

**IN THE HIGH COURT OF DELHI AT NEW DELHI**  
**(EXTRA ORDINARY CIVIL WRIT JURISDICTION)**

**W.P. (C) NO. \_\_\_\_\_ OF 2021**

**IN THE MATTER OF:**

**WHATSAPP LLC**

**...PETITIONER**

**VERSUS**

**UNION OF INDIA**

**...RESPONDENT**

**INDEX**

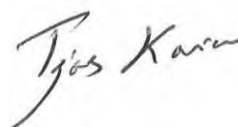
<b>Sr. No.</b>	<b>Particulars</b>	<b>Page Nos.</b>
1.	Court Fees	<b>1</b>
2.	Notice of Motion	<b>2</b>
3.	Memo of Parties	<b>3 – 4</b>
4.	Synopsis with List of Dates and Events	<b>5 – 14</b>
5.	Writ Petition under Article 226 of the Constitution of India for issuance of Writ of Mandamus or any other Writ as deemed appropriate along with supporting Affidavit.	<b>15 - 60</b>
6.	<b><u>ANNEXURE-P-1:</u></b> Copy of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.	<b>61 – 76</b>
7.	<b><u>ANNEXURE-P-2:</u></b> Copy of Petitioner's Key Updates to Petitioner's 2021 update to its Terms of Service and Privacy Policy.	<b>77</b>

8.	<b><u>ANNEXURE-P-3:</u></b> Copy of FAQ on end-to-end encryption.	<b>78 – 79</b>
9.	<b><u>ANNEXURE-P-4:</u></b> Copy of WhatsApp Encryption Overview, Technical White Paper, updated on October 22, 2020.	<b>80 – 92</b>
10.	<b><u>ANNEXURE-P-5:</u></b> Copy of Petitioner’s FAQ on Information for Law Enforcement Authorities.	<b>93 – 95</b>
11.	<b><u>ANNEXURE-P-6:</u></b> Copy of the Official Gazette Notification notifying the Information Technology (Intermediaries Guidelines) 2011.	<b>96 – 99</b>
12.	<b><u>ANNEXURE-P-7</u></b> Copy of Draft Information Technology [Intermediaries Guidelines (Amendment)] Rules, 2018.	<b>100 – 103</b>
13.	<b><u>ANNEXURE-P-8:</u></b> Copy of the public comments received from COAI as published by the Respondent as MIT/79/077.	<b>104 – 113</b>
14.	<b><u>ANNEXURE-P-9:</u></b> Copy of the public comments received from SFLC as published by the Respondent as MIT/79/063.	<b>114 – 136</b>
15.	<b><u>ANNEXURE-P-10:</u></b> Copy of the public comments received from Article 19 Free Word Centre as published by the Respondent as MIT/79/050.	<b>137 – 140</b>
16.	<b><u>ANNEXURE-P-11:</u></b> Copy of the public comments received from Centre for Communication Governance at National Law University Delhi as published by the Respondent as MIT/79/084.	<b>141 – 159</b>

17.	<b><u>ANNEXURE-P-12:</u></b> Copy of the public comments published by the Respondent as MIT/79/087.	<b>160 – 163</b>
18.	<b><u>ANNEXURE-P-13:</u></b> Copy of the public comments received from Mozilla as published by the Respondent as MIT/79/071.	<b>164 – 170</b>
19.	<b><u>ANNEXURE-P-14:</u></b> Copy of the press release dated February 25, 2021 issued by Respondent with respect to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.	<b>171 – 178</b>
20.	<b><u>ANNEXURE-P-15:</u></b> Copy of the Gazette Notification dated February 26, 2021 notifying the threshold of 50 lakh active users for Significant Social Media Intermediaries.	<b>179</b>
21.	<b><u>ANNEXURE-P-16:</u></b> Copy the letter submitted by Professor David Kaye (United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression).	<b>180 – 186</b>
22.	<b><u>C.M. NO. OF 2021</u></b> Application for interim relief along with Affidavit.	<b>187 – 196</b>
23.	<b><u>C.M. NO. OF 2021</u></b> Application under Section 151 Code of Civil Procedure, 1908 praying for exemption from filing legible copies of dim annexures, proper left hand margin, and font size of annexures along with affidavit.	<b>197 – 204</b>

24.	<b><u>C.M. NO. OF 2021</u></b> Application under Section 151 Code of Civil Procedure, 1908 praying for exemption from filing apostilled versions of the pleadings and affidavits.	<b>205 – 212</b>
25.	Vakalatnama along with Power of Attorney.	<b>213 - 219</b>
26.	Proof of service	<b>220</b>

FILED THROUGH:



**TEJAS KARIA (G-1390/2000)**  
**PAVIT SINGH KATOCH (KAR/1712/2007)**  
**FOR SHARDUL AMARCHAND MANGALDAS & CO.**  
**ADVOCATES FOR THE PETITIONER**  
**216, AMARCHAND TOWERS,**  
**OKHLA INDUSTRIAL AREA, PHASE-III,**  
**NEW DELHI-110020**  
**EMAIL: TEJAS.KARIA@AMSSHARDUL.COM**  
**PHONE: 9871790539**

**DATE: MAY 25, 2021**  
**PLACE: NEW DELHI**



**COURT FEES**

**IN THE HIGH COURT OF DELHI AT NEW DELHI**  
**(EXTRA ORDINARY CIVIL WRIT JURISDICTION)**

**W.P. (C) NO. \_\_\_\_\_ OF 2021**

**IN THE MATTER OF:**

**WHATSAPP LLC**

**...PETITIONER**

**VERSUS**

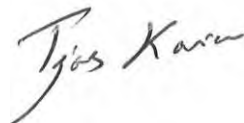
**UNION OF INDIA**

**...RESPONDENT**

**NOTICE OF MOTION**

Take notice that the accompanying Writ Petition is likely to be listed before the Hon'ble Court on \_\_\_\_\_ or on such other day thereafter, as may be fixed by the Hon'ble Court. Please take notice accordingly.

**FILED THROUGH:**



**TEJAS KARIA (G-1390/2000)**  
**PAVIT SINGH KATOCH (KAR/1712/2007)**  
**FOR SHARDUL AMARCHAND MANGALDAS & CO.**  
**ADVOCATES FOR THE PETITIONER**  
**216, AMARCHAND TOWERS**  
**OKHLA INDUSTRIAL AREA, PHASE-III**  
**NEW DELHI-110020**  
**EMAIL: TEJAS.KARIA@AMSSHARDUL.COM**  
**PHONE: 9871790539**

**DATE: MAY 25, 2021**

**PLACE: NEW DELHI**

**IN THE HIGH COURT OF DELHI AT NEW DELHI**  
**(EXTRA ORDINARY CIVIL WRIT JURISDICTION)**

**W.P. (C) NO. \_\_\_\_\_ OF 2021**

IN THE MATTER OF:

WHATSAPP LLC

...PETITIONER

VERSUS

UNION OF INDIA

...RESPONDENT

**MEMO OF PARTIES**

IN THE MATTER OF:

WhatsApp LLC

1601 Willow Road

Menlo Park, California 94025

USA

Email: pavit.katoch@amsshardul.com

... Petitioner

VERSUS

Union of India

Through the Secretary

Ministry of Electronics and IT

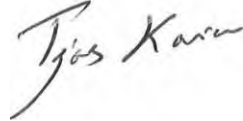
Electronics Niketan, 6, CGO Complex,

Lodhi Road, New Delhi 110 003

Email: webmaster@meity.gov.in

... Respondent

**FILED THROUGH:**



**TEJAS KARIA (G-1390/2000)**  
**PAVIT SINGH KATOCH (KAR/1712/2007)**  
**FOR SHARDUL AMARCHAND MANGALDAS & CO.**  
**ADVOCATES FOR THE PETITIONER**  
**216, AMARCHAND TOWERS**  
**OKHLA INDUSTRIAL AREA, PHASE-III**  
**NEW DELHI-110020**  
**EMAIL: TEJAS.KARIA@AMSSHARDUL.COM**  
**PHONE: 9871790539**

**DATE: MAY 25, 2021**  
**PLACE: NEW DELHI**

## SYNOPSIS

Petitioner WhatsApp LLC (“**Petitioner**”) files this Writ Petition challenging the requirement in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**Intermediary Rules**”) that intermediaries like Petitioner enable “*the identification of the first originator of the information*” in India on their end-to-end encrypted messaging services (commonly referred to as “**traceability**”), upon government or court order. Petitioner respectfully submits that this requirement forces Petitioner to break end-to-end encryption on its messaging service, as well as the privacy principles underlying it, and infringes upon the fundamental rights to privacy and free speech of the hundreds of millions of citizens using WhatsApp to communicate privately and securely.

Since its founding, Petitioner has been committed to providing a private and secure space where users can freely communicate without fear of third parties reading or listening to their most private thoughts. Consistent with that commitment, Petitioner has spent years building and implementing a state-of-the-art end-to-end encrypted messaging service that allows people to communicate privately and securely. End-to-end encryption ensures that every communication sent on WhatsApp, both messages and calls, can only be decrypted by the recipient. No one else, not even Petitioner, can read or listen to encrypted communications or determine their contents.

WhatsApp thus enables government officials, law enforcement, journalists, members of ethnic or religious groups, scholars,

teachers, students, and the like to exercise their right to freedom of speech and expression without fear of retaliation. WhatsApp also allows doctors and patients to discuss confidential health information with total privacy, enables clients to confide in their lawyers with the assurance that their communications are protected, and allows financial and government institutions to trust that they can communicate securely without anyone listening to their conversations.

However, the requirement that intermediaries like Petitioner enable the identification of the first originator of information in India on their platforms puts end-to-end encryption and its benefits at risk. There is no way to predict which message will be the subject of such a tracing order. Therefore, Petitioner would be forced to build the ability to identify the first originator for *every* message sent in India on its platform upon request by the government *forever*. This breaks end-to-end encryption and the privacy principles underlying it, and impermissibly infringes upon users' fundamental rights to privacy and freedom of speech.

Indeed, several commentators echoed the dangers of enabling the identification of the first originator of information when the requirement was proposed in 2018, emphasizing that it would break end-to-end encryption:

- *“Introducing a traceability requirement for end-to-end encrypted services will lead to **breaking of such encryption** and thus compromising the privacy of individuals making use of such services for their private communication.”* (Software

Freedom Law Center, India (SFLC) (MIT/79/063) (emphasis added))

- “Where speakers in the offline context were assured a limited degree of secrecy and obscurity in their communications, **the proposed measure [to enable the identification of the first originator of information] renders encrypted and therefore secret communication impossible.**” (Centre for Communication Governance at National Law University Delhi (MIT/79/084) (emphasis added))
- “To be clear, **traceability is incompatible with end-to-end encryption.** Encryption as a service is used by journalists and whistleblowers to legitimately protect their privacy and in that is an enabler of the right to privacy and the freedom of expression. Apart from protecting privacy, encryption also makes communications more secure and helps ensure integrity of information.” (MIT/79/087 (emphasis added))
- “This [tracing] obligation also **undermines the use of encryption technology**, which ensures that content is not accessible to the intermediary or third parties.” (COAI (MIT/79/077) (emphasis added).)

Requiring intermediaries like Petitioner to enable the identification of the first originator of information in India on their platforms thus undermines the privacy and security provided by end-to-end encryption. For example, (i) journalists could be at risk of retaliation for investigating issues that may be unpopular; (ii) civil or political activists could be at risk of retaliation for discussing certain rights and criticizing or advocating for

politicians or policies; and (iii) clients and attorneys could become reluctant to share confidential information for fear that the privacy and security of their communications are no longer ensured.

Petitioner is thus constrained to file this Writ Petition challenging Rule 4(2) of the Intermediary Rules (“**Impugned Rule 4(2)**”) for at least the following reasons:

***First***, Impugned Rule 4(2) infringes upon the fundamental right to privacy without satisfying the three-part test set forth by the Hon’ble Supreme Court: (i) legality; (ii) necessity; and (iii) proportionality. (See *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (“*Puttaswamy I*”).)

- Legality. To satisfy the legality requirement, there must be a valid law allowing for the invasion of privacy. However, there is no statute requiring intermediaries to enable the identification of the first originator of information in India on end-to-end encrypted messaging services upon government or court order. Nor is there any statute that allows the imposition of such a requirement through subordinate legislation like the Intermediary Rules.
- Necessity. To satisfy the necessity requirement, there must be a “*guarantee against arbitrary State action*”. (*Puttaswamy I*.) Notably, the Hon’ble Supreme Court has emphasized the importance of *judicial review before* the invasion of privacy occurs to guarantee against arbitrary State action. (*Puttaswamy I*; see also *K.S. Puttaswamy v. UOI*, (2019) 1 SCC 1 (“*Puttaswamy II*”).) The Impugned Rule, however, allows tracing orders to be issued with *no judicial review*.



- Proportionality. To satisfy the proportionality requirement, the infringement of fundamental rights must “*be through the least restrictive alternatives*”. (*Kerala State Beverages (M&M) Corp. Ltd. v. P.P. Suresh*, (2019) 9 SCC 710, at para 30.) However, enabling the identification of the first originator of information in India is not the least restrictive alternative. Since there is no way to predict which message will be the subject of a tracing order, intermediaries like Petitioner would have to build the ability to identify the first originator of *every* communication sent in India on their platforms for all time, infringing upon the privacy of even *lawful* users. Enabling the identification of the first originator of information in India breaks end-to-end encryption and the privacy principles underlying it.

**Second**, Impugned Rule 4(2) violates the fundamental right to freedom of speech and expression, as it chills even lawful speech. Citizens will not speak freely for fear that their private communications will be traced and used against them, which is antithetical to the very purpose of end-to-end encryption.

**Third**, Impugned Rule 4(2)’s requirement to enable the identification of the first originator of information in India is *ultra vires* its parent statutory provision, Section 79 of the Information Technology Act, 2000 (“**IT Act**”), and the intent of the IT Act itself for the following reasons:

- To require intermediaries like Petitioner to enable the identification of the first originator of information in India on their end-to-end encrypted messaging services, there must be

a clear policy declaration in Section 79 that Parliament intended to impose such a requirement. However, no such declaration exists in Section 79. Nothing in Section 79 suggests that Parliament intended to impose such a requirement, and certainly not at the expense of changing the fundamental nature of intermediaries' platforms. Respondent may not seek to fulfil an essential legislative function by declaring such a policy through the Intermediary Rules.

- Section 79 only allows the Central Government to prescribe the “*due diligence*” that intermediaries must observe to maintain their immunity. Compelling an intermediary to fundamentally alter its platform to enable the ability to identify the first originator of information in India falls far outside “*due diligence*”.
- The preamble of the IT Act provides that the intent of the statute is to achieve “*uniformity of the law*” with other countries. Petitioner is not aware of any country that requires intermediaries to enable the identification of the first originator of information on end-to-end encrypted messaging services, even if it means fundamentally changing their platforms to do so.

For all these reasons, and others set forth below, Petitioner respectfully requests that this Hon’ble Court may be pleased to declare that (i) Impugned Rule 4(2) is unconstitutional, *ultra vires* the IT Act, and illegal; and (ii) no criminal liability may be imposed for any alleged non-compliance with Impugned Rule 4(2).

**LIST OF DATES**

Date	Event
<b>17 October 2000</b>	The Information Technology Act, 2000 (“ <b>IT Act</b> ”) was notified.
<b>2009</b>	Petitioner was incorporated under the laws of the State of California in the United States of America, and started offering “ <i>WhatsApp</i> ”, a free, simple, secure, and reliable internet-based end-to-end encrypted messaging service.
<b>5 February 2009</b>	The Information Technology (Amendment) Act, 2008 (“ <b>Amendment</b> ”), amending the IT Act, became effective. The Amendment amended Section 79 of the IT Act by, <i>inter alia</i> , providing intermediaries with an exemption from liability for third-party information on their platforms, subject to certain conditions.
<b>27 October 2009</b>	Respondent published the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 in the Official Gazette.
<b>11 April 2011</b>	Respondent published the Information Technology (Intermediaries Guidelines) Rules, 2011 in the Official Gazette.

<b>1 June 2011</b>	<p>The Joint Declaration on Freedom of Expression and the Internet, signed by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACPHR) Special Rapporteur on Freedom of Expression and Access to Information was signed.</p> <p>This is available at <a href="https://www.osce.org/fom/78309?download=true">https://www.osce.org/fom/78309?download=true</a></p>
<b>April 2016 to July 2016</b>	<p>Petitioner published “<i>FAQs Regarding End to End Encryption</i>”, available at <a href="https://faq.whatsapp.com/en/28030015/">https://faq.whatsapp.com/en/28030015/</a></p>
<b>24 December 2018</b>	<p>Respondent published the Draft Information Technology (Intermediaries Guidelines (Amendment)) Rules, 2018 (“<b>Proposed Amendments</b>”). Respondent also commenced a consultative process by inviting comments and counter-comments to the Proposed Amendments.</p>

<b>24 December 2018 to 14 February 2019</b>	<p>Respondent received several comments and counter-comments from a variety of stakeholders, many of whom were critical of requiring intermediaries to trace originator information. Professor David Kaye, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, submitted a letter which highlighted concerns regarding the Proposed Amendments, including the dangers of imposing a requirement to enable the identification of the first originator of information.</p>
<b>22 October 2020</b>	<p>Petitioner published an updated version of its Technical White Paper, (originally published on 5 April 2016 and then updated on 19 December 2017) which is available at <a href="https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&amp;_nc_sid=2fbf2a&amp;_nc_ohc=jzWIa3g6xI0AX9iW43o&amp;_nc_ht=scontent.whatsapp.net&amp;oh=a990a493adf25bb1a08ad4f7d6c7aa0e&amp;oe=60CD0719">https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&amp;_nc_sid=2fbf2a&amp;_nc_ohc=jzWIa3g6xI0AX9iW43o&amp;_nc_ht=scontent.whatsapp.net&amp;oh=a990a493adf25bb1a08ad4f7d6c7aa0e&amp;oe=60CD0719</a> .</p>
<b>25 February 2021</b>	<p>Respondent held a press conference to announce that it had framed the Information</p>

	Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to regulate, amongst others, social media intermediaries. Respondent specifically identified Petitioner as such a social media intermediary.
<b>25 February 2021</b>	Respondent published the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in the Official Gazette.
<b>26 February 2021</b>	Respondent notified the threshold for “ <i>significant social media intermediaries</i> ” as social media companies with at least 5 million registered users in India.
<b>25 May 2021</b>	Hence, the present Writ Petition.

**IN THE HON'BLE HIGH COURT OF DELHI  
(EXTRAORDINARY WRIT JURISDICTION)  
WRIT PETITION (CIVIL) NO. \_\_\_\_ OF 2021**

**IN THE MATTER OF:**

**WHATSAPP LLC (Formerly known as WhatsApp Inc.)**

**1601 WILLOW ROAD**

**MENLO PARK**

**CALIFORNIA, USA 94025**

**... PETITIONER**

**VERSUS**

**UNION OF INDIA**

**THROUGH ITS SECRETARY**

**MINISTRY OF ELECTRONICS**

**& INFORMATION TECHNOLOGY**

**NEW DELHI**

**... RESPONDENT**

**MEMORANDUM OF WRIT PETITION ON BEHALF OF  
PETITIONER UNDER ARTICLE 226 OF THE  
CONSTITUTION OF INDIA, 1950**

**TO**

**THE HON'BLE CHIEF JUSTICE AND THE HON'BLE  
COMPANION JUDGES OF THE HON'BLE HIGH  
COURT OF DELHI:**

**THE HUMBLE PETITION ON BEHALF OF  
PETITIONER ABOVE NAMED:**

**MOST RESPECTFULLY SHOWETH:**

1. Petitioner is constrained to approach this Hon'ble Court to challenge the validity of Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Impugned Rule 4(2)**") on the grounds that it (i) violates the fundamental rights to privacy and freedom of speech and expression guaranteed under Articles 19 and 21 of the Constitution of India of more than 400 million WhatsApp users in India; (ii) is *ultra vires* the Information Technology Act, 2000 ("**IT Act**"), the parent statute under which Impugned Rule 4(2) was prescribed; and (iii) violates Article 14 of the Constitution of India. A copy of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Rules**") is annexed herewith as **Annexure P-1**.
2. Petitioner is a company incorporated under the laws of the State of Delaware, United States of America, and is located at 1601 Willow Road, Menlo Park, California 94025, in the United States of America.
3. Respondent is the Union of India through its Secretary, Ministry of Electronics and Information Technology. Respondent is responsible for matters relating to cyber laws and the administration of the IT Act and other information technology related laws, and has issued the Intermediary Rules. Respondent is the "State" within the meaning of Article 12 of the Constitution of India.



