution.

MeitY must take into account and adhere to the constitutional and international human rights principles, as well as the Supreme Court's jurisprudence on the freedom of speech and expression and the right to privacy, while updating the rules to bring them in consonance with the current India law.

We appreciate MeitY's open and consultative approach and hope that it will adopt the same approach before finalizing the rules.

Online Services, CENTRE FOR DEMOCRACY AND TECHNOLOGY (Apr. 7, 2017), https://cdt.org/blog/german-proposal-threatens-censorship-on-wide-array-of-online-services/.