4. Petitioner has not filed any other petition regarding the subject matter of the present Writ Petition in either this Hon'ble Court or any other Court in India.
5. Petitioner has no alternative remedy, much less an equally efficacious remedy, with respect to the subject matter of the present Writ Petition. Further, adjudication by this Hon'ble Court in exercise of its extraordinary powers under Article 226 of the Constitution of India is warranted because, *inter alia*, Impugned Rule 4(2) (i) violates the fundamental rights to privacy and freedom of speech and expression; (ii) is *ultra vires* the parent statute under which it was prescribed; and (iii) violates Article 14 of the Constitution, thereby raising substantial questions of law and public importance.

**I. BACKGROUND ON PETITIONER AND ITS COMMITMENT TO PRIVACY AND SECURITY**

6. Petitioner was founded in 2009 and has built its service on a foundation of user privacy and security. Indeed, Petitioner is dedicated to creating a private and secure space where users can freely communicate. As Petitioner states on its website, “[r]espect for your privacy is coded into our DNA. Since we started WhatsApp, we’ve built our Services with a set of **strong privacy principles** in mind.” (Emphasis added.) A copy of the Key Updates to the Petitioner’s 2021 Update to its Terms and Privacy Policy from the Petitioner’s website is annexed herewith as **Annexure P-2** to this Petition.

7. Consistent with these principles of privacy and security, Petitioner offers users throughout the world, including over 400 million users in India, a state-of-the-art end-to-end encrypted messaging and calling service, WhatsApp. Petitioner's end-to-end encryption is used when a user messages another person using WhatsApp. End-to-end encryption ensures only a user and the person they are communicating with can read or listen to what is sent, and nobody in between, not even Petitioner. This is because with end-to-end encryption, users' messages are secured with a lock, and only the recipient and the sender have the special key needed to unlock and read them. All of this happens automatically: there is no need to turn on settings or set up special secret chats to secure users' messages.
8. Petitioner explains its end-to-end encryption and the privacy it provides in its *FAQs Regarding End to End Encryption*. As stated there:

*“WhatsApp end-to-end encryption **ensures only you and the person you’re communicating with can read what’s sent, and nobody in between, not even WhatsApp**. Your messages are secured with locks, and only the recipient and you have the special keys needed to unlock and read your messages. . .*

*WhatsApp has no ability to see the content of messages or listen to calls on WhatsApp. That’s because the **encryption and decryption occurs***

*entirely on your device. Before a message ever leaves your device, it's secured with a cryptographic lock, and **only the recipient has the keys.***" (Emphasis added.)

A copy of the FAQ on end-to-end encryption is enclosed herewith as **Annexure P-3** to this Petition.

9. A more detailed explanation of how Petitioner's end-to-end encryption system works is provided in its Technical White Paper, where it states:

*"The Signal Protocol, designed by Open Whisper Systems, is the basis for WhatsApp's end-to-end encryption. This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls....*

*WhatsApp defines end-to-end encryption as communications that remain encrypted from a device controlled by the sender to one controlled by the recipient, **where no third parties, not even WhatsApp or our parent company Facebook, can access the content in between.** A third party in this context means any organization that is not the sender or recipient user directly participating in the conversation.*" (Emphasis added.)

A copy of WhatsApp Encryption Overview, Technical White Paper, updated October 22, 2020, is annexed herewith as **Annexure P-4** to this Petition.

10. Notably, the way many people use WhatsApp is by nature, private. Approximately 90% of the messages sent on WhatsApp are from *one person to another*, and the *majority of groups have fewer than ten people*. Indeed, people increasingly use WhatsApp to chat with their loved ones, conduct business, or talk confidentially with a doctor.
11. In addition to protecting the privacy and security of user communications, Petitioner has also undertaken a number of measures to protect the privacy of users and help users stay safe. For example:
  - a. On July 10, 2018, Petitioner added a label that highlights when a user receives a message that has been forwarded to them. Petitioner subsequently added a double arrow icon to identify highly forwarded messages such as a chain message (the number of times a message has been forwarded is end-to-end encrypted). These indicators help people know when a message they have received was not created by the person who sent it — and Petitioner encourages users to think before sharing messages that are forwarded.
  - b. Petitioner limited the ability of users to forward messages to just five chats at once. This limitation

was initially imposed in India only on July 19, 2018 to curb the virality of unlawful content. About six months later on January 21, 2019, Petitioner implemented the limitation for all users across the world on the latest versions of WhatsApp. In addition, Petitioner launched an extensive advertising campaign in over 11 Indian languages across multiple formats (including print, online, and radio) to help people understand the importance of this new forward label and to ask people to think before sharing messages. This change has resulted in a 25% reduction in forwarding behaviour globally, approximately 1 billion forwards per day, making Petitioner one of the few technology companies to intentionally constrain sharing.

- c. Petitioner provides its users with controls that they can use as they see fit to help protect themselves. This includes the ability to control who a user communicates with by giving users the ability to block users they do not want to communicate with, including unknown contacts. Users also have control over who sees their last seen, profile photo, and/or status information. Petitioner also provides a privacy setting to give users control over who can add them to a group. This is a significant measure that was requested by users, policy makers, and privacy advocates to help prevent phone numbers from being exposed to unwanted groups.

- d. As explained above, to protect the privacy and security of its users, Petitioner provides end-to-end encryption by default, which means only the sender and recipient can decrypt and see the content of messages. However, Petitioner relies on available unencrypted information including user reports, profile photos, and group photos, group subject, and descriptions to detect and prevent abuse such as child sexual abuse material. Should Petitioner's systems detect such an image on its unencrypted surfaces, Petitioner removes the image, provides it along with associated account details to the National Center for Missing and Exploited Children ("NCMEC"), and bans the user as well as associated accounts within a group. NCMEC, in turn, provides India's National Crime Records Bureau with immediate access to India-specific reports through a secure Virtual Private Network (VPN) connection. Petitioner also provides a monthly report to India's National Crime Records Bureau with the NCMEC report IDs that Petitioner referred to NCMEC pertaining to Indian users.
- e. When Petitioner is made aware of conduct that violates its Terms of Service, Petitioner investigates and takes appropriate action, which may include banning user accounts. Indeed, Petitioner bans about 2 million WhatsApp accounts per month globally for violations of its Terms of Service.

- f. Petitioner cooperates with law enforcement authorities in India and continues to take steps to assist in their efforts to keep people safe. For example:
  - i. Petitioner has a dedicated team of individuals who review, validate, and respond to law enforcement requests for user data in India.
  - ii. Petitioner provides law enforcement agencies with dedicated communication channels for the submission, tracking and processing of requests (available at <https://www.whatsapp.com/records/login>).
  - iii. Petitioner provides well-documented operational guidelines for law enforcement officials seeking information from Petitioner (available at <https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities>). A copy of the FAQ on Information for Law Enforcement Authorities is annexed herewith as **Annexure P-5** to this Petition.
  - iv. Petitioner has trained law enforcement officers from various States across India on how to request information from Petitioner during their investigations, consistent with published

information for law enforcement agencies on Petitioner's website.

- v. Petitioner has also separately reached out to over 150 local and state law enforcement offices in India to share these best practices for obtaining information from Petitioner during their investigations.

## II. THE 2011 GUIDELINES AND INTERMEDIARY RULES

12. In 2011, the Central Government notified the Information Technology (Intermediaries Guidelines) 2011 (“**2011 Guidelines**”), which set forth the “[d]ue diligence to be observed by intermediary”. (Rule 3, 2011 Guidelines.) The 2011 Guidelines were prescribed under Section 79, which provide intermediaries with a safe harbour immunity for third-party content on their platforms. A copy of the Official Gazette Notification notifying the 2011 Guidelines is annexed herewith as **Annexure P-6** to this Petition.
13. On December 24, 2018, Respondent released a draft of proposed amendments to the 2011 Guidelines. A copy of the Draft Information Technology (Intermediaries Guidelines) (Amendment) Rules, 2018 is annexed herewith as **Annexure P-7** to this Petition.
14. Respondent commenced a consultation process on the proposed amendments by inviting comments and counter-comments from the public. Several civil society, human



rights, and business entities raised various constitutional, legal, and feasibility concerns with the proposed amendments, including on the proposed requirement that intermediaries enable the identification of the first originator of information on their platforms. These comments emphasized that such a requirement would force intermediaries to break end-to-end encryption and compromise the security and safety of India and its citizens.

- a. *“This [tracing] obligation also **undermines the use of encryption technology**, which ensures that content is not accessible to the intermediary or third parties. Thus, placing the obligation of tracing on an intermediary creates a restrictive regime which **seeks to dictate the underlying technology governing the intermediary’s business**, in addition to incentivising the development of technology that undermines globally recognised best practice for preserving the privacy and security of communications, in particular the deployment of robust encryption tools.”* (COAI (emphasis added).) A copy of the public comments received from COAI as published by the Respondent as MIT/79/077 is annexed herewith as **Annexure P-8** to this Petition.
- b. *“Introducing a traceability requirement for end-to-end encrypted services will lead to **breaking of such encryption** and thus compromising the privacy of individuals making use of such services for their private communication.”* (SFLC (emphasis added).) A

copy of the public comments received from SFLC as published by the Respondent as MIT/79/063 is annexed herewith as **Annexure P-9** to this Petition.

- c. *“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. . . . All of these implicit requirements translate to a significant dilution of privacy, freedom of expression and security of users online. . . .”* (ARTICLE 19 Free Word Centre (emphasis added).) A copy of the public comments received from Article 19 Free Word Centre as published by the Respondent as MIT/79/050 is annexed herewith as **Annexure P-10** to this Petition.

- d. *“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.** . . . 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.”* (Centre for Communication Governance at National Law University Delhi (emphasis added).) A copy of the public comments received from Centre for Communication Governance at National Law University Delhi as published by the Respondent as MIT/79/084 is annexed herewith as **Annexure P-11** to this Petition.

- e. *“To be clear, **traceability is incompatible with end-to-end encryption.** Encryption as a service is used by journalists and whistleblowers to legitimately protect their privacy and in that is an enabler of the right to privacy and the freedom of expression. Apart from protecting privacy, encryption also makes communications more secure and helps ensure integrity of information. Moreover, in many cases traceability that requires service providers to roll back or reduce the strength of encryption over their services is also likely to be ineffective. For example, content that poses a threat to public order and national security (such as fake news) can be created on*

*platforms and on forums that are not subject to Indian law and then released on to popularly used platforms where they can go viral. In situations such as these, tracing the pathway through which the content was shared by well-meaning users is unlikely to result in the apprehension of the true authors of such content.”* (emphasis added). A copy of the public comments as published by the Respondent as MIT/79/087 is annexed herewith as **Annexure P-12** to this Petition.

- f. *“For users, the guarantees of both end-to-end encryption with minimal collection of metadata is an assurance of privacy and security in the products. **Compelling companies to modify their infrastructure based on government requests undermines this trust and denies them the ability to provide secure products and services to their customers**”* (Mozilla (emphasis added).) A copy of the public comments received from Mozilla and published by the Respondent as MIT/79/071 is annexed herewith as **Annexure P-13** to this Petition.

15. Two years later, on February 25, 2021, Respondent notified the Intermediary Rules, which were issued pursuant to Sections 79(2)(c) and 69A of the IT Act. The Intermediary Rules include a requirement that certain “*significant social media intermediaries*” (“**SSMIs**”) — *i.e.*, social media intermediaries with more than 50 lakh registered users in India — “*shall enable the identification of the first originator of the information*” in India on their messaging

services upon court order or an order under Section 69 of the IT Act. A copy of the press release dated February 25, 2021, issued by Respondent with respect to the Intermediary Rules, is enclosed herewith as **Annexure P-14** to this Petition. A copy of the Gazette Notification dated February 26, 2021 notifying the threshold of 50 lakh active users for SSIMs is enclosed herewith as **Annexure P-15** to this Petition.

16. Impugned Rule 4(2) provides in full:

*“A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the competent authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form:*

*Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of*

*incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:*

*Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:*

*Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users:*

*Provided also that where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for the purpose of this clause.*

17. Aggrieved by Impugned Rule 4(2), Petitioner files this Writ Petition for violation of its rights under Articles 14 and 21 of the Constitution, and the rights of its more than 400

million WhatsApp users in India. These users have the same interest in this Writ Petition since Impugned Rule 4(2) also violates their rights under Articles 14, 19 and 21 of the Constitution, including the fundamental rights to privacy and freedom of speech and expression.

**III. IMPUGNED RULE 4(2) OF THE INTERMEDIARY RULES SHOULD BE DECLARED UNCONSTITUTIONAL OR OTHERWISE INVALIDATED**

18. Indian law is well-settled that subordinate legislation like the Intermediary Rules may be challenged and invalidated on any of the following grounds:

*“(a) Lack of legislative competence to make the subordinate legislation.*

*(b) Violation of fundamental rights guaranteed under the Constitution of India.*

*(c) Violation of any provision of the Constitution of India.*

*(d) Failure to conform to the statute under which it is made or exceeding the limits of authority conferred by the enabling Act.*

*(e) Repugnancy to the laws of the land, that is, any enactment.*

*(f) Manifest arbitrariness/unreasonableness (to an extent where the court might well say that the legislature never intended to give authority to make such rules).”*

(See *State of TN v. P. Krishnamurthy*, (2006) 4 SCC 517, at paras 15-16; *Cellular Operators Assn of India v. TRAI*, (2016) 7 SCC 703, at para 34.)

19. For reasons set forth below, Petitioner respectfully submits that Impugned Rule 4(2) should be invalidated on one or more of the above grounds.

## **GROUND**

### **Impugned Rule 4(2) Should Be Struck Down As Unconstitutional and *Ultra Vires* the IT Act**

20. Under Impugned Rule 4(2), SSIMs providing services primarily in the nature of messaging must enable the identification of the first originators of information in India on their platforms when required by an order under Section 69 of the IT Act or a court order.
21. Petitioner respectfully submits that Impugned Rule 4(2) should be struck down on the grounds that it (i) violates the fundamental right to privacy guaranteed under Article 21 of the Constitution; (ii) violates the fundamental right to freedom of speech and expression guaranteed under Article 19 of the Constitution; (iii) is *ultra vires* the parent statutory provisions, Sections 69A and 79 of the IT Act, as well as the



intent of the IT Act itself; (iv) is “*manifestly arbitrary*” in violation of Article 14 of the Constitution; and (v) violates the principle of data minimisation.

**i. Impugned Rule 4(2) violates the fundamental right to privacy**

22. In the landmark decision of *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (“*Puttaswamy I*”), the Hon’ble Supreme Court held that the right to privacy is a fundamental right guaranteed under Article 21 of the Constitution. (*Puttaswamy I*, at paras 375, 644.) In reaching its decision, the Hon’ble Supreme Court identified nine types of privacy, including:
  - a. “*communicational privacy which is reflected in enabling an individual to restrict access to communications or control the use of information which is communicated to third parties*”;
  - b. “*informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information*”; and
  - c. “*associational privacy which is reflected in the ability of the individual to choose who she wishes to interact with*”. (*Puttaswamy I*, at para 250 (emphasis added).)
23. More recently, the Hon’ble Supreme Court affirmed that the right to privacy includes the right to anonymity. (See

*Central Public Information Officer, Supreme Court v. Subhash Chandra Agrawal*, (2020) 5 SCC 481, at para 54 (“Privacy and confidentiality encompass a bundle of rights including the right to protect identity and anonymity.”).)

24. Requiring intermediaries “to enable the identification of the first originator of the information” in India on end-to-end encrypted messaging services constitutes a dangerous invasion of privacy. This would require Petitioner to build the ability to identify the first originator of *every* communication sent in India on its platform, as there is no way to predict which message will be the subject of such an order seeking first originator information. This eliminates the right of the hundreds of millions Indian citizens using WhatsApp to maintain the privacy of their messages, which is antithetical to end-to-end encryption and the core privacy principles underlying it.
25. Under the test announced in *Puttaswamy I*, to justify an intrusion into the fundamental right of privacy, the following three requirements must be satisfied: “(i) *legality, which postulates the existence of law*; (ii) *need, defined in terms of a legitimate State aim*; and (iii) *proportionality, which ensures a rational nexus between the objects and the means adopted to achieve them*.” (See *Puttaswamy I*, at para 325.) Here, none of these requirements — much less all three — are met by Impugned Rule 4(2).

### 1. Impugned Rule 4(2) does not satisfy the valid law requirement

26. There is no law enacted by Parliament that expressly requires an intermediary to enable the identification of the first originator of information in India on its end-to-end encrypted platform or otherwise authorizes the imposition of such a requirement through rule-making. While Impugned Rule 4(2) seeks to impose such a requirement, the Impugned Rule is not a valid law as it is subordinate legislation, passed by a Ministry and not Parliament, that is *ultra vires* its parent statute, Section 79. (See *Indian Young Lawyers Assn. v. State of Kerala*, (2019) 11 SCC 1, at paras 137-140; *Union of India v. S. Srinivasan*, (2012) 7 SCC 683, at para 21; *General Officer Commanding-in-Chief v. Subhash Chandra Yadav*, (1988) 2 SCC 351, at para 14.) Indeed, nothing in Section 79 contemplates empowering Respondent to impose an obligation that requires intermediaries to enable the identification of the first originator of information, even at the expense of breaking end-to-end encryption. (See *infra* at Paragraphs 52-57.)

### 2. Impugned Rule 4(2) does not satisfy the necessity requirement

27. In describing the “*necessity*” requirement, the Hon’ble Supreme Court observed that the law must “*guarantee against arbitrary State action*”, and highlighted the importance of *judicial review* to ensure the absence of arbitrariness:

*“Second, the requirement of a need, in terms of a legitimate State aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, **which is a guarantee against arbitrary State action.** The pursuit of a legitimate State aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. **Judicial review** does not reappreciate or second guess the value judgment of the legislature but **is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness.**” (Puttaswamy I, at para 310 (emphasis added).)*

28. More recently, in *K.S. Puttaswamy v. UOI*, (2019) 1 SCC 1 (*“Puttaswamy II”*), the Hon’ble Supreme Court highlighted the importance of judicial review *before* there is an invasion of privacy by the Government. In that case, the statutory provision at issue allowed the Government to issue directions requiring the disclosure of personal information in the interest of national security. The Hon’ble Supreme Court held the statutory provision unconstitutional as it did not provide adequate safeguards to protect the fundamental right to privacy. In reaching its decision, the Hon’ble Supreme Court emphasized that it was critical that the

Government obtain **prior approval** from a **judicial officer** to curb any potential misuse of authority:

*“Insofar as Section 33(2) is concerned, it is held that disclosure of information in the interest of national security cannot be faulted with. However, for determination of such an eventuality, an officer higher than the rank of a Joint Secretary should be given such a power. Further, in order to avoid any possible misuse, a Judicial Officer (preferably a sitting High Court Judge) should also be associated with. We may point out that such provisions of application of **judicial mind** for arriving at the conclusion that disclosure of information is in the interest of national security, are prevalent in some jurisdictions.” (Puttaswamy II, at para 513.6 (emphasis added).)*

29. Notably, even Section 93 of the Criminal Procedure Code requires judicial approval before the Government is allowed to execute a search-warrant for a physical search. As an 8-judge bench of the Hon’ble Supreme Court held — before privacy was even recognized as a fundamental right — the *“issue of a search warrant is **normally the judicial function of the Magistrate.**” (MP Sharma v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300 (emphasis added).)* There is no reason that a search of private, encrypted conversations should escape the same judicial scrutiny required to protect fundamental rights.

30. Here, as in *Puttaswamy II*, Impugned Rule 4(2) allows for the issuance of orders to identify the first originator of information in India ***without judicial oversight***, let alone prior judicial oversight, which means there is no “*guarantee against arbitrary State action*”. Impugned Rule 4(2) therefore should be struck down as it is an unconstitutional invasion of the fundamental right to privacy.

### **3. Impugned Rule 4(2) does not satisfy the proportionality requirement**

31. The Hon’ble Supreme Court has held that to be proportional, the infringement of fundamental rights must “*be through the least restrictive alternatives.*” (*Kerala State Beverages (M&M) Corp. Ltd. v. P.P. Suresh*, (2019) 9 SCC 710, at para 30.) Impugned Rule 4(2) is not proportional for at least the following reasons.
32. ***First***, to enable the ability to identify the first originator of information in India, SSIMs would have to build a mechanism that would permit tracing of ***every*** communication sent in India on its messaging service, including those who are using the service lawfully, as there is no way to predict which message will be the subject of such an order seeking first originator information. This is contrary to the Hon’ble Supreme Court’s precedent that surveillance must be targeted and limited only to those “*persons, whether or not previously convicted, whose conduct shows a determination to lead a life of crime*”. (*Gobind v. State of M.P.*, (1975) 2 SCC 148; see also *Malak*

*Singh v. State of P&H*, (1981) 1 SCC 420; *Puttaswamy II*, at para 183.)

33. More recently, in *Indian Hotels & Restaurant Ass’n (AHAR) v. State of Maharashtra*, (2019) 3 SCC 429, the Government argued that it should be allowed to require the installation of CCTV cameras at the entrances of bar rooms and other places of amusement and public entertainment, citing the need to control crime and protect women who are likely to be exploited. Relying on *Puttaswamy I*, the Hon’ble Supreme Court rejected those arguments, concluding that surveillance of public behaviour in a public place constituted an unlawful invasion of privacy.
34. Enabling the identification of the first originator of information in India on end-to-end encrypted platforms like WhatsApp is a much more serious invasion of privacy than requiring businesses to film public behaviour in public areas, as WhatsApp was designed to facilitate the exchange of *private* communications. Further, the invasion is not limited to only certain places (such as a bar room), but rather, extends to *any* communication that takes place in India on WhatsApp and every other SSMI’s end-to-end encrypted messaging service in India. This harm is particularly dangerous and disproportionate as the Impugned Rule does not impose a time limit, forcing Petitioner to be able to identify the first originator of information in India on its platform years after the message was sent.

35. ***Second***, enabling the identification of the first originator of information in India results in significant harm, including breaking end-to-end encryption and chilling lawful speech. Indeed, Professor David Kaye (United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression) submitted a letter (“**Kaye Letter**”) highlighting the dangers of implementing such a measure, observing that “*the ensuing security and privacy risks to large numbers of users may disproportionately chill and hinder their exercise of freedom of expression.*” (**Kaye Letter** at page 4.) A copy of the Kaye Letter is annexed herewith as **Annexure P-15** to this Petition.
36. States throughout the world, including India, have likewise recognized the important benefits of end-to-end encryption and the dangers of undermining that security protocol. For example, end-to-end encryption:
- a. ensures the integrity of the content of communications, whether for private, commercial, or financial purposes, ensuring that it is not tampered with or manipulated while it is being transmitted, preventing serious and common crimes like hacking and identity theft;
  - b. promotes a citizen’s fundamental right to privacy by empowering individuals to read and share opinions and information with others, including their friends and loved ones, without fear of misappropriation or interference;



- c. enables journalists, civil society organizations, members of ethnic or religious groups, activists, scholars, and artists to exercise their right to freedom of speech and expression without fear of surveillance or retaliation;
- d. protects conversations that are deeply personal, allowing a person to discuss extremely sensitive issues such as one's identity, gender, religion, ethnicity, national origin, health, or sexuality;
- e. allows doctors and patients to discuss confidential health information with total privacy, facilitating the doctor-patient privilege;
- f. allows clients to confide in their lawyers, and vice versa, with the assurance that their communications are protected, facilitating the attorney-client privilege;
- g. allows many businesses and financial institutions to share sensitive financial information without the fear of it being misappropriated or manipulated; and
- h. protects communications amongst persons who are part of the State such as the Central Government, law enforcement agencies, and the military, and also enables citizens to report unlawful activity with increased confidence that they will not be subjected to retaliation.

37. Imposing a requirement to enable the identification of the first originator of information in India would undermine all of these benefits. For example, (i) journalists could be at risk of retaliation for investigating issues that may be unpopular; (ii) civil or political activists could be at risk of retaliation for discussing certain rights and criticizing or advocating for politicians or policies; and (iii) clients and attorneys could become reluctant to share confidential information for fear that the privacy and security of their communications is no longer ensured.
38. In short, forcing Petitioner to build the ability to identify the first originator of information in India would infringe upon the privacy of *every* individual who uses WhatsApp in India. Such a result would clearly be disproportionate, particularly in light of the Hon'ble Supreme Court's warning against invading a law-abiding person's privacy in order to investigate another's misconduct, as "*fundamental rights cannot be sacrificed on the anvil of fervid desire to find instantaneous solutions to systemic problems*". (*Ram Jethmalani v. Union of India*, (2011) 8 SCC 1.)
39. Accordingly, Impugned Rule 4(2) should be struck down as an unconstitutional violation of the fundamental right to privacy.

**ii. Impugned Rule 4(2) violates the fundamental right to freedom of speech and expression**

40. The Hon'ble Supreme Court has long recognized that freedom of speech and expression is a fundamental right guaranteed under Article 19(1)(a) of the Constitution. This includes "*freedom not only for the thought that we cherish, but also for the thought that we hate.*" (See *Naraindas Indurkha v. State of M.P.*, (1974) 4 SCC 788, at para 23.) It also includes "*the right to propagate one's views through the print media or through any other communication channel*", and "*any attempt to deny the same must be frowned upon unless it falls within the mischief of Article 19(2) of the Constitution.*" (See *LIC v. Manubhai D. Shah (Prof.)*, (1992) 3 SCC 637, at para 8.)
41. Critical to protecting the right to freedom of speech and expression is protecting the privacy of the speaker. Indeed, privacy is inextricably intertwined with the right to freedom of speech and expression because it protects people from retaliation for expressing unpopular, but lawful, views. It encourages users to express their ideas and opinions, report unlawful activities, and challenge popular views without fear of reprisal, whereas enabling the identification of the first originator of information in India subverts privacy and discourages freedom of expression. Professor Kaye has thus observed that online privacy is essential to protecting the right to free speech because it allows people to "*to hold opinions and exercise freedom of expression without*

*arbitrary and unlawful interference or attacks*". (Kaye Letter at page. 4.)

42. Here, Impugned Rule 4(2)'s requirement to enable the identification of the first originator of information in India unreasonably infringes upon the fundamental right to freedom of speech and expression for at least two reasons.
43. **First**, the Hon'ble Supreme Court has held that a law violates the fundamental right to freedom of speech and expression if it chills lawful speech. (See *Shreya Singhal*, at para 90; *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632, at page 647; *S. Khushboo v. Kanniammal*, (2010) 5 SCC 600, at para 47.)
44. With end-to-end encryption, users feel safe to communicate freely. However, as explained above, enabling the identification of the first originator of information in India on WhatsApp breaks end-to-end encryption and infringes user privacy. As a result, it also significantly restricts the right to freedom of speech and expression online. Once citizens become aware that SSMLs have built the ability to identify the first originator of information in India on their end-to-end encrypted messaging services, individuals will not feel safe to speak freely for fear that their lawful private communications will be used against them, thereby infringing their rights to privacy and free speech.

45. ***Second***, Impugned Rule 4(2) is an unreasonable restriction on the right to free speech for many of the same reasons that it violates the right to privacy. In particular:

- a. There is no express valid law passed by Parliament authorizing this infringement upon the fundamental right to freedom of speech and expression (see *Bishan Das and Others v. State of Punjab* AIR 1961 SC 1570, at para 14 (holding that any infringement on a fundamental right must be backed by law));
- b. The Impugned Rule permits tracing orders to be issued without prior judicial review, and, therefore, fails to provide constitutionally adequate safeguards to guarantee against arbitrary Government action; and
- c. The Impugned Rule is not proportional as the harm it causes outweighs its purported benefits.

46. Accordingly, Impugned Rule 4(2) should be struck down as an unconstitutional violation of the fundamental right to freedom of speech and expression.

**iii. Impugned Rule 4(2) is *ultra vires* Sections 69A and 79 by compelling intermediaries like Petitioner to fundamentally alter their platforms**

47. Indian law is well-settled that subordinate legislation like the Intermediary Rules must not be *ultra vires* the parent statute under which they have been prescribed. (See *Bombay Dyeing and Mfg. v. Bombay Env. Action Grp.*,

(2006) 3 SCC 434, at para 104.) Indeed, the Hon’ble Supreme Court “*has clearly held that a subordinate legislation can be challenged not only on the ground that it is contrary to the provisions of the Act or other statutes; but also if it is violative of the legislative object.*” (*Id.*)

48. Impugned Rule 4(2) is *ultra vires* the Intermediary Rules’ parent statutory provisions, Sections 69A and 79, as well as the intent of the IT Act.

**1. Impugned Rule 4(2) is *ultra vires* Sections 69A and 79**

49. Subordinate legislation is *ultra vires* the parent statute if it travels beyond, or does not conform with, the parent statute. (See *Kunj Behari Lal Butail v. State of H.P.*, (2000) 3 SCC 40 (“*It is a well-recognised principle of interpretation of a statute that conferment of rule-making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent therewith or repugnant thereto.*”).)
50. Here, the scope of Respondent’s authority to prescribe the Intermediary Rules is defined by 69A and 79(2) of the IT Act. Impugned Rule 4(2)’s requirement that SSIMs like Petitioner enable the identification of the first originators of information on end-to-end encrypted messaging services “*travels beyond*”, and is thus *ultra vires*, Sections 69A and 79.

51. **Section 69A.** Section 69A empowers the Central Government to direct an intermediary to block access to content on its platform. Section 69A(2) also empowers the Central Government to prescribe “*procedures and safeguards subject to which such blocking for access by the public may be carried out*”. However, Impugned Rule 4(2) is neither a “*procedure*” nor “*safeguard*” “*subject to which a blocking order may be carried out.*” Indeed, determining the first originator of information in India on end-to-end encrypted platforms has nothing to do with the removal of unlawful content. Accordingly, Impugned Rule 4(2) exceeds the scope of Respondent’s rule-making authority under Section 69A.
52. **Section 79.** Section 79 is a safe harbor immunity provision that protects intermediaries from liability for third-party content on their platforms, and provides that an intermediary must observe “*due diligence*” prescribed by the Central Government to enjoy that immunity. As explained immediately below, Section 79 does ***not*** enable Respondent to impose a requirement that intermediaries enable the identification of the first originator of information in India on end-to-end encrypted messaging services.
53. ***First***, the law is well-settled that ***only*** Parliament — not the Central Government — may undertake essential legislative functions, “*which consists in declaring its policy and making it a binding rule of conduct.*” (See *In re Delhi Laws Act, 1912*, *Ajmer-Merwara (Extension of Laws) Act, 1947*,

1951 SCR 747, at para 311.) Indeed, it is only after “*a policy is laid down and a standard established **by statute***” — and “*declared with sufficient clearness*” — that subordinate legislation may be prescribed consistent with that policy and standard. (*Id.*, at paras 308, 326 (emphasis added).)

54. Thus, to impose a requirement that SSIMs enable the identification of the first originator of information in India on their end-to-end encrypted messaging services, there must be a clear policy declaration in Section 79 that Parliament intended to impose such a requirement. However, nothing in Section 79 suggests that Parliament declared such a policy, let alone clearly, and certainly not at the expense of breaking end-to-end encryption. Respondent may not declare and implement such a policy through the Intermediary Rules. Therefore, as Impugned Rule 4(2) exceeds Respondent’s rule-making authority under Section 79, it is *ultra vires* its parent statutory provision.
55. **Second**, Section 79 only allows Respondent to prescribe the “*due diligence*” guidelines that intermediaries must observe to maintain their exemption from liability for third-party content on their respective platforms. However, Impugned Rule 4(2) seeks to impose obligations that fall far outside “*due diligence*”, as it forces fundamental alterations to WhatsApp by breaking end-to-end encryption and changing the fundamental nature of the service that people love and use today in India and across more than 100 countries.



56. Indeed, as explained above, several commentators confirm that enabling the identification of the first originator of information is antithetical to, and destroys, end-to-end encryption:
- a. *“Introducing a traceability requirement for end-to-end encrypted services will lead to **breaking of such encryption** and thus compromising the privacy of individuals making use of such services for their private communication.”* (Software Freedom Law Center, India (SFLC) available at **Annexure P-9** (emphasis added).)
  - b. *“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.**”* (Centre for Communication Governance at National Law University Delhi available at **Annexure P-11** (emphasis added).)
  - c. *“To be clear, **traceability is incompatible with end-to-end encryption.** Encryption as a service is used by journalists and whistleblowers to legitimately protect their privacy and in that is an enabler of the right to privacy and the freedom of expression. Apart from protecting privacy, encryption also makes communications more secure and helps ensure integrity of information.”* (MIT/79/087 available at **Annexure P-12** (emphasis added).)

- d. “This [tracing] obligation also **undermines the use of encryption technology**, which ensures that content is not accessible to the intermediary or third parties.” (COAI available at **Annexure P-8** (emphasis added).)
- e. “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 ... 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.” (ARTICLE 19 Free Word Centre available at **Annexure P-10** (emphasis added).)

57. As a result, Impugned Rule 4(2) far exceeds the scope of Respondent’s rule-making authority under Section 79 and, therefore, is *ultra vires* Section 79.

## 2. Impugned Rule 4(2) is *ultra vires* the intent of the IT Act itself

58. The preamble of the IT Act states that the statute was enacted in part to promote “*uniformity of the law*” with other nations with respect to “*alternatives to paper-based methods of communications*”. The preamble provides, in relevant part:

*“WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;*

*AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, **in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;***

*AND WHEREAS it is considered necessary to **give effect to the said resolution** and to promote efficient delivery of Government services by means of reliable electronic records.”* (Emphasis added.)

59. Petitioner is not aware of any other country that compels intermediaries to change their systems to enable the identification of the first originator of information on end-to-end encrypted messaging services, let alone by breaking end-to-end encryption. Thus, this requirement contravenes the intent of the IT Act to achieve “*uniformity of the law*”, rendering Impugned Rule 4(2) *ultra vires* the intent of the IT Act.

**iv. Impugned Rule 4(2) is “*manifestly arbitrary*” in violation of Article 14 of the Constitution**

60. The Hon’ble Supreme Court has held that laws are “*manifestly arbitrary*” in violation of Article 14 of the Constitution when they are “*obviously unreasonable*”, capricious, irrational, without adequate determining principle, or excessive and disproportionate. (See *Shayara Bano v. Union of India*, AIR 2017 SC 4609, at para 101; *Puttaswamy II*, at para 105.) Impugned Rule 4(2)’s requirement to enable the identification of the first originator of information in India is “*manifestly arbitrary*” for at least two reasons.
61. **First**, as explained above in Paragraphs 31-39, Impugned Rule 4(2) is disproportionate as the harms it causes far outweigh its purported benefits.
62. **Second**, the Hon’ble Supreme Court has held that subordinate legislation suffers from manifest arbitrariness when Parliament did not intend to give authority to make such legislation. (See *State of TN v. P. Krishnamurthy*, (2006) 4 SCC 517, at paras 15-16 (explaining that subordinate legislation may be struck down for “[m]anifest arbitrariness/unreasonableness (to an extent where the court might well say that the legislature never intended to give authority to make such rules)”).) As explained above in Paragraphs 49-59, nothing in the IT Act suggests that Parliament ever intended to empower Respondent to require

SSMIs to enable the identification of the first originator of information in India.

**v. Impugned Rule 4(2) violates the principle of data minimisation**

63. Data minimisation principles dictate that, generally, an online service should only collect and store user data that is essential to provide its service in order to minimize the risks of unauthorized entities accessing that data. The Hon'ble Supreme Court, in Sikri, J.'s majority judgment in *Puttaswamy II*, observed that only with "*strict observance*" of the principles of data minimisation and storage limitation "*can the State successfully discharge the burden of proportionality while affecting the privacy rights of its citizens.*" (*Puttaswamy II*, at para 221.) Chandrachud J.'s decision likewise observed that the statute at issue in the case was unconstitutional for violating, *inter alia*, the principle of data minimisation. (*Puttaswamy II*, at para 510.4.)
64. To the extent the Impugned Rule requires intermediaries like Petitioner to store additional data for every message sent in India on its platform, it is contrary to data minimization principles. Such a requirement would also be particularly disproportionate as the Impugned Rule does not prescribe a time limit, forcing Petitioner to store this additional data even years after the message was sent.

65. Accordingly, Impugned Rule 4(2)'s requirement that SSIMs like Petitioner enable the identification of the first originator of information in India on end-to-end encrypted messaging services should be struck down as unconstitutional, *ultra vires* the IT Act, and illegal. Petitioner further submits that criminal liability may not be imposed for non-compliance with Impugned Rule 4(2), and that any attempt to impose criminal liability for non-compliance with Impugned Rule 4(2) is unconstitutional, *ultra vires* the IT Act, and illegal.
66. Petitioner reserves its right to request leave of this Hon'ble Court to add or amend any of the aforementioned grounds at a later stage, if required.

### **PRAYER**

In view of the above grounds and submissions, Petitioner most respectfully prays that this Hon'ble Court may be pleased to:

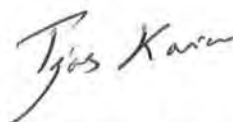
- a. Issue a writ of mandamus or any other appropriate writ, direction, or order to declare that (i) Impugned Rule 4(2) is violative of Articles 14, 19(1)(a), 19(1)(g), and 21 of the Constitution, *ultra vires* the IT Act, and illegal as to end-to-end encrypted messaging services; and (ii) criminal liability may not be imposed for non-compliance with Impugned Rule 4(2) and any attempt to impose criminal liability for non-compliance with Impugned Rule 4(2) is unconstitutional, *ultra vires* the IT Act, and illegal; and

- B. Pass any further orders that this Hon'ble Court may deem fit and proper in light of the facts and circumstances of the present case.

FOR WHICH ACT OF KINDNESS THE PETITIONER SHALL AS DUTY  
BOUND FOREVER PRAY

  
PETITIONER

FILED THROUGH



M/S. SHARDUL AMARCHAND MANGALDAS  
& CO., ADVOCATES FOR THE PETITIONER  
AMARCHAND TOWERS, 216, OKHLA  
INDUSTRIAL ESTATE, PHASE-III, NEW  
DELHI -110020

EMAIL: TEJAS.KARIA@AMSSHARDUL.COM

PAVIT.KATOCH@AMSSHARDUL.COM

MOB: 9871790539

PLACE: NEW DELHI  
DATE: 21 MAY 2021

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

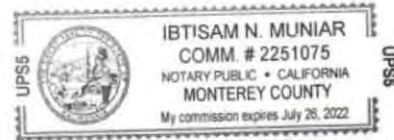
County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

*[Handwritten Signature]*

Ibtisam N. Muniar (Notary)



(Seal)

## Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document



**IN THE HIGH COURT OF DELHI AT NEW DELHI****CIVIL WRIT JURISDICTION****WRIT PETITION (CIVIL) NO.      OF 2021****IN THE MATTER OF:****WHATSAPP LLC****...PETITIONER****VERSUS****UNION OF INDIA****... RESPONDENT****AFFIDAVIT ON BEHALF OF PETITIONER**

I, Brian Hennessy, son of Mark Hennessy, aged about 41 years, Power of Attorney holder of the Petitioner, WhatsApp LLC ("WhatsApp"), having its office at 1601 Willow Road, Menlo Park, California 94025, USA, do hereby solemnly affirm and state as under:

1. I am the Power of Attorney Holder of WhatsApp and am duly authorized and competent to swear this affidavit on behalf of WhatsApp. I am acquainted with the facts of the present case as derived from the official records maintained in the usual and ordinary course of business, and therefore competent to affirm this affidavit.
  2. I have read and understood the contents of Writ Petition under Article 226 of the Constitution of India and state that the facts stated therein are true to the best of my knowledge and the submissions made therein are based on legal advice received and believed by me
-

to be true and correct. The contents of the affidavit are true to my personal knowledge.

3. I adopt the contents of the accompanying Writ Petition as part and parcel of my affidavit, the same not being reproduced herein for the sake of brevity.

SOLEMNLY AFFIRMED AT 22401 SAN VICENTE AVENUE, SAN JOSE, CALIFORNIA 95120, USA ON THIS 21ST DAY OF MAY 2021.

  
**DEPONENT**

**VERIFICATION**

I, the Deponent above named, do hereby verify that the contents of the aforesaid Affidavit are true and correct to the best of my knowledge and information based on the records, no part of the Affidavit is false, and nothing material has been concealed therefrom.

Verified by me at 22401 San Vicente Avenue, San Jose, California 95120, USA on this 21st day of May 2021.

  
**DEPONENT**

## Jurat

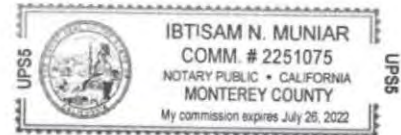
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 20 21,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibti Sam N. Muniar (Notary)

(Seal)

## Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

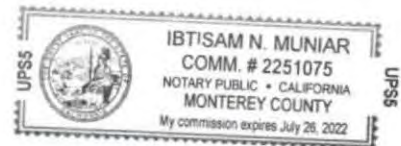
County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 20 21,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_



Ibtiham N. Muniar (Notary)



(Seal)

Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document

**MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY****NOTIFICATION**

New Delhi, the 25th February, 2021

**G.S.R. 139(E).**—In exercise of the powers conferred by sub-section (1), clauses (z) and (zg) of sub-section (2) of section 87 of the Information Technology Act, 2000 (21 of 2000), and in supersession of the Information Technology (Intermediaries Guidelines) Rules, 2011, except as respect things done or omitted to be done before such supersession, the Central Government hereby makes the following rules, namely:—

**PART I****PRELIMINARY**

**1. Short Title and Commencement.**—(1) These rules may be called the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

(2) They shall come into force on the date of their publication in the Official Gazette.

**2. Definitions.**— (1) In these rules, unless the context otherwise requires-

- (a) 'access control mechanism' means any measure, including a technical measure, through which access to online curated content may be restricted based on verification of the identity or age of a user;
- (b) 'access services' means any measure, including technical measure such as closed captioning, subtitles and audio descriptions, through which the accessibility of online curated content may be improved for persons with disabilities;
- (c) 'Act' means the Information Technology Act, 2000 (21 of 2000);
- (d) 'child' means any person below the age of eighteen years;
- (e) 'committee' means the Inter-Departmental Committee constituted under rule 14;
- (f) 'communication link' means a connection between a hypertext or graphical element, and one or more items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which can be another electronic record or another website or application or graphical element;
- (g) 'content' means the electronic record defined in clause (t) of section 2 of the Act;
- (h) 'content descriptor' means the issues and concerns which are relevant to the classification of any online curated content, including discrimination, depiction of illegal or harmful substances, imitable behaviour, nudity, language, sex, violence, fear, threat, horror and other such concerns as specified in the *Schedule* annexed to the rules;
- (i) 'digital media' means digitized content that can be transmitted over the internet or computer networks and includes content received, stored, transmitted, edited or processed by-
  - (i) an intermediary; or
  - (ii) a publisher of news and current affairs content or a publisher of online curated content;
- (j) 'grievance' includes any complaint, whether regarding any content, any duties of an intermediary or publisher under the Act, or other matters pertaining to the computer resource of an intermediary or publisher, as the case may be;
- (k) 'Grievance Officer' means an officer appointed by the intermediary or the publisher, as the case may be, for the purposes of these rules;
- (l) 'Ministry' means, for the purpose of Part II of these rules unless specified otherwise, the Ministry of Electronics and Information Technology, Government of India, and for the purpose of Part III of these rules, the Ministry of Information and Broadcasting, Government of India;
- (m) 'news and current affairs content' includes newly received or noteworthy content, including analysis, especially about recent events primarily of socio-political, economic or cultural

nature, made available over the internet or computer networks, and any digital media shall be news and current affairs content where the context, substance, purpose, import and meaning of such information is in the nature of news and current affairs content.

- (n) 'newspaper' means a periodical of loosely folded sheets usually printed on newsprint and brought out daily or at least once in a week, containing information on current events, public news or comments on public news;
- (o) 'news aggregator' means an entity who, performing a significant role in determining the news and current affairs content being made available, makes available to users a computer resource that enable such users to access the news and current affairs content which is aggregated, curated and presented by such entity.
- (p) 'on demand' means a system where a user, subscriber or viewer is enabled to access, at a time chosen by such user, any content in electronic form, which is transmitted over a computer resource and is selected by the user;
- (q) 'online curated content' means any curated catalogue of audio-visual content, other than news and current affairs content, which is owned by, licensed to or contracted to be transmitted by a publisher of online curated content, and made available on demand, including but not limited through subscription, over the internet or computer networks, and includes films, audio visual programmes, documentaries, television programmes, serials, podcasts and other such content;
- (r) 'person' means a person as defined in sub-section (31) of section 2 of the Income tax Act, 1961 (43 of 1961);
- (s) 'publisher' means a publisher of news and current affairs content or a publisher of online curated content;
- (t) 'publisher of news and current affairs content' means an online paper, news portal, news aggregator, news agency and such other entity called by whatever name, which is functionally similar to publishers of news and current affairs content but shall not include newspapers, replica e-papers of the newspaper and any individual or user who is not transmitting content in the course of systematic business, professional or commercial activity;
- (u) 'publisher of online curated content' means a publisher who, performing a significant role in determining the online curated content being made available, makes available to users a computer resource that enables such users to access online curated content over the internet or computer networks, and such other entity called by whatever name, which is functionally similar to publishers of online curated content but does not include any individual or user who is not transmitting online curated content in the course of systematic business, professional or commercial activity;
- (v) 'significant social media intermediary' means a social media intermediary having number of registered users in India above such threshold as notified by the Central Government;
- (w) 'social media intermediary' means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;
- (x) 'user' means any person who accesses or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and includes other persons jointly participating in using such computer resource and addressee and originator;
- (y) 'user account' means the account registration of a user with an intermediary or publisher and includes profiles, accounts, pages, handles and other similar presences by means of which a user is able to access the services offered by the intermediary or publisher.

(2) Words and expressions used and not defined in these rules but defined in the Act and rules made thereunder shall have the same meaning as assigned to them in the Act and the said rules, as the case may be.

## PART II

## DUE DILIGENCE BY INTERMEDIARIES AND GRIEVANCE REDRESSAL MECHANISM

3. (1) **Due diligence by an intermediary:** An intermediary, including social media intermediary and significant social media intermediary, shall observe the following due diligence while discharging its duties, namely:—

- (a) the intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person;
- (b) the rules and regulations, privacy policy or user agreement of the intermediary shall inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that,—
  - (i) belongs to another person and to which the user does not have any right;
  - (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
  - (iii) is harmful to child;
  - (iv) infringes any patent, trademark, copyright or other proprietary rights;
  - (v) violates any law for the time being in force;
  - (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
  - (vii) impersonates another person;
  - (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;
  - (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
  - (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;
- (c) an intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be;
- (d) an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

*Provided that* any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

*Provided further that* if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

*Provided also that* the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act;

- (e) the temporary or transient or intermediate storage of information automatically by an intermediary in a computer resource within its control as an intrinsic feature of that computer resource, involving no exercise of any human, automated or algorithmic editorial control for onward transmission or communication to another computer resource shall not amount to hosting, storing or publishing any information referred to under clause (d);
- (f) the intermediary shall periodically, and at least once in a year, inform its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be;
- (g) where upon receiving actual knowledge under clause (d), on a voluntary basis on violation of clause (b), or on the basis of grievances received under sub-rule (2), any information has been removed or access to which has been disabled, the intermediary shall, without vitiating the evidence in any manner, preserve such information and associated records for one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by Government agencies who are lawfully authorised;
- (h) where an intermediary collects information from a user for registration on the computer resource, it shall retain his information for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be;
- (i) the intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011;
- (j) the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:

*Provided that* any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be;

- (k) the intermediary shall not knowingly deploy or install or modify technical configuration of computer resource or become party to any act that may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

*Provided that* the intermediary may develop, produce, distribute or employ technological means for the purpose of performing the acts of securing the computer resource and information contained therein;

- (l) the intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.



- (2) **Grievance redressal mechanism of intermediary:** (a) The intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall -
- (i) acknowledge the complaint within twenty four hours and dispose off such complaint within a period of fifteen days from the date of its receipt;
  - (ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.
- (b) The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is *prima facie* in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:
- (c) The intermediary shall implement a mechanism for the receipt of complaints under clause (b) of this sub-rule which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link.

**4. Additional due diligence to be observed by significant social media intermediary.—**(1) In addition to the due diligence observed under rule 3, a significant social media intermediary shall, within three months from the date of notification of the threshold under clause (v) of sub-rule (1) of rule 2, observe the following additional due diligence while discharging its duties, namely:—

- (a) appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder:

*Provided that* no liability under the Act or rules made thereunder may be imposed on such significant social media intermediary without being given an opportunity of being heard.

*Explanation.—*For the purposes of this clause “*Chief Compliance Officer*” means a key managerial personnel or such other senior employee of a significant social media intermediary who is resident in India;

- (b) appoint a nodal contact person for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.

*Explanation.—*For the purposes of this clause “*nodal contact person*” means the employee of a significant social media intermediary, other than the Chief Compliance Officer, who is resident in India;

- (c) appoint a Resident Grievance Officer, who shall, subject to clause (b), be responsible for the functions referred to in sub-rule (2) of rule 3.

*Explanation.—*For the purposes of this clause, “*Resident Grievance Officer*” means the employee of a significant social media intermediary, who is resident in India;

- (d) publish periodic compliance report every month mentioning the details of complaints received and action taken thereon, and the number of specific communication links or parts of information that the intermediary has removed or disabled access to in pursuance of any

proactive monitoring conducted by using automated tools or any other relevant information as may be specified;

(2) A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form:

*Provided that* an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:

*Provided further* that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:

*Provided also that* in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users:

*Provided also that* where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for the purpose of this clause.

(3) A significant social media intermediary that provides any service with respect to an information or transmits that information on behalf of another person on its computer resource—

- (a) for direct financial benefit in a manner that increases its visibility or prominence, or targets the receiver of that information; or
- (b) to which it owns a copyright, or has an exclusive license, or in relation with which it has entered into any contract that directly or indirectly restricts the publication or transmission of that information through any means other than those provided through the computer resource of such social media intermediary,

shall make that information clearly identifiable to its users as being advertised, marketed, sponsored, owned, or exclusively controlled, as the case may be, or shall make it identifiable as such in an appropriate manner.

(4) A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

*Provided that* the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

*Provided further that* such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

*Provided also that* the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

(5) The significant social media intermediary shall have a physical contact address in India published on its website, mobile based application or both, as the case may be, for the purposes of receiving the communication addressed to it.

(6) The significant social media intermediary shall implement an appropriate mechanism for the receipt of complaints under sub-rule (2) of rule 3 and grievances in relation to the violation of provisions under this rule, which shall enable the complainant to track the status of such complaint or grievance by providing a unique ticket number for every complaint or grievance received by such intermediary:

*Provided that* such intermediary shall, to the extent reasonable, provide such complainant with reasons for any action taken or not taken by such intermediary in pursuance of the complaint or grievance received by it.

(7) The significant social media intermediary shall enable users who register for their services from India, or use their services in India, to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users, and where any user voluntarily verifies their account, such user shall be provided with a demonstrable and visible mark of verification, which shall be visible to all users of the service:

*Provided that* the information received for the purpose of verification under this sub-rule shall not be used for any other purpose, unless the user expressly consents to such use.

(8) Where a significant social media intermediary removes or disables access to any information, data or communication link, under clause (b) of sub-rule (1) of rule 3 on its own accord, such intermediary shall,—

- (a) ensure that prior to the time at which such intermediary removes or disables access, it has provided the user who has created, uploaded, shared, disseminated, or modified information, data or communication link using its services with a notification explaining the action being taken and the grounds or reasons for such action;
- (b) ensure that the user who has created, uploaded, shared, disseminated, or modified information using its services is provided with an adequate and reasonable opportunity to dispute the action being taken by such intermediary and request for the reinstatement of access to such information, data or communication link, which may be decided within a reasonable time;
- (c) ensure that the Resident Grievance Officer of such intermediary maintains appropriate oversight over the mechanism for resolution of any disputes raised by the user under clause (b).
- (9) The Ministry may call for such additional information from any significant social media intermediary as it may consider necessary for the purposes of this part.

**5. Additional due diligence to be observed by an intermediary in relation to news and current affairs content.**—In addition to adherence to rules 3 and 4, as may be applicable, an intermediary shall publish, on an appropriate place on its website, mobile based application or both, as the case may be, a clear and concise statement informing publishers of news and current affairs content that in addition to the common terms of service for all users, such publishers shall furnish the details of their user accounts on the services of such intermediary to the Ministry as may be required under rule 18:

*Provided that* an intermediary may provide such publishers who have provided information under rule 18 with a demonstrable and visible mark of verification as being publishers, which shall be visible to all users of the service.

*Explanation.*—This rule relates only to news and current affairs content and shall be administered by the Ministry of Information and Broadcasting.

**6. Notification of other intermediary.**—(1) The Ministry may by order, for reasons to be recorded in writing, require any intermediary, which is not a significant social media intermediary, to comply with all or any of the obligations mentioned under rule 4, if the services of that intermediary permits the publication or transmission of information in a manner that may create a material risk of harm to the sovereignty and integrity of India, security of the State, friendly relations with foreign States or public order.

(2) The assessment of material risk of harm referred to in sub-rule (1) shall be made having regard to the nature of services of such intermediary, and if those services permit,—

- (a) interaction between users, notwithstanding, whether it is the primary purpose of that intermediary; and
- (b) the publication or transmission of information to a significant number of other users as would be likely to result in widespread dissemination of such information.

(3) An order under this rule may be issued in relation to a specific part of the computer resources of any website, mobile based application or both, as the case may be, if such specific part is in the nature of an intermediary:

*Provided that* where such order is issued, an entity may be required to comply with all or any of the obligations mentioned under rule 4, in relation to the specific part of its computer resource which is in the nature of an intermediary.

**7. Non-observance of Rules.**—Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

### PART III

#### CODE OF ETHICS AND PROCEDURE AND SAFEGUARDS IN RELATION TO DIGITAL MEDIA

**8. Application of this Part.**—(1) The rules made under this Part shall apply to the following persons or entities, namely:—

- (a) publishers of news and current affairs content;
- (b) publishers of online curated content; and

shall be administered by the Ministry of Information and Broadcasting, Government of India, which shall be referred to in this Part as the “Ministry”:

*Provided that* the rules made under this Part shall apply to intermediaries for the purposes of rules 15 and 16;

- (2) the rules made under this Part shall apply to the publishers, where,—
  - (a) such publisher operates in the territory of India; or
  - (b) such publisher conducts systematic business activity of making its content available in India.

*Explanation.*—For the purposes of this rule,—

- (a) a publisher shall be deemed to operate in the territory of India where such publisher has a physical presence in the territory of India;
- (b) “*systematic activity*” shall mean any structured or organised activity that involves an element of planning, method, continuity or persistence.

(3) The rules made under this Part shall be in addition to and not in derogation of the provisions of any other law for the time being in force and any remedies available under such laws including the Information Technology (Procedure and Safeguards for Blocking of Access of Information by the Public) Rules, 2009.

**9. Observance and adherence to the Code.**—(1) A publisher referred to in rule 8 shall observe and adhere to the Code of Ethics laid down in the *Appendix* annexed to these rules.

(2) Notwithstanding anything contained in these rules, a publisher referred to in rule 8 who contravenes any law for the time being in force, shall also be liable for consequential action as provided in such law which has so been contravened.

(3) For ensuring observance and adherence to the Code of Ethics by publishers operating in the territory of India, and for addressing the grievances made in relation to publishers under this Part, there shall be a three-tier structure as under—

- (a) Level I - Self-regulation by the publishers;
- (b) Level II – Self-regulation by the self-regulating bodies of the publishers;
- (c) Level III - Oversight mechanism by the Central Government.

## CHAPTER I

### GRIEVANCE REDRESSAL MECHANISM

**10. Furnishing and processing of grievance.**—(1) Any person having a grievance regarding content published by a publisher in relation to the Code of Ethics may furnish his grievance on the grievance mechanism established by the publisher under rule 11.

(2) The publisher shall generate and issue an acknowledgement of the grievance for the benefit of the complainant within twenty-four hours of it being furnished for information and record.

(3) The manner of grievance redressal shall have the following arrangement—

- (a) the publisher shall address the grievance and inform the complainant of its decision within fifteen days of the registration of the grievance;
- (b) if the decision of the publisher is not communicated to the complainant within the stipulated fifteen days, the grievance shall be escalated to the level of the self-regulating body of which such publisher is a member.
- (c) where the complainant is not satisfied with the decision of the publisher, it may prefer to appeal to the self-regulating body of which such publisher is a member within fifteen days of receiving such a decision.
- (d) the self-regulating body shall address the grievance referred to in clauses (b) and (c), and convey its decision in the form of a guidance or advisory to the publisher, and inform the complainant of such decision within a period of fifteen days..
- (e) where the complainant is not satisfied with the decision of the self-regulating body, it may, within fifteen days of such decision, prefer an appeal to the Oversight Mechanism referred to in rule 13 for resolution.

## CHAPTER II

### SELF REGULATING MECHANISM - LEVEL I

**11. Self-Regulating mechanism at Level I.**— (1) The publisher shall be the Level I of the self-regulating mechanism.

(2) A publisher shall—

- (a) establish a grievance redressal mechanism and shall appoint a Grievance Officer based in India, who shall be responsible for the redressal of grievances received by him;
- (b) display the contact details related to its grievance redressal mechanism and the name and contact details of its Grievance Officer at an appropriate place on its website or interface, as the case may be;
- (c) ensure that the Grievance Officer takes a decision on every grievance received by it within fifteen days, and communicate the same to the complainant within the specified time;
- (d) be a member of a self-regulating body as referred to in rule 12 and abide by its terms and conditions.

(3) The Grievance Officer shall,—

- (a) be the contact point for receiving any grievance relating to Code of Ethics;

- (b) act as the nodal point for interaction with the complainant, the self-regulating body and the Ministry.

(4) Online curated content shall be classified by the publisher of such content into the categories referred to in the *Schedule*, having regard to the context, theme, tone, impact and target audience of such content, with the relevant rating for such categories based on an assessment of the relevant content descriptors in the manner specified in the said *Schedule*.

(5) Every publisher of online curated content shall display the rating of any online curated content and an explanation of the relevant content descriptors, prominently to its users at an appropriate place, as the case may be, in a manner that ensures that such users are aware of this information before accessing such content.

### CHAPTER III

#### SELF REGULATING MECHANISM – LEVEL II

**12. Self-regulating body.—** (1) There may be one or more self-regulatory bodies of publishers, being an independent body constituted by publishers or their associations.

(2) The self-regulatory body referred to in sub-rule (1) shall be headed by a retired judge of the Supreme Court, a High Court, or an independent eminent person from the field of media, broadcasting, entertainment, child rights, human rights or such other relevant field, and have other members, not exceeding six, being experts from the field of media, broadcasting, entertainment, child rights, human rights and such other relevant fields.

(3) The self-regulating body shall, after its constitution in accordance with sub-rule (2), register itself with the Ministry within a period of thirty days from the date of notification of these rules, and where a self-regulating body is constituted after such period, within thirty days from the date of its constitution:

Provided that before grant of registration to the self-regulating body, the Ministry shall satisfy itself that the self-regulating body has been constituted in accordance with sub-rule (2) and has agreed to perform the functions laid down in sub-rules (4) and (5).

- (4) The self-regulating body shall perform the following functions, namely:—
  - (a) oversee and ensure the alignment and adherence by the publisher to the Code of Ethics;
  - (b) provide guidance to publishers on various aspects of the Code of Ethics;
  - (c) address grievances which have not been resolved by publishers within the specified period of fifteen days;
  - (d) hear appeals filed by the complainant against the decision of publishers;
  - (e) issue such guidance or advisories to such publishers as specified in sub-rule (5) for ensuring compliance to the Code of Ethics.
- (5) The self-regulating body while disposing a grievance or an appeal referred to it in sub-rule (4) may issue following guidance or advisories to the publishers as under, namely:—
  - (a) warning, censuring, admonishing or reprimanding the publisher; or
  - (b) requiring an apology by the publisher; or
  - (c) requiring the publisher to include a warning card or a disclaimer; or
  - (d) in case of online curated content, direct the publisher to,—
    - (i) reclassify ratings of relevant content;
    - (ii) make appropriate modification in the content descriptor, age classification and access control measures;
    - (iii) edit synopsis of relevant content; or
  - (e) in case of any content where it is satisfied that there is a need for taking action to delete or modify the content for preventing incitement to the commission of a cognizable offence

relating to public order, or in relation to the reasons enumerated in sub-section (1) of section 69A of the Act, refer such content to the Ministry for consideration by the Oversight Mechanism referred to in rule 13 for appropriate action.

(6) Where the self-regulating body is of the opinion that there is no violation of the Code of Ethics, it shall convey such decision to the complainant and such entity.

(7) Where a publisher fails to comply with the guidance or advisories of the self-regulating body within the time specified in such guidance or advisory, the self-regulating body shall refer the matter to the Oversight Mechanism referred to in rule 13 within fifteen days of expiry of the specified date.

## CHAPTER IV

### OVERSIGHT MECHANISM - LEVEL III

**13. Oversight mechanism.—** (1) The Ministry shall co-ordinate and facilitate the adherence to the Code of Ethics by publishers and self regulating bodies, develop an Oversight Mechanism, and perform the following functions, namely:—

- (a) publish a charter for self regulating bodies, including Codes of Practices for such bodies;
- (b) establish an Inter-Departmental Committee for hearing grievances;
- (c) refer to the Inter-Departmental Committee grievances arising out of the decision of the self-regulating body under rule 12, or where no decision has been taken by the self-regulating body within the specified time period, or such other complaints or references relating to violation of Code of Ethics as it may consider necessary;
- (d) issue appropriate guidance and advisories to publishers;
- (e) issue orders and directions to the publishers for maintenance and adherence to the Code of Ethics.

(2) The Ministry shall appoint an officer of the Ministry not below the rank of a Joint Secretary to the Government of India, as the “*Authorised Officer*”, for the purposes of issuing directions under rules 15 or 16, as the case may be.

**14. Inter-Departmental Committee.—** (1) The Ministry shall constitute an Inter-Departmental Committee, called the Committee, consisting of representatives from the Ministry of Information and Broadcasting, Ministry of Women and Child Development, Ministry of Law and Justice, Ministry of Home Affairs, Ministry of Electronics and Information Technology, Ministry of External Affairs, Ministry of Defence, and such other Ministries and Organisations, including domain experts, that it may decide to include in the Committee:

*Provided that* the Authorised Officer designated under sub-rule (2) of rule 13 shall be the Chairperson of such Committee.

(2) The Committee shall meet periodically and hear the following complaints regarding violation or contravention of the Code of Ethics by the entities referred to in Rule 8—

- (a) arising out of the grievances in respect of the decisions taken at the Level I or II, including the cases where no such decision is taken within the time specified in the grievance redressal mechanism; or
- (b) referred to it by the Ministry.

(3) Any complaint referred to the Committee, whether arising out of the grievances or referred to it by the Ministry, shall be in writing and may be sent either by mail or fax or by e-mail signed with electronic signature of the authorised representative of the entity referring the grievance, and the Committee shall ensure that such reference is assigned a number which is recorded along with the date and time of its receipt.

(4) The Ministry shall make all reasonable efforts to identify the entity referred to in Rule 8 which has created, published or hosted the content or part thereof, and where it is able to identify such entity, it shall issue a duly signed notice to such entity to appear and submit their reply and clarifications, if any, before the Committee.

(5) In the hearing, the Committee shall examine complaints or grievances, and may either accept or allow such complaint or grievance, and make the following recommendations to the Ministry, namely:—

- (a) warning, censuring, admonishing or reprimanding such entity; or
- (b) requiring an apology by such entity; or
- (c) requiring such entity to include a warning card or a disclaimer; or
- (d) in case of online curated content, direct a publisher to—
  - (i) reclassify ratings of relevant content; or
  - (ii) edit synopsis of relevant content; or
  - (iii) make appropriate modification in the content descriptor, age classification and parental or access control;
- (e) delete or modify content for preventing incitement to the commission of a cognisable offence relating to public order;
- (f) in case of content where the Committee is satisfied that there is a need for taking action in relation to the reasons enumerated in sub-section (1) of section 69A of the Act, it may recommend such action.

(6) The Ministry may, after taking into consideration the recommendations of the Committee, issue appropriate orders and directions for compliance by the publisher:

*Provided that* no such order shall be issued without the approval of the Secretary, Ministry of Information and Broadcasting, Government of India (hereinafter referred to as the “Secretary, Ministry of Information and Broadcasting”).

**15. Procedure for issuing of direction.—** (1) In respect of recommendations referred to in clauses (e) and (f) of sub-rule (5) of rule 14, the Authorised Officer shall place the matter for consideration before the Secretary, Ministry of Information and Broadcasting for taking appropriate decision.

(2) The Authorised Officer shall, on approval of the decision by the Secretary, Ministry of Information and Broadcasting, direct the publisher, any agency of the Government or any intermediary, as the case may be to delete or modify or block the relevant content and information generated, transmitted, received, stored or hosted in their computer resource for public access within the time limit specified in the direction:

Provided that in case the recommendation of the Authorised Officer is not approved by the Secretary, Ministry of Information and Broadcasting, the Authorised Officer shall convey the same to the Committee.

(3) A direction under this rule may be issued only in respect of a specific piece of content or an enumerated list of content, as the case may be, and shall not require any entity to cease its operations.

**16. Blocking of information in case of emergency.—** (1) Notwithstanding anything contained in rules 14 and 15, the Authorised Officer, in any case of emergency nature, for which no delay is acceptable, shall examine the relevant content and consider whether it is within the grounds referred to in sub-section (1) of section 69A of the Act and it is necessary or expedient and justifiable to block such information or part thereof and submit a specific recommendation in writing to the Secretary, Ministry of Information and Broadcasting.

(2) In case of emergency nature, the Secretary, Ministry of Information and Broadcasting may, if he is satisfied that it is necessary or expedient and justifiable for blocking for public access of any information or part thereof through any computer resource and after recording reasons in writing, as an interim measure issue such directions as he may consider necessary to such identified or identifiable persons, publishers or intermediary in control of such computer resource hosting such information or part thereof without giving him an opportunity of hearing.

(3) The Authorised Officer, at the earliest but not later than forty-eight hours of issue of direction under sub-rule (2), shall bring the request before the Committee for its consideration and recommendation.



(4) On receipt of recommendations of the Committee under sub-rule (3), the Secretary, Ministry of Information and Broadcasting, shall pass the final order as regard to approval of such request and in case the request for blocking is not approved by the Secretary, Ministry of Information and Broadcasting in his final order, the interim direction issued under sub-rule (2) shall be revoked and the person, publisher or intermediary in control of such information shall be accordingly, directed to unblock the information for public access.

**17. Review of directions issued.—**(1) The Authorised Officer shall maintain complete records of the proceedings of the Committee, including any complaints referred to the Committee, and shall also maintain records of recommendations made by the Committee and any directions issued by the Authorised Officer.

(2) The Review Committee shall meet at least once in every two months and record its findings whether the directions of blocking of content or information issued under these rules are in accordance with the provisions of sub-section (1) of section 69A of the Act and if it is of the opinion that the directions are not in accordance with the said provisions, it may set aside the directions and issue order for unblocking of such content or information generated, transmitted, received, stored or hosted in a computer resource.

*Explanation.*—For the purpose of this rule, “*Review Committee*” shall mean the Review Committee constituted under rule 419A of the Indian Telegraph Rules, 1951.

## CHAPTER V

### FURNISHING OF INFORMATION

**18. Furnishing of information.—**(1) A publisher of news and current affairs content and a publisher of online curated content operating in the territory of India, shall inform the Ministry about the details of its entity by furnishing information along with such documents as may be specified, for the purpose of enabling communication and coordination.

(2) The information referred to in sub-rule (1) shall be furnished within a period of thirty days of the publication of these rules, and where such publisher begins operation in the territory of India or comes into existence after commencement of these rules, within thirty days from the date of start of its operations in the territory of India or its coming into existence, as the case may be.

(3) The publisher of news and current affairs content and the publisher of online curated content shall publish periodic compliance report every month mentioning the details of grievances received and action taken thereon.

(4) The Ministry may call for such additional information from the publisher as it may consider necessary for the implementation of this Rule.

## CHAPTER VI

### MISCELLANEOUS

**19. Disclosure of Information.—**(1) A publisher and a self-regulating body, shall make true and full disclosure of all grievances received by it, the manner in which the grievances are disposed of, the action taken on the grievance, the reply sent to the complainant, the orders or directions received by it under these rules and action taken on such orders or directions.

(2) The information referred to in sub-rule (1) shall be displayed publicly and updated monthly.

(3) Subject to any law for the time being in force, the publisher shall preserve records of content transmitted by it for a minimum period of sixty days and make it available to the self-regulating body or the Central Government, or any other Government agency, as may be requisitioned by them for implementation of these rules.

## APPENDIX

## CODE OF ETHICS

**I News and current affairs:**

- (i) Norms of Journalistic Conduct of the Press Council of India under the Press Council Act, 1978;
- (ii) Programme Code under section 5 of the Cable Television Networks Regulation) Act, 1995;
- (iii) Content which is prohibited under any law for the time being in force shall not be published or transmitted.

**II Online curated content:***(A) General Principles:*

- (a) A publisher shall not transmit or publish or exhibit any content which is prohibited under any law for the time being in force or has been prohibited by any court of competent jurisdiction.
- (b) A publisher shall take into consideration the following factors, when deciding to feature or transmit or publish or exhibit any content, after duly considering the implications of any content as falling under the following categories, and shall exercise due caution and discretion in relation to the same, namely:—
  - (i) content which affects the sovereignty and integrity of India;
  - (ii) content which threatens, endangers or jeopardises the security of the State;
  - (iii) content which is detrimental to India's friendly relations with foreign countries;
  - (iv) content which is likely to incite violence or disturb the maintenance of public order.
- (c) A publisher shall take into consideration India's multi-racial and multi-religious context and exercise due caution and discretion when featuring the activities, beliefs, practices, or views of any racial or religious group.

*(B) Content Classification:*

- (i) All content transmitted or published or exhibited by a publisher of online curated content shall be classified, based on the nature and type of content, into the following rating categories, namely:—
  - (a) Online curated content which is suitable for children as well as people of all ages shall be classified as "U" rating;
  - (b) Online curated content which is suitable for persons aged 7 years and above, and can be viewed by a person under the age of 7 years with parental guidance, shall be classified as "U/A 7+" rating;
  - (c) Online curated content which is suitable for persons aged 13 years and above, and can be viewed by a person under the age of 13 years with parental guidance, shall be classified as "U/A 13+" rating;
  - (d) Online curated content which is suitable for persons aged 16 years and above, and can be viewed by a person under the age of 16 years with parental guidance, shall be classified as "U/A 16+" rating; and
  - (e) Online curated content which is restricted to adults shall be classified as "A" rating.
- (ii) The Content may be classified on the basis of.—i) Themes and messages; ii) Violence; iii) Nudity; iv) Sex; v) Language; vi) Drug and substance abuse; and (vii) Horror as described in the *Schedule*, as may be modified from time to time by the Ministry of Information & Broadcasting.

*(C) Display of Classification:*

- (a) The publisher of online curated content shall prominently display the classification rating specific to each content or programme together with a content descriptor informing the user about the nature of the content, and advising on viewer discretion (if applicable) at the beginning of every programme enabling the user to make an informed decision, prior to watching the programme.

- (b) The publisher of online curated content making available content that is classified as U/A 13+ or higher shall ensure that access control mechanisms, including parental locks, are made available for such content.
- (c) A publisher of online curated content which makes available content or programme that is classified as “A” shall implement a reliable age verification mechanism for viewership of such content.
- (d) A publisher of online curated content must strive to include classification rating and consumer advice for their programmes in any print, televised or online promotional or publicity material and prominently display the classification rating specific to each such content.

*(D) Restriction of access to certain curated content by a child:*

Every publisher of online curated content providing access to online curated content which has an “A” rating shall take all efforts to restrict access to such content by a child through the implementation of appropriate access control measures.

*(E) Measures to improve accessibility of online curated content by persons with disabilities:*

Every publisher of online curated content shall, to the extent feasible, take reasonable efforts to improve the accessibility of online curated content transmitted by it to persons with disabilities through the implementation of appropriate access services.

## SCHEDULE

**Classification of any curated content shall be guided by the following sets of guidelines, namely:—**

### PART I

#### GENERAL GUIDELINES FOR CLASSIFICATION OF FILMS AND OTHER ENTERTAINMENT PROGRAMMES, INCLUDING WEB BASED SERIALS

There are general factors that may influence a classification decision at any level and in connection with any issue and the following factors are elucidated which may be read along with Part II of the Guidelines -

**(a) Context:**

Curated content may be considered in the light of the period depicted in such content and the contemporary standards of the country and the people to which such content relates. Therefore, the context in which an issue is presented within a film or video may be given consideration. Factors such as the setting of a work (historical, fantasy, realistic, contemporary etc.), the manner of presentation of the content, the apparent intention of the content, the original production date of the content, and any special merits of the work may influence the classification decision.

**(b) Theme:**

Classification decisions may take into the theme of any content but will depend significantly on the treatment of that theme, especially the sensitivity of its presentation. The most challenging themes (for example, drug misuse, violence, pedophilia, sex, racial or communal hatred or violence etc.) are unlikely to be appropriate at the junior levels of classification.

**(c) Tone and impact:**

Curated content may be judged in its entirety from the point of view of its overall impact. The tone of content can be an important factor in deciding the influence it may have on various groups of people. Thus, films/serials that have a stronger depiction of violence may receive a higher classification.

**(d) Target audience:**

The classification of any content may also depend upon the target audience of the work and the impact of the work on such audience.

## PART II

### ISSUE RELATED GUIDELINES

This part of the guidelines comprises the issues and concerns that apply in varying degrees to all categories of classification and elaborates the general approach that may be taken in this regard to the same. These concerns are listed in alphabetical order, and are to be read with the four General Guidelines listed in Part I

**(a) Discrimination:**

The categorical classification of content shall take into account the impact of a film on matters such as caste, race, gender, religion, disability or sexuality that may arise in a wide range of works, and the classification decision will take account of the strength or impact of their inclusion.

**(b) Psychotropic substances, liquor, smoking and tobacco:**

Films or serials, etc. that as a whole portray misuse of psychotropic substances, liquor, smoking and tobacco would qualify for a higher category of classification.

**(c) Imitable behaviour:**

- (1) Classification decisions may take into account any portrayal of criminal and violent behaviour with weapons.
- (2) Portrayal of potentially dangerous behaviour that are likely to incite the commission of any offence (including suicide, and infliction of self-harm) and that children and young people may potentially copy, shall receive a higher classification.
- (3) Films or serials with song and dance scenes comprising lyrics and gestures that have sexual innuendos would receive a higher classification.

**(d) Language:**

- (1) Language is of particular importance, given the vast linguistic diversity of our country. The use of language, dialect, idioms and euphemisms vary from region to region and are culture-specific. This factor has to be taken into account during the process of classification of a work in a particular category.
- (2) Language that people may find offensive includes the use of expletives. The extent of offence may vary according to age, gender, race, background, beliefs and expectations of the target audience from the work as well as the context, region and language in which the word, expression or gesture is used.
- (3) It is not possible to set out a comprehensive list of words, expressions or gestures that are acceptable at each category in every Indian language. The advice at different classification levels, therefore, provides general guidance to consider while judging the level of classification for content, based on this guideline.

**(e) Nudity:**

- (1) No content that is prohibited by law at the time being in force can be published or transmitted.
- (2) Nudity with a sexual context will receive a higher classification of "A".

**(f) Sex:**

No content that is prohibited by law at the time being in force can be published or transmitted. The classification of content in various ratings from U/A 16+ to "A" shall depend upon the portrayal of non-explicit (implicit) to explicit depiction of sexual behaviour.

**(g) Violence:**

Classification decisions shall take account of the degree and nature of violence in a work.

[F. No. 16(4)/2020-CLES]

Dr. RAJENDRA KUMAR, Addl. Secy.

## Key Updates

Last modified: January 04, 2021

Respect for your privacy is coded into our DNA. Since we started WhatsApp, we've built our services with a set of strong privacy principles in mind. In our updated [Terms of Service](#) and [Privacy Policy](#) you'll find:

- **Additional Information On How We Handle Your Data.** Our updated Terms and Privacy Policy provide more information on how we process your data, and our commitment to privacy. For example, we've added more information about more recent product features and functionalities, how we process your data for safety, security and integrity, and added more direct links to user settings, Help Center articles and how you can manage your information.
- **Better Communication With Businesses.** Many businesses rely on WhatsApp to communicate with their customers and clients. We work with businesses that use Facebook or third parties to help store and better manage their communications with you on WhatsApp.
- **Making It Easier To Connect.** As part of the [Facebook Companies](#), WhatsApp partners with Facebook to offer experiences and integrations across Facebook's family of apps and products.

[Back to top](#)

**TRUE COPY**

### About end-to-end encryption

Privacy and security is in our DNA, which is why we built end-to-end encryption into our app. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, status updates and calls are secured from falling into the wrong hands.



### Personal Messaging

WhatsApp's end-to-end encryption is used when you chat with another person using WhatsApp Messenger. End-to-end encryption ensures only you and the person you're communicating with can read or listen to what is sent, and nobody in between, not even WhatsApp. This is because with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. All of this happens automatically: no need to turn on any special settings to secure your messages.

### Business Messaging

Every WhatsApp message is protected by the same Signal encryption protocol that secures messages before they leave your device. When you message a WhatsApp business account, your message is delivered securely to the destination chosen by the business.

WhatsApp considers chats with businesses that use the WhatsApp Business app or manage and store customer messages themselves to be end-to-end encrypted. Once the message is received, it will be subject to the business's own privacy practices. The business may designate a number of employees, or even other vendors, to process and respond to the message.

Some businesses<sup>1</sup> will be able to choose WhatsApp's parent company, Facebook, to securely store messages and respond to customers. While Facebook will not automatically use your messages to inform the ads that you see, businesses will be able to use chats they receive for their own marketing purposes, which may include advertising on Facebook. You can always contact that business to learn more about its privacy practices.

**Note:** The encryption status of an end-to-end encrypted chat cannot change without the change being visible to the user. For more information about which chats are end-to-end encrypted, please read our [white paper](#).

### Payments

Payments on WhatsApp, which are available in select countries, enable transfers between accounts at financial institutions. Card and bank numbers are stored encrypted and in a highly-secured network. However, because financial institutions can't process transactions without receiving information related to these payments, these payments aren't end-to-end encrypted.

### What's the "Verify Security Code" screen in the contact info screen?

End-to-end encrypted chats have their own security code used to verify that the calls and the messages you send to that chat are end-to-end encrypted.

**Note:** The verification process is optional for end-to-end encrypted chats, and only used to confirm that the messages and calls you send are end-to-end encrypted.

This code can be found in the contact info screen, both as a QR code and a 60-digit number. These codes are unique to each chat and can be compared between people in each chat to verify that the messages you send to the chat are end-to-end encrypted. Security codes are just visible versions of the special key shared between you – and don't worry, it's not the actual key itself, that's always kept secret.

To verify that a chat is end-to-end encrypted:

1. Open the chat.
2. Tap on the name of the contact to open the contact info screen.
3. Tap **Encryption** to view the QR code and 60-digit number.

- **Note:** This feature is only available for a contact in an end-to-end encrypted chat.

If you and your contact are physically next to each other, one of you can scan the other's QR code or visually compare the 60-digit number. If you scan the QR code, and the code is indeed the same, a green check mark will appear. Since they match, you can be sure no one is intercepting your messages or calls.

If the codes don't match, it's likely you're scanning the code of a different contact, or a different phone number. If your contact has recently reinstalled WhatsApp or changed phones, we recommend you refresh the code by sending them a new message and then scanning the code. Learn more about security codes changing in [this article](#).

If you and your contact aren't physically near each other, you can send them the 60-digit number. Let your contact know that once they receive your code, they should write it down and then visually compare it to the 60-digit number that appears in the contact info screen under Encryption. For Android and iPhone, you can use the Share button from the Verify Security Code screen to send the 60-digit number via SMS, email, etc.

[Why does WhatsApp offer end-to-end encryption and what does it mean for keeping people safe?](#)

Security is essential to the service WhatsApp provides. We've seen multiple examples where criminal hackers illegally obtained vast sums of private data and abused technology to hurt people with their stolen information. Since completing the implementation of end-to-end encryption in 2016, digital security has become even more important.

WhatsApp has no ability to see the content of messages or listen to calls that are end-to-end encrypted. That's because the encryption and decryption of messages sent and received on WhatsApp occurs entirely on your device. Before a message ever leaves your device, it's secured with a cryptographic lock, and only the recipient has the keys. In addition, the keys change with every single message that's sent. While all of this happens behind the scenes, you can confirm your conversations are protected by checking the security verification code on your device. You can find more details about how this works in our [white paper](#).

Naturally, people have asked what end-to-end encryption means for the work of law enforcement. WhatsApp appreciates the work that law enforcement agencies do to keep people safe around the world. We carefully review, validate and respond to law enforcement requests based on applicable law and policy, and we prioritize responses to emergency requests. As part of our education efforts, we published information for law enforcement about the limited information we collect and how they can make requests of WhatsApp, which you can read [here](#).

To learn more about your security on WhatsApp, please visit [WhatsApp Security](#).

1In 2021.

HELP CENTER



# WhatsApp Encryption Overview

Technical white paper

Version 3 Updated October 22, 2020

Version 2 Updated December 19, 2017

Version 1 Originally published April 5, 2016



# Contents

Introduction . . . . .	3
Terms . . . . .	3
Client Registration . . . . .	4
Initiating Session Setup . . . . .	4
Receiving Session Setup. . . . .	5
Exchanging Messages. . . . .	5
Transmitting Media and Other Attachments. . . . .	6
Group Messages . . . . .	6
Call Setup . . . . .	7
Statuses. . . . .	8
Live Location . . . . .	8
Verifying Keys. . . . .	10
Transport Security . . . . .	10
Defining End-to-End Encryption . . . . .	11
Implementation on WhatsApp Services . . . . .	11
Encryption Has No Off Switch. . . . .	13
Displaying End-to-End Encryption Status . . . . .	13
Conclusion . . . . .	13

## Introduction

This white paper provides a technical explanation of WhatsApp's end-to-end encryption system. Please visit WhatsApp's website at [www.whatsapp.com/security](https://www.whatsapp.com/security) for more information.

WhatsApp Messenger allows people to exchange messages (including chats, group chats, images, videos, voice messages and files), share status posts, and make WhatsApp calls around the world. WhatsApp messages, voice and video calls between a sender and receiver that use WhatsApp client software released after March 31, 2016 use the Signal protocol outlined below. See "Defining End-to-End Encryption" for information about which communications are end-to-end encrypted.

The Signal Protocol, designed by Open Whisper Systems, is the basis for WhatsApp's end-to-end encryption. This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls. What's more, even if encryption keys from a user's device are ever physically compromised, they cannot be used to go back in time to decrypt previously transmitted messages.

This document gives an overview of the Signal Protocol and its use in WhatsApp.

## Terms

### Public Key Types

- **Identity Key Pair** – A long-term Curve25519 key pair, generated at install time.
- **Signed Pre Key** – A medium-term Curve25519 key pair, generated at install time, signed by the **Identity Key**, and rotated on a periodic timed basis.
- **One-Time Pre Keys** – A queue of Curve25519 key pairs for one time use, generated at install time, and replenished as needed.

### Session Key Types

- **Root Key** – A 32-byte value that is used to create **Chain Keys**.
- **Chain Key** – A 32-byte value that is used to create **Message Keys**.
- **Message Key** – An 80-byte value that is used to encrypt message contents. 32 bytes are used for an AES-256 key, 32 bytes for a HMAC-SHA256 key, and 16 bytes for an IV.

## Client Registration

At registration time, a WhatsApp client transmits its public Identity Key, public Signed Pre Key (with its signature), and a batch of public One-Time Pre Keys to the server. The WhatsApp server stores these public keys associated with the user's identifier.

## Initiating Session Setup

To communicate with another WhatsApp user, a WhatsApp client first needs to establish an encrypted session. Once the session is established, clients do not need to rebuild a new session with each other until the existing session state is lost through an external event such as an app reinstall or device change.

To establish a session:

1. The initiating client ("initiator") requests the public Identity Key, public Signed Pre Key, and a single public One-Time Pre Key for the recipient.
2. The server returns the requested public key values. A One-Time Pre Key is only used once, so it is removed from server storage after being requested. If the recipient's latest batch of One-Time Pre Keys has been consumed and the recipient has not replenished them, no One-Time Pre Key will be returned.
3. The initiator saves the recipient's Identity Key as  $I_{\text{recipient}}$ , the Signed Pre Key as  $S_{\text{recipient}}$ , and the One-Time Pre Key as  $O_{\text{recipient}}$ .
4. The initiator generates an ephemeral Curve25519 key pair,  $E_{\text{initiator}}$ .
5. The initiator loads its own Identity Key as  $I_{\text{initiator}}$ .
6. The initiator calculates a master secret as  $\text{master\_secret} = \text{ECDH}(I_{\text{initiator}}, S_{\text{recipient}}) || \text{ECDH}(E_{\text{initiator}}, I_{\text{recipient}}) || \text{ECDH}(E_{\text{initiator}}, S_{\text{recipient}}) || \text{ECDH}(E_{\text{initiator}}, O_{\text{recipient}})$ . If there is no One Time Pre Key, the final ECDH is omitted.
7. The initiator uses HKDF to create a Root Key and Chain Keys from the master\_secret.

## Receiving Session Setup

After building a long-running encryption session, the initiator can immediately start sending messages to the recipient, even if the recipient is offline. Until the recipient responds, the initiator includes the information (in the header of all messages sent) that the recipient requires to build a corresponding session. This includes the initiator's `Einitiator` and `Iinitiator`.

When the recipient receives a message that includes session setup information:

1. The recipient calculates the corresponding `master_secret` using its own private keys and the public keys advertised in the header of the incoming message.
2. The recipient deletes the `One-Time Pre Key` used by the initiator.
3. The initiator uses HKDF to derive a corresponding `Root Key` and `Chain Keys` from the `master_secret`.

## Exchanging Messages

Once a session has been established, clients exchange messages that are protected with a `Message Key` using `AES256` in CBC mode for encryption and `HMAC-SHA256` for authentication.

The `Message Key` changes for each message transmitted, and is ephemeral, such that the `Message Key` used to encrypt a message cannot be reconstructed from the session state after a message has been transmitted or received.

The `Message Key` is derived from a sender's `Chain Key` that "ratchets" forward with every message sent. Additionally, a new ECDH agreement is performed with each message roundtrip to create a new `Chain Key`. This provides forward secrecy through the combination of both an immediate "hash ratchet" and a round trip "DH ratchet."

## Calculating a Message Key from a Chain Key

Each time a new `Message Key` is needed by a message sender, it is calculated as:

1. `Message Key = HMAC-SHA256(Chain Key, 0x01)`.
2. The `Chain Key` is then updated as `Chain Key = HMAC-SHA256(Chain Key, 0x02)`.

This causes the `Chain Key` to "ratchet" forward, and also means that a stored `Message Key` can't be used to derive current or past values of the `Chain Key`.

## Calculating a Chain Key from a Root Key

Each time a message is transmitted, an ephemeral Curve25519 public key is advertised along with it. Once a response is received, a new Chain Key and Root Key are calculated as:

1. `ephemeral_secret = ECDH(Ephemeral_sender, Ephemeral_recipient).`
2. `Chain Key, Root Key = HKDF(Root Key, ephemeral_secret).`

A chain is only ever used to send messages from one user, so message keys are not reused. Because of the way Message Keys and Chain Keys are calculated, messages can arrive delayed, out of order, or can be lost entirely without any problems.

## Transmitting Media and Other Attachments

Large attachments of any type (video, audio, images, or files) are also end-to-end encrypted:

1. The WhatsApp user sending a message ("sender") generates an ephemeral 32 byte AES256 key, and an ephemeral 32 byte HMAC-SHA256 key.
2. The sender encrypts the attachment with the AES256 key in CBC mode with a random IV, then appends a MAC of the ciphertext using HMAC-SHA256.
3. The sender uploads the encrypted attachment to a blob store.
4. The sender transmits a normal encrypted message to the recipient that contains the encryption key, the HMAC key, a SHA256 hash of the encrypted blob, and a pointer to the blob in the blob store.
5. The recipient decrypts the message, retrieves the encrypted blob from the blob store, verifies the SHA256 hash of it, verifies the MAC, and decrypts the plaintext.

## Group Messages

Traditional unencrypted messenger apps typically employ "server-side fan-out" for group messages. A client wishing to send a message to a group of users transmits a single message, which is then distributed N times to the N different group members by the server.

This is in contrast to “client-side fan-out,” where a client would transmit a single message  $N$  times to the  $N$  different group members itself.

Messages to WhatsApp groups build on the pairwise encrypted sessions outlined above to achieve efficient server-side fan-out for most messages sent to groups. This is accomplished using the “Sender Keys” component of the Signal Messaging Protocol.

The first time a WhatsApp group member sends a message to a group:

1. The sender generates a random 32-byte Chain Key.
2. The sender generates a random Curve25519 Signature Key key pair.
3. The sender combines the 32-byte Chain Key and the public key from the Signature Key into a Sender Key message.
4. The sender individually encrypts the Sender Key to each member of the group, using the pairwise messaging protocol explained previously.

For all subsequent messages to the group:

1. The sender derives a Message Key from the Chain Key, and updates the Chain Key.
2. The sender encrypts the message using AES256 in CBC mode.
3. The sender signs the ciphertext using the Signature Key.
4. The sender transmits the single ciphertext message to the server, which does server-side fan-out to all group participants.

The “hash ratchet” of the message sender’s Chain Key provides forward secrecy. Whenever a group member leaves, all group participants clear their Sender Key and start over.

## Call Setup

WhatsApp voice and video calls are also end-to-end encrypted. When a WhatsApp user initiates a voice or video call:

1. The initiator builds an encrypted session with the recipient (as outlined in Section *Initiating Session Setup*), if one does not already exist.
2. The initiator generates a random 32-byte SRTP master secret.
3. The initiator transmits an encrypted message to the recipient that signals an incoming call, and contains the SRTP master secret.
4. If the responder answers the call, a SRTP encrypted call ensues.

## Statuses

WhatsApp statuses are encrypted in much the same way as group messages. The first status sent to a given set of recipients follows the same sequence of steps as the first time a WhatsApp group member sends a message to a group. Similarly, subsequent statuses sent to the same set of recipients follow the same sequence of steps as all subsequent messages to a group. When a status sender removes a receiver either through changing status privacy settings or removing a number from their address book, the status sender clears their Sender Key and starts over.

## Live Location

Live location messages and updates are encrypted in much the same way as group messages. The first live location message or update sent follows the same sequence of steps as the first time a WhatsApp group member sends a message to a group. But, live location demands a high volume of location broadcasts and updates with lossy delivery where receivers can expect to see large jumps in the number of ratchets, or iteration counts. The Signal Protocol uses a linear-time algorithm for ratcheting that is too slow for this application. This document offers a fast ratcheting algorithm to solve this problem.

Chain keys are currently one-dimensional. To ratchet  $N$  steps takes  $N$  computations. Chain keys are denoted as  $CK(\text{iteration count})$  and message keys as  $MK(\text{iteration count})$ .

```

CK(0)
  ↓
CK(1)
  ↓
...
  ↓
CK(N-1) → MK(N-1)

```

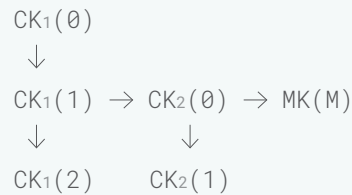
Consider an extension where we keep two chains of chain keys:

```

CK1(0) → CK2(0)
  ↓       ↓
CK1(1)   CK2(1)
           ↓
           ...
           ↓
        CK2(M-1) → MK(M-1)

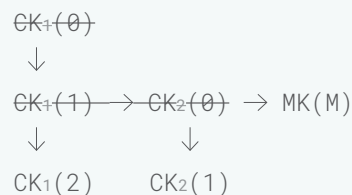
```

In this example, message keys are always derived from  $CK_2$ . A receiver who needs to ratchet by a large amount can skip  $M$  iterations at a time (where  $M$  is an agreed-upon constant positive integer) by ratcheting  $CK_1$  and generating a new  $CK_2$ :



A value of  $CK_2$  may be ratcheted up to  $M$  times. To ratchet  $N$  steps takes up to  $\lceil N/M \rceil + M$  computations.

After a sender creates a message key and encrypts a message with it, all chain keys on the path that led to its creation must be destroyed to preserve forward secrecy.



Generalizing to  $D$  dimensions, a sender can produce  $D$  initial chain keys. Each chain key but the first is derived from the preceding chain key using a distinct one-way function: these are the right-pointing arrows in the diagram above. Senders distribute all  $D$  chain keys to receivers who need them, except as noted below.



Legal values for  $D$  are positive powers of two less than or equal to the number of bits in the iteration counter: 1, 2, 4, 8, 16, and 32. Implementors select a value of  $D$  as an explicit CPU-memory (or CPU-network bandwidth) tradeoff.

If a chain key  $CK_j$  (for  $j$  in  $[1, D]$ ) has an iteration count of  $M$ , it cannot be used. This algorithm restores the chain keys to a usable state:

1. If  $j = 1$ , fail because the iteration count has reached its limit.
2. Derive  $CK_j$  from  $CK_{j-1}$
3. Ratchet  $CK_{j-1}$  once, recursing if necessary.

Moving from one iteration count to another never ratchets a single chain key more than  $M$  times. Therefore, no ratcheting operation takes more than  $D \times M$  steps.



Signal uses different functions for ratcheting versus message key computation, since both come from the same chain key. In this notation  $\{x\}$  refers to an array of bytes containing a single byte  $x$ .

$$\begin{aligned} \text{MK} &= \text{HmacSHA256}(\text{CK}_j(i), \{1\}) \\ \text{CK}_j(i+1) &= \text{HmacSHA256}(\text{CK}_j(i), \{2\}) \end{aligned}$$

Each dimension must use a different function. Keys are initialized as:

$$\begin{aligned} j = 1 &: \text{CK}_1(0) = \text{RNG}(32) \\ j > 1 &: \text{CK}_j(0) = \text{HmacSHA256}(\text{CK}_{j-1}(0), \{j+1\}) \end{aligned}$$

And ratcheted as:

$$\text{CK}_j(i) = \text{HmacSHA256}(\text{CK}_j(i-1), \{j+1\})$$

## Verifying Keys

WhatsApp users additionally have the option to verify the keys of the other users with whom they are communicating in end-to-end encrypted contexts so that they are able to confirm that an unauthorized third party (or WhatsApp) has not initiated a man-in-the-middle attack. This can be done by scanning a QR code, or by comparing a 60-digit number.

The QR code contains:

1. A version.
2. The user identifier for both parties.
3. The full 32-byte public `Identity Key` for both parties.

When either user scans the other's QR code, the keys are compared to ensure that what is in the QR code matches the `Identity Key` as retrieved from the server.

The 60-digit number is computed by concatenating the two 30-digit numeric fingerprints for each user's `Identity Key`. To calculate a 30-digit numeric fingerprint:

1. Iteratively SHA-512 hash the public `Identity Key` and user identifier 5200 times.
2. Take the first 30 bytes of the final hash output.
3. Split the 30-byte result into six 5-byte chunks.
4. Convert each 5-byte chunk into 5 digits by interpreting each 5-byte chunk as a big-endian unsigned integer and reducing it modulo 100000.
5. Concatenate the six groups of five digits into thirty digits.

## Transport Security

Communication between WhatsApp clients and WhatsApp chat servers is layered within a separate encrypted channel. On KaiOS, iPhone, and Android, those end-to-end encryption capable clients use Noise Pipes with Curve25519, AES-GCM, and SHA256 from the Noise Protocol Framework for long running interactive connections.

This provides clients with a few nice properties:

1. Extremely fast lightweight connection setup and resume.
2. Encrypts metadata to hide it from unauthorized network observers. No information about the connecting user's identity is revealed.
3. No client authentication secrets are stored on the server. Clients authenticate themselves using a Curve25519 key pair, so the server only stores a client's public authentication key. If the server's user database is ever compromised, no private authentication credentials will be revealed.

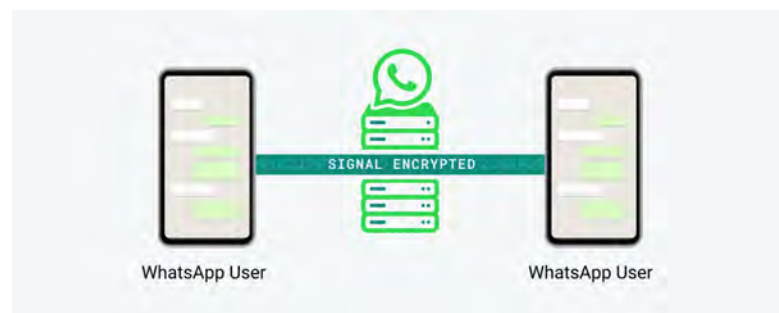
Note: In cases where a business user delegates operation of their Business API client to a vendor, that vendor will have access to their private keys - including if that vendor is Facebook. However, these private keys will still not be stored on the WhatsApp chat server. See below for details.

## Defining End-to-End Encryption

WhatsApp defines end-to-end encryption as communications that remain encrypted from a device controlled by the sender to one controlled by the recipient, where no third parties, not even WhatsApp or our parent company Facebook, can access the content in between. A third party in this context means any organization that is not the sender or recipient user directly participating in the conversation.

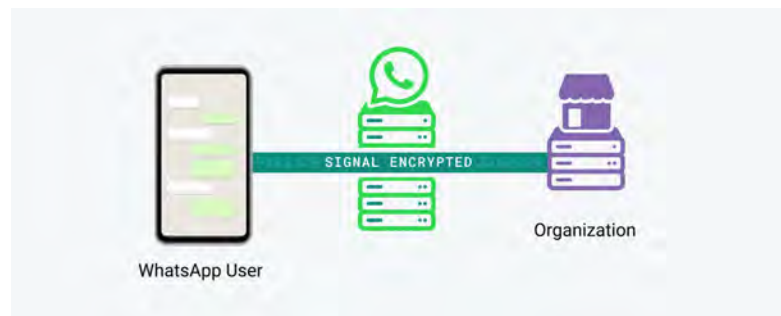
## Implementation on WhatsApp Services

This is straightforward when it comes to two people communicating on their phones or computers using WhatsApp Messenger or the WhatsApp Business App: each person's WhatsApp endpoint is running on a device they control.



Some organizations may use the WhatsApp Business API, an application that can be deployed as a WhatsApp endpoint on a server. The Business API allows those organizations to programmatically send and receive messages.

WhatsApp considers communications with Business API users who manage the API endpoint on servers they control to be end-to-end encrypted since there is no third-party access to content between endpoints.



Some organizations may choose to delegate management of their WhatsApp Business API endpoint to a vendor. In these instances, communication still uses the same Signal protocol encryption and clients on or after version v2.31 are configured to generate private keys within the vendor-controlled API endpoint. However, because the WhatsApp Business API user has chosen a third party to manage their endpoint, WhatsApp does not consider these messages end-to-end encrypted.



In 2021, organizations who use the Business API will be able to designate WhatsApp's parent company, Facebook, as the vendor that operates the Business API endpoint on their behalf. Since such messages are not delivered directly to an endpoint controlled by the organization, WhatsApp does not consider chats with organizations who choose to use Facebook to operate their API endpoint to be end-to-end encrypted.

## Encryption Has No Off Switch

All chats use the same Signal protocol outlined in this whitepaper, regardless of their end-to-end encryption status. The WhatsApp server has no access to the client's private keys, though if a business user delegates operation of their Business API client to a vendor, that vendor will have access to their private keys - including if that vendor is Facebook.

When chatting with an organization that uses the Business API, WhatsApp determines the end-to-end encryption status based only on the organization's choice of who operates its endpoint.

The encryption status of an end-to-end encrypted chat cannot change without the change being visible to the user.

## Displaying End-to-End Encryption Status

Across all our services, WhatsApp makes the end-to-end encryption status of a chat clear. If the user's phone sees that it's communicating with an API endpoint that delegates operation of its API to a vendor, the phone will display this to the user. The user can also double check the encryption status within the chat or in the business info section of their app.

These changes will take effect in all WhatsApp versions after January 2021.

## Conclusion

All WhatsApp messages are sent with the same Signal protocol outlined above, and WhatsApp considers all messages from a device controlled by the sender to one whose device is controlled by the recipient to be end-to-end encrypted. Communications with a recipient who elects to use a vendor to manage their API endpoint are not considered end-to-end encrypted. If this occurs, WhatsApp makes it clear to users within the chat.

The Signal Protocol library used by WhatsApp is based on the Open Source library, available here:

<http://github.com/whispersystems/libsignal-protocol-java/>

## Information for Law Enforcement Authorities

### About WhatsApp

WhatsApp provides messaging, Internet calling and other services to users around the world. You can learn more about WhatsApp by visiting our [Help Center](#).

WhatsApp appreciates the work law enforcement agencies do to keep people safe around the world. We are prepared to carefully review, validate and respond to law enforcement requests based on applicable law and policy.

The following operational guidelines are for law enforcement officials seeking records from WhatsApp. Users seeking information on their own accounts can access WhatsApp's [Request Account Info](#) feature. This information may change at any time.

### Responding to Law Enforcement Requests

In addition to this guide, law enforcement officials may also contact WhatsApp with questions or in emergency situations as detailed below. To ensure a timely response, please do not send law enforcement inquiries to WhatsApp Support or any other channel not intended for law enforcement.

### U.S. Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under U.S. law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include (if available): name, service start date, last seen date, IP address and email address.
- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include numbers blocking or blocked by the user, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include "about" information, profile photos, group information and address book, if available. In the ordinary course of providing our service, WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages, and undelivered messages are deleted from our servers after 30 days. WhatsApp offers end-to-end encryption for our services, which is always activated.
- We interpret the national security letter provision as applied to WhatsApp to require the production of only two categories of information: name and length of service.

### International Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law. Additionally, we will assess whether requests are consistent with internationally recognized standards including human rights, due process, and the rule of law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.

### Account Preservation

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. You may expeditiously submit formal preservation requests via the [WhatsApp Law Enforcement Online Request System](#) as indicated below.

## Emergency Requests

In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request via the [WhatsApp Law Enforcement Online Request System](#). For expedited processing of such requests, we recommend including the word "EMERGENCY" in the subject line of your message.

**Note:** We will not review or respond to requests submitted by non-law enforcement officials. Please submit emergency requests from an official government-issued email address. Users aware of an emergency situation should immediately contact their local law enforcement directly.

## Child Safety Matters

We report all apparent instances of child exploitation appearing on our service from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC), including content drawn to our attention by government requests. NCMEC coordinates with the International Centre for Missing and Exploited Children and law enforcement authorities from around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances in the request and include relevant NCMEC report identifiers to ensure that we are able to address these matters expeditiously and effectively.

## Data Retention and Availability

We will search for and disclose information that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve. We do not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service.

In the ordinary course of providing our service, WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages. Undelivered messages are deleted from our servers after 30 days. As stated in the [WhatsApp Privacy Policy](#), we may collect, use, preserve, and share user information if we have a good-faith belief that it is reasonably necessary to (a) keep our users safe, (b) detect, investigate, and prevent illegal activity, (c) respond to legal process, or to government requests, (d) enforce our Terms and policies. This may include information about how some users interact with others on our service. We also offer end-to-end encryption for our services, which is always activated. End-to-end encryption means that messages are encrypted to protect against WhatsApp and third parties from reading them. Additional information about WhatsApp's security can be found [here](#).

## Form of Requests

We will be unable to process overly broad or vague requests. All requests must identify requested records with particularity and include the following:

- The name of the issuing authority, badge or ID number of responsible agent, email address from a law enforcement domain and direct contact phone number
- The WhatsApp account number, including any applicable country codes
- More information about country codes is available in [this article](#).

## User Consent

If a law enforcement official is seeking information about a WhatsApp user who has provided consent for the official to access or obtain the user's account information, the user should be directed to obtain that information on their own from their account. Users can access WhatsApp's [Request Account Info](#) feature.

## Notification

WhatsApp reserves the right to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive.

### Testimony

WhatsApp does not provide expert testimony support. In addition, WhatsApp records are self-authenticating pursuant to law and should not require the testimony of a records custodian. If a special form of certification is required, please attach it to your records request.

### Cost Reimbursement

We may seek reimbursement for costs in responding to requests for information as provided by law. These fees apply on a per account basis. We may also charge additional fees for costs incurred in responding to unusual or burdensome requests. We may waive these fees in matters investigating potential harm to children, WhatsApp and our users and emergency requests.

### Submission of Requests

#### Online

Law enforcement officials may use the [Law Enforcement Online Request System](#) for the submission, tracking and processing of requests. A government-issued email address is required to access the Law Enforcement Online Request System.

Law enforcement officials seeking account records from WhatsApp must address their request to WhatsApp LLC.

#### Address

Attention: WhatsApp LLC, Law Enforcement Response Team

WhatsApp LLC

1601 Willow Road

Menlo Park, California 94025

United States of America

Law enforcement officials who do not submit requests through the [Law Enforcement Online Request System](#) should expect longer response times. Sending requests both electronically and via hard copy might also increase processing time.

#### Note:

- Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or proper service.
- We will not respond to correspondence sent by non-law enforcement officials to the addresses above.

### Updates to the Guidelines

WhatsApp may update this information periodically. Please consult the guidelines before making any request.

HELP CENTER

**NOTIFICATION**

New Delhi, the 11th April, 2011

**G.S.R. 314(E).**— In exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.:-

**1. Short title and commencement** — (1) These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette

**2. Definitions** — (1) In these rules, unless the context otherwise requires,--

- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (b) "Communication link" means a connection between a hyperlink or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document website or graphical element.
- (c) "Computer resource" means computer resources as defined in clause (k) of sub-section (1) of section 2 of the Act;
- (d) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
- (e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;



- (f) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;
- (g) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub section (1) section 70 (B) of the Act;
- (h) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
- (i) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
- (j) "User" means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

**3. Due diligence to be observed by intermediary** — The intermediary shall observe following due diligence while discharging his duties, namely : —

- (1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.
- (2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
  - (a) belongs to another person and to which the user does not have any right to;
  - (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
  - (c) harm minors in any way;
  - (d) infringes any patent, trademark, copyright or other proprietary rights;
  - (e) violates any law for the time being in force;
  - (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
  - (g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule: (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non-compliant information..

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

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for

investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

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

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force:

provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

[F. No. 11(3)/2011-CLFE]  
N. RAVI SHANKER, Jt. Secy.

**TRUE COPY**

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

1. **Short title and commencement** — (1) These rules may be called the Information Technology [Intermediaries Guidelines (Amendment) Rules, 2018. (2) They shall come into force on the date of their publication in the Official Gazette.
2. **Definitions** — (1) In these rules, unless the context otherwise requires,--
  - (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
  - (b) "Appropriate Government" means appropriate Government as defined in clause (e) of sub-section (1) of section 2 of the Act;
  - (c) "Communication link" means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item; the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element;
  - (d) "Computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
  - (e) "Critical Information Infrastructure" means critical information infrastructure as defined in Explanation of sub-section (1) of section 70 of the Act;
  - (f) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
  - (g) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
  - (h) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;
  - (i) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub-section (1) of section 70B of the Act;
  - (j) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
  - (k) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
  - (l) "User" means any person who accesses or avails any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary;

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.
3. **Due diligence to be observed by intermediary** — The intermediary shall observe following due diligence while discharging his duties, namely: —

- (1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person
- (2) Such rules and regulations, **privacy policy** ~~terms and conditions~~ or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

- (a) belongs to another person and to which the user does not have any right ~~to~~;
- (b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
- (c) harm minors in any way;
- (d) infringes any patent, trademark, copyright or other proprietary rights;
- (e) violates any law for the time being in force;
- (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
- (g) impersonates another person;
- (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
- (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.
- (j) threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;**
- (k) threatens critical information infrastructure.**

- (3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

Provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule(2):

- (a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

~~(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,<sup>1</sup>~~

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

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

(6) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

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

- (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.**

**(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**

---

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

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 authorised.

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

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

(11) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(12) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule (3) can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint;

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



MIT/79/077



**COAI Position on Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018”**

At the outset, we thank you and sincerely appreciate the opportunity provided to us to present our inputs on the Draft of “The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018” (“Draft Amendment”) which seeks to amend the Information Technology (Intermediary Guidelines) Rules, 2011 (“Intermediary Guidelines”) under the Information Technology Act, 2000 (“IT Act”).

We take this opportunity to introduce us as COAI which was constituted in 1995 as a registered society. COAI has emerged as the official voice of the digital communications industry that interacts directly with ministries, policy makers, regulators, financial institutions and technical bodies. Our membership comprises of *inter alia* telecom service providers, internet service providers, search engines, e-commerce companies, and also social media platforms who are classified as “intermediaries” under the Information Technology Act. Our members are key constituents of the digital ecosystem and are committed to working with the government to realise the vision of a Digital India.

It is critical that the exercise of amending the Guidelines which govern the responsibilities of Intermediaries for user-generated content should be in line with international norms. In this regard the regulations need to strike a careful balance between the rights and obligations of users and intermediaries, promoting and upholding Internet freedom while putting in place appropriate safeguards for the privacy and security of users. It is also important to ensure that there is enough protection built to prevent online dissemination of illegal and harmful content. Additionally, it is also important that the proposed guidelines are consistent with the existing laws, rules and regulations including the License conditions of the Telecom Service Providers and not in conflict with any of the same. Any requirement that is added should be reasonable and without added burden which is onerous in nature.

We believe that the Draft Amendment would run contrary to the Supreme Court ruling in *Shreya Singhal Vs Union of India* where the Supreme Court had significantly read down the statutory provisions and held that ‘knowledge’ under Section 79(3) of the IT Act would only mean knowledge by the intermediary pursuant to an order of a court of law. The Supreme Court of India has recently also upheld the fundamental right to privacy of individuals in the case of *KS Puttaswamy v. Union of India*, as a critical and essential component of the right to life and liberty under Article 21 of the Constitution of India. While upholding this right, the Supreme Court stated that any limitation on the right to privacy should satisfy the triple test of legality, necessity and proportionality.



The Draft Amendment proposes changes that could be detrimental to citizens, democracy and free speech. The amendments pose several critical impediments to the right to privacy of individuals as they fail to satisfy the three-tier test that has been laid down for this purpose. While all sub-rules under Rule 3 of the Intermediary Guidelines deal with the obligations that an intermediary must fulfil in order to claim safe harbour from prosecution, it is important for the language to be adequately clear and the obligations spelt out clearly. The lack of clarity in relation to the obligations under the Intermediary Guidelines could lead to inadvertent non-compliance resulting in arbitrary prosecution. Further, the lack of clarity shall also result in onerous obligations that are likely to potentially drive several intermediaries out of business in India and preclude the possibility of new intermediaries developing in the future.

In this context, we would like to offer our inputs on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018.

The draft rules use various terms such as 'any government agency', lawfully authorized government agency, appropriate government agency, government agencies who are legally authorized, in various provisions, which is creating confusion and ambiguity and is likely to lead to implementation challenges as well as monitoring challenges. It is suggested that the terminology be uniform, clear and unambiguous. We suggest that the term legally authorized and duly designated Government agencies may be used and, either the authorised agency be named, or it be made clear as to what would be the process and criteria for designating such government agencies.

## 1. Rule 3(2)

**The existing Rule 3(2) of the Intermediary Guidelines prescribes that intermediaries must inform their users not to host, display, upload, modify, publish, transmit, update or share certain type of content – failing which [under Rule 3(4)] such content could be removed and the user's access to respective resources and content could be terminated. The Draft Rules add two additional types of content that cannot be shared: (i) content that threatens public health or safety (promotion of cigarettes or any other tobacco products or consumption of intoxicants including alcohol and Electronic Nicotine Delivery Systems); (ii) content that threatens critical information infrastructure.**

### **COAI Response:**

We would like to submit that these two clauses of the Draft Rules have been drafted very broadly and should be removed for the reasons detailed below:

- i. **Ambiguity** - The Draft Amendment does not specify as to what would be 'threatening' to public health or safety and critical information infrastructure, or what would tantamount to 'promoting' intoxicants and thus fail to identify the particular kind of content that is meant to be restricted from publication. For example, would online content depicting a person holding a glass of liquor or smoking would be considered as "threatening" to public health or safety as

prescribed in the Draft Amendment. We submit that the restricted content be described clearly which will allow the intermediaries to communicate to the users in clear and unambiguous terms.

- ii. **Constitutionality** – The terms such as ‘threaten’ and ‘promotion’ suffer from the same kind of vagueness that Hon’ble Supreme Court cautioned against in the case of Shreya Singhal by striking down Section 66A of the IT Act and holding that they were likely to have a chilling effect on freedom of speech by intermediaries. The Hon’ble Supreme Court took note that vague restrictions are not only against the spirit of providing a safe harbour for intermediaries but also challenging to implement and enforce.
- iii. **Conflict with other Regulations:** We submit that depending on the issue and product/services involved, there would also be separate regulatory authorities, for example for food product, Foods Standards and Safety Authority (FSSA) is the sectoral regulator, who has already published independent guidelines regarding the health and safety of products coming under their domain. Another example is the Cable regulation Act, which states that no advertisement is permitted to be aired by the channels, if the same is prohibited by another body like ASCI. It is therefore submitted that, there are enough checks and balances already in place and the proposed regulation to that effect if not only in excess, but also may run in conflict with other sectoral regulations. Alternatively, it should be clearly established and stated in the Regulations of which Regulation will take precedence or all such ambiguities should be considered and removed.

## 2. Rule 3(4)

**The existing provision prescribes that intermediaries shall 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 intermediaries to inform their users regarding the above at least once every month.**

### COAI Response:

This provision places an unreasonable and disproportionate burden on intermediaries without any corresponding public benefit and should therefore be removed. Further, this amendment is not required as this provision is already incorporated in the terms and conditions of use of all websites, and mandating changes to the interface of all intermediaries across several jurisdictions for this purpose will be unduly onerous without serving any corresponding purpose. Further, this could lead to notice fatigue on the part of users and fail to have the intended impact i.e. to increase the awareness of this provision.

### 3. Rule 3(5)

The existing Rule 3(5) of the Intermediary Guidelines requires intermediaries to provide information or assistance when required by lawful order. The Draft Rules amend this rule significantly by changing the timelines and by mandating that any government agency can seek such data.

The Draft Rules also mandate intermediary to proactively trace the originator of the content as may be required by legally authorized government agencies in order to claim exemption from intermediary liability.

#### COAI Response:

We would like to submit that these two clauses of the Draft Rules should be removed or modified accordingly, for the reasons detailed below:

- i. **Time limit** - The Draft Rules mandate a time limit of 72 hours within which intermediaries are required to provide the information or assistance which is arbitrary; timing can vary as it depends on the nature, volume, scale, duration, historicity and type of information being sought. This duration is also unduly onerous as it does not allow the intermediaries the time to collate, review the legitimacy of the information request and respond appropriately. While the obligation on the intermediary comes with a strict time limit that has no specific justification, there is no corresponding obligation on the government agency as regards the specificity of the information or assistance being sought.

**Stop the Clock Provisions:** In all instances, the provision should also contain “Stop the Clock” provisions by listing out a set of criteria (such as seeking clarifications, technical infeasibility, etc.) under which the time limit would cease to apply to allow for due process and fair play in enforcing such requests.

- ii. To comply with the draft law intermediaries would need to put in place organisational measures that today may not be generally built-in due to various reasons. COAI suggests that the legality of the removal order should be open to and be determined through judicial review. More time should be provided to respond to the removal order itself. This is essential to give sufficient time to the hosting service provider to undertake the technical review to ascertain that the order is complete, can be carried out correctly, and possibly appeal the decision.
- iii. **Inadequate procedural safeguards** – This provision lacks any procedural safeguards (both in terms of defining the scope of “information and assistance”, as well as specifying which government agencies and specific

officers who can issue these requests, and for what purpose) and hence it is extremely prone to misuse.

**Vagueness** - The use of the term “or” before “assistance concerning security of state” etc. seems to imply that assistance can be sought by government agencies for any purpose, in addition to the security of state, cyber security, and related reasons. This indicates that there is no purpose limitation on the kind of assistance that may be sought. The term “any agency” also implies no limitations on who may seek such assistance.

- iv. **Provision for information requests already exists** - Information requests to help with criminal investigations are already addressed under existing criminal law and are applicable to intermediaries. There is no need for a separate process which contains fewer safeguards. In this regard, it is also important that the proposed guidelines are consistent with the existing telecom regulations of Department of Telecommunication (DoT), the security obligations under the Licence conditions and more importantly consistent with the existing telecom regulations of Department of Telecommunication (DoT), in this area.
- v. **Mode of communication of data requests** - The Draft Amendment includes requests made by electronic means. This provision should clearly specify the procedures that can be used by legally authorized and duly designated government agencies to communicate such orders for information or assistance in order to have a clear and transparent process. In this context, it is vital to note that the Manila Principles on Intermediary Liability specifically state that requests for restrictions of content must be clear, unambiguous and follow due process.
- vi. **Inconsistency:** The first part of new Rule 5 calls for intermediaries to respond to requests from ‘any government agency’ whereas earlier rules read “government agencies which are lawfully authorised for investigative, protective, cyber security activity.” Thus, this new rule expands the scope of which agencies can seek such information. This should be narrowed down to only the agencies lawfully authorised to do so. The last part of new Rule 5, however, restricts agencies to those which are legally authorised to do so. This creates an inconsistency and differential standards for requests for information.
- vii. **Tracing obligation poses multiple challenges** - The Draft Amendment also imposes an obligation on the intermediaries to enable tracing of originators of information, as required by government agencies.
  - a. **Technical Challenges** – We submit that this requirement would not be applicable to Telecom Companies as the same may not be practically possible to implement as in case of information that flows through a

series of intermediaries, each intermediary would only be able to assist to the extent of the origin of the information at their end. Alternatively, it is suggested that where the applicability is not possible, the carve outs should be provided.

- b. **Undermines security and privacy of communications** - This is deeply problematic from a privacy perspective and would be difficult to operationalise given that the intermediary does not control or monitor content. This obligation also undermines the use of encryption technology, which ensures that content is not accessible to the intermediary or third parties. Thus, placing the obligation of tracing on an intermediary creates a restrictive regime which seeks to dictate the underlying technology governing the intermediary's business, in addition to incentivising the development of technology that undermines globally recognised best practice for preserving the privacy and security of communications, in particular the deployment of robust encryption tools.
- c. **Lacking in procedural safeguards** - There are no procedural safeguards limiting the scope of the tracing request to ensure that the provision is not misused. In this context, it is important to note that the recent Supreme Court judgement on the Aadhaar Act, 2016, has ensured that unfettered access to citizen's data is not permitted even if data is sought for national security purposes. The Supreme Court has delineated a clear and a high standard of needing due process safeguards when it comes to accessing an individual's data even if it is for national security purposes. Thus, on similar grounds, the tracing requirement contemplated in the Draft Rule would not stand judicial scrutiny.
- d. **Technological changes** - From the perspective of the user, this constitutes a violation of their right to freedom of speech and expression, as well as their right to privacy, while from the perspective of the intermediary, this may impinge on their freedom of business and commerce as it may require the introduction of procedures to comply with these requirements that would potentially change several underlying technologies and business practices.

In this context, it is worth noting that several intermediary platforms are already working closely with the government in order to come up with the best ways to combine the interests of law enforcement with the business and technology operations of said intermediaries, we urge the government to follow international best practices in this regard. To proceed with the legally problematic approach outlined in the draft law could have restrictive impacts on such online platforms without giving rise to a corresponding public benefit.

#### 4. Rule 3(7)

**This provision of the Draft Rules prescribes that intermediaries with more than fifty lakh users in India or those notified by the Central Government must meet certain conditions, such as local incorporation, maintaining a permanent registered office in India, and appointing persons of contact in India for 24x7 coordination with law enforcement agencies.**

#### **COAI Response:**

The principle of “Same Service, Same Rules” relating to the Over-The-Top (OTT) services, needs to be applied so as to address the licensing, regulatory and security asymmetries between the two sets of services. COAI is of the firm view that bringing parity between the licensed telecom players and the OTT players offering any services that are permissible to the former, is essential, not only for fair business but also for addressing various national security concerns in terms of access to data/records and ensuring security, safety and privacy of the consumer data.

In this regard COAI supports the measures described under rule 3(7) which would ensure that online intermediaries which compete directly with licensed telecom service providers are subject to an equivalent level of regulation, and do not obtain a competitive advantage through the existence of regulatory safe harbours for online intermediaries.

The proposal that intermediaries over a certain size should meet certain conditions, such as local incorporation, maintaining a permanent registered office and appointing a local contact person are proportionate and necessary to ensure a level-regulatory playing field between competing service providers. As such we would lodge no specific objection to the inclusion of these measures in the draft Rules.

#### 5. Rule 3(8)

**Under this rule, the Draft Rules create an obligation on intermediaries to take down content upon a court order or being notified by the appropriate Government or its agency within 24 hours, where the content pertains to the restrictions under Article 19(2) of the Constitution. The Rules also extend the period of time that the information must be stored for, and even authorises government agencies to extend it further.**

#### **COAI Response:**

Our concerns on this are highlighted below:

- i. **No procedural safeguard** – There are no procedural safeguards built into content takedown notices by appropriate government. This rule contains a process for the removal or disabling of content but does not incorporate any

safeguards while creating this new process as it neither specifies who can pass the orders, nor does it require reasons to be recorded for such orders.

- ii. **Time Limit** – The Draft Amendment provides for an unreasonable time limit of 24 hours to implement orders of removing or disabling access to content. This time limit does not provide any opportunity to intermediary to review the order and ascertain whether it is legitimate or to identify the specific content which needs to be removed or disabled. Sufficient time should be given to the intermediary to: undertake the technical activities ensuring the order's completeness; make sure it can be carried out correctly; and avail of the possibility to appeal the decision. The required response time should be proportionate to the level of risk and exposure to illegal/harmful content of the platform. Hence, it is requested that existing sub-rule 4 of the 2011 intermediary rules be retained, which has specified the time limit as 36 hours.
- iii. **Storage of data** – When requiring service providers to preserve content for an undefined period lawmakers risk imposing new data retention requirements on telecom service providers. This would increase legal uncertainty and confront companies with new financial, logistical and technical challenges. There should be a time limit prescribed and it should be clarified that the storage is required for a maximum period (example - 180 days or 240 days) and longer periods should only be provided that there is a direction from the Court of Law or a lawfully authorized Government agency.
- iv. **Checks and balances to avoid misuse of the regulations and cost Sharing:** It is necessary that the regulations are not misused to enable individuals / Corporates to obtain court orders which benefits their commercial activity and ensure compliance through ISP's. It is important that there should be equal penal provision on the individuals/ corporates / authorities who may misuse or take advantage of this regulation.

## 6. Rule 3(9)

**Rule 3(9) of the Draft Rules mandates that intermediaries undertake proactive identification, monitoring and filtering of content through automated tools, as a pre-requisite for an intermediary to be able to claim exemption from liability.**

### COAI Response:

We recommend removing this for the reasons detailed below:

- i. **Violation of Fundamental Right to Privacy** - This creates a legal incentive for intermediaries to engage in overbearing censoring of content in order to retain legal immunity, thereby potentially censoring lawful content and violating the privacy of users.



- ii. **Contrary to Supreme Court Ruling** - The obligation of the intermediary to adjudicate content as unlawful, has been read down by the SC's decision in *Shreya Singhal v. Union of India*. This obligation is being re-introduced in the Draft Amendment, which goes against the Supreme Court mandate. 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 authorized government agency along the lines of the 'notice and take down' model applied via international best practice.
- iii. **Censorship role assigned to intermediaries** - By making intermediaries the monitoring bodies, the rule also places the responsibility for assessing the legality of speech and expression of users in the hands of private entities that are neither the Court nor authorized government agencies, contrary to what is envisaged by the IT Act, Supreme Court judgment in the *Shreya Singhal* matter, and the Manila Principles. We are concerned that this obligation amounts to the privatisation of law enforcement, and places upon intermediary's obligations which go well beyond their role as commercial entities. This will also lead to subjectivity and uneven implementation across intermediaries. As telecom operators, the telecom license conditions also state that *'once specific instances of such infringement are reported to the Licensee by the enforcement agencies/Licensor, the Licensee shall take necessary measures to prevent carriage of such messages in its network immediately.'*
- iv. **Blocking orders can be issued without any safeguards** - Section 69A of the IT Act and the rules notified thereunder already provide for a procedure of issuing blocking orders with specific processes and safeguards. The Draft Amendment seeks to introduce a parallel process for the same under Section 79 of the IT Act without providing for any safeguards.
- v. **Onerous** - Deployment of automated tools or appropriate mechanisms to monitor content is also extremely onerous as a precondition to getting safe harbour as it involves creating new technology or deploying additional resources with very little clarity on what would be the threshold of content monitoring that would meet the relevant criteria.
- vi. **Violation of international standards and Manila Principles** - The global best practices in intermediary guidelines are usually structured along the lines of the Manila Principles, which states that Intermediaries should be shielded from liability for third-party content stored and uploaded at the request of a user. This is the fundamental principle based on which any intermediary liability regime should be structured. Making intermediaries liable to monitor content would put India's legal regime out of step with global best practices.



- vii. **Contradiction:** The proposed amendment is in contradiction of the very definition of intermediaries under the IT Act, as intermediaries are only making available a communication link over which the information of the users is transmitted or temporarily stored/hosted.

In conclusion, we would like to submit that if the Draft Amendment were to come into effect in the present form, it would put India's legal regime significantly out of step with global best practices. Further, requiring intermediaries to deploy mechanisms to identify, filter, and remove access to unlawful content adds to the chilling effect to free speech and expression as the intermediaries may apply these measures too aggressively in the interest of legal compliance.

As COAI, we support the introduction of proportionate rules which incentivise operators of digital platforms to take more responsibility for the dissemination of illegal and harmful material on their sites. In the context of the draft rules, we believe that a sensible balance can be struck which does not penalise digital platforms for acting in a more responsible way.

Crucially any such measures need to be narrowly targeted at the Internet layer where the harm actually takes place: i.e. online platforms which allow for the upload of user generated content and the broad dissemination of illegal and harmful material. Such measures should expressly not apply to service providers involved in technical/passive activities ('mere conduits') who do not store or provide end users with the ability to access or share content with a wide audience on the public Internet. Thus providers of electronic communications services, caching services, enterprise cloud hosting services, content delivery networks and Internet registries should not be within scope.

We would urge that an opportunity of personal hearing be provided when our members can visit your good offices and explain our position with evidences and international best practices.

We look forward to your favourable consideration of our submissions made herein above.

**Please note that one of our members, Reliance Jio has divergent views on this issue and may respond separately.**



MIT/79/063

## Comments on “Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 ”

### Executive Summary

- I. The objective of the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (“the Draft Rules”) seems to be to counter disinformation / fake news on social media and messaging platforms (among other things like – circulation of obscene content and recruitment of terrorists). However, the Draft Rules have exceeded the power of delegated legislation and are violative of the fundamental rights to free speech and privacy.
- II. The obligations of intermediaries need to be classified based on their roles and their control over content. Mere conduits like TSPs cannot have the same obligations as a social media platform.
- III. The Draft Rules have gone against the dictum of the judgment of the Supreme Court in *Shreya Singhal v Union of India*. The broad list of information characterized as “unlawful” provided in Sub-Rule 2 of Rule 3 has terms and expressions that are vague and ambiguous and would result in violating the right to Freedom of Speech and expression of a citizen as guaranteed by the Constitution.
- IV. Restrictions on content/ speech cannot be beyond what is laid down in Art.19(2) of the Constitution. It was held in *Shreya Singhal* that “*Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79*”. Thus, the rules cannot mandate restrictions on content beyond those enumerated under Art.19(2) of the Constitution.
- V. Proactive monitoring of content is in effect a mandate on the intermediary to decide on the legitimacy of any content posted by a third party and this is violative of the fundamental right to freedom of speech and expression.
- VI. Traceability cannot be mandated as per these Rules as it is beyond the rule making power of the Government. No steps should be taken that violates the right to privacy of citizens and affects the security of users. Requirement of monthly notification will result in excessive communication from intermediaries to users and lead to consent fatigue.

We fear that the rationale for these proposed amendments to 'strengthen the legal framework and make the social media platforms accountable under the law', in the light of the spread of fake news, will not be served by such arbitrary and sweeping provisions. We request you to protect the principles of open and accessible internet, safe harbour granted to intermediaries and the fundamental rights of privacy and freedom of speech and expression of the internet users in India.

While being cognizant of national security interests, we appeal for a less-invasive and proportional means of regulation of the internet.

### **Summary of Recommendations**

- One size fits all approach for regulation of intermediaries is problematic and the obligation of intermediaries should be dependent on their role and the control that they have over content
- Intermediaries should be free to come out with their own Terms of Service and the content of such terms should not be mandated. Any restriction on content should not go beyond those laid out under Article 19(2) of the Constitution.
- The intermediary should not be required to actively monitor posted content using automated tools or any other mechanism.
- The intermediary should not be mandated to determine on its own whether any given content is legal or not.
- Fundamental right to privacy of users have to be protected and there should not be any mandate to weaken the encryption of communication tools.
- Traceability of user goes beyond the rule making power of the Government and cannot be mandated.
- Safeguards guaranteed under Section 69A should not be violated by these Draft Rules.

## Comments in Detail

The Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 (“the Draft Rules”), were issued by the Ministry of Electronics and Information Technology (“MeitY”) on the 24th of December, 2018. The Draft Rules seek to amend existing ‘due diligence’ guidelines [The Information Technology (Intermediaries Guidelines) Rules, 2011 (“the Current Rules”)] which are to be followed by ‘intermediaries’ [as per the Information Technology Act, 2000 (“IT Act”)]. Section 79 of the IT Act provides for a safe-harbour to intermediaries for, “*any third party information, data, or communication like made available or hosted by him*”. Intermediaries are required to observe due diligence while discharging their duties under the IT Act and observe guidelines as laid down by the Central Government.<sup>1</sup>

In a press note issued by MeitY,<sup>2</sup> it has been mentioned that social network platforms are required to follow due diligence as provided in Section 79 of the IT Act and the Rules notified therein, subject to the import of Article 19(2) of the Constitution. They have to ensure that their platforms are not used to commit and provoke terrorism, extremism, violence and crime. The press note also states that instances of misuse of social media platforms by criminals and anti-national elements have brought new challenges to law enforcement agencies, such as inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, incitement of violence, public order, fake news etc. The press note points to fake news / rumours being circulated on WhatsApp and other social media platforms for various mob-lynching incidents reported across India in the last year - “*A number of lynching incidents were reported in 2018 mostly alleged to be because of Fake News / rumours being circulated through WhatsApp and other Social Media sites.*” As MeitY has not issued any other official statement behind their intent in revising the intermediaries guidelines under the IT Act, the Draft Rules will have to be read in conjunction with the press note for a critical examination of the proposed changes therein.

Section 79 of the Act was introduced to provide a “safe harbour” for intermediaries to protect them from liability on account of user generated content. However, the Draft Rules could result in eroding this safe harbour. The Rules would have implications on social media and messaging platforms as well as community run platforms like Wikipedia and Diaspora. The Draft Rules in their current form could also have a chilling effect on free speech and infringe the privacy rights of

<sup>1</sup> Section 79(2)(c) of the IT Act, 2000.

<sup>2</sup> The press note issued by MeitY, available at <http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770>. Last accessed on 27 January 2019

citizens.

### **A. Obligation on Intermediaries remains same irrespective of roles**

At first instance, it is important to highlight the definition of the term ‘intermediary’ as per the IT Act, as the Draft Rules are applicable to only this category of service providers. Section 2(1)(w) of the IT Act defines an intermediary as - *“with respect to any particular electronic records, means 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-market places and cyber cafes.”* On a careful reading of the definition, it is clear that the following service providers are intermediaries as per the IT Act: (a) all social media platforms; (b) messaging services; (c) e-commerce marketplaces; (d) telecom and Internet service providers; (e) search engines; (f) web-hosting services; (g) online payment sites; and (h) cyber cafes (this is an indicative list and not an exhaustive list). All these service providers will be required to abide by the provisions of the Draft Rules as they are intermediaries as per the IT Act.

Most of the changes proposed by the Draft Rules, such as monthly notification requirement;<sup>3</sup> traceability of originator of information;<sup>4</sup> take down of content and preservation of information;<sup>5</sup> and deployment of automated tools for disabling content;<sup>6</sup> seem to be targeted toward a select group of intermediaries - social media platforms and messaging applications. This becomes clearer when read alongside the press note issued by MeitY on the Draft Rules.

The above listed requirements, by their very logic, don’t apply to other categories of intermediaries such as telecom service providers (“TSPs”), Internet service providers (“ISPs”), web hosting service providers and cyber cafes. Application of the Draft Rules to such intermediaries is disproportionate and doesn’t serve the purpose for which these changes are being introduced. This is one of the major concerns with incorporating requirements such as traceability of originator and proactive filtering of unlawful content within the Intermediaries Guidelines under the IT Act. Making the safe-harbour protection of certain intermediaries (like TSPs, ISPs and cyber cafes) conditional on requirements which they cannot adhere to is contrary and counter productive.

3 Rule 3(4) of the Draft Rules

4 Rule 3(5) of the Draft Rules

5 Rule 3(8) of the Draft Rules

6 Rules 3(9) of the Draft Rules

We recommend that MeitY should first identify the categories of intermediaries that the Draft Rules would apply to (such as social media platforms and messaging services) and then create separate conditions for distinct categories, so as not to have a blanket requirement for all intermediaries. As established, the definition of ‘intermediary’ is wide in its ambit. Due to the differences in the way that these unrelated intermediaries function, a one-size-fits-all approach to their regulation will lead to excessive regulation without appreciating the context of their operation. We recommend that the Draft Rules be tweaked to clarify the categories of intermediaries that different provisions would apply to, so that the guidelines become more coherent and consistent with the different roles played by dissimilar intermediaries in the digital sphere.

For an example of a regime which prescribes separate conditions for intermediary safe harbour based on the role the intermediary, we can look at EU’s Directive on electronic commerce (Directive 2000 / 31 / EC of the European Parliament and the Council).<sup>7</sup> Section 4 under Chapter II of the EU e-commerce directive prescribes conditions for the liability of intermediary service providers. Different conditions are applicable to distinct categories of intermediaries according to their functions. These are: intermediaries who are:

1. ‘mere conduits’: a service provider which merely provides access to a communication network (TSPs, ISPs and Web Hosting Service Providers);
2. engaged in caching services: intermediaries who temporarily store information for the sole purpose of making more efficient the information's onward transmission to other recipients of the service; and
3. providing hosting services: intermediaries who store information at the request of the recipient of service (social media platforms, online payment sites, market-places etc.).

According to the EU Directive on e-commerce, hosting service providers are liable only when they have actual knowledge of illegal activity or information and do not expeditiously remove content on obtaining such knowledge. This requirement doesn’t apply to providers of caching services and those that are mere conduits. In effect, conditions applicable to TSPs, ISPs and Web Hosting Service Providers for their safe harbour are not the same as those applicable to Social Media or Messaging Applications.

Regulations meant to make social media platforms and online communication applications more accountable for the information circulated on their services should not impose arbitrary conditions on all intermediaries in the digital realm. Doing so would result in an incoherent regulatory regime.

<sup>7</sup> The EU Directive on electronic commerce, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN>. Last accessed on 27 January 2019.

Appreciating the distinct roles played by various intermediaries in the online space, categorization of intermediaries based on their functions is the need of the hour.

## B. Ambiguous and vague terms

The Draft Rules contain mandates regarding a broad category of content that is classified as unlawful. Such a broad category of content described using terms such as “grossly harmful”, “harassing” and “blasphemous” could result in a chilling effect with intermediaries being forced to remove even lawful content. The Hon’ble Supreme Court had struck down Section 66A of the IT Act in *Shreya Singhal v Union of India*, (2015) 5 SCC 1.<sup>8</sup> However, terms used in Section 66A such as “grossly harmful” and “harassing” are still used in the Draft Rules. The Hon’ble Supreme Court held that “Section 66A is unconstitutionally vague” The Draft Rules have persisted with the same terminology that was found to be flawed by the Supreme Court and have thus ignored the dictum of the judgment.

The Hon’ble Supreme Court held that “It is obvious that an expression of a view on any matter may cause annoyance, inconvenience or may be grossly offensive to some. A few examples will suffice. A certain section of a particular community may be grossly offended or annoyed by communications over the Internet by “liberal views” such as the emancipation of women or the abolition of the caste system or whether certain members of a non proselytizing religion should be allowed to bring persons within their fold who are otherwise outside the fold. Each one of these things may be grossly offensive, annoying, inconvenient, insulting or injurious to large sections of particular communities and would fall within the net cast by Section 66A. In point of fact, Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the Section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total.”<sup>9</sup> Use of vague and ambiguous terms in the Draft Rules will lead to a chilling effect on free speech.

## C. Violation of Right to freedom of speech and expression

Article 19(1)(a) of the Constitution of India provides citizens the right to freedom of speech and expression. The broad set of unlawful material as listed in sub rule (2) of Rule 3 of the Draft Rules

<sup>8</sup> Available at <https://indiankanoon.org/doc/110813550/>. Last accessed on 29 January 2019.

<sup>9</sup> Paragraph 83 of *Shreya Singhal v. Union of India* [(2015) 5 SCC 1].



could restrict this freedom to a great extent.

The Hon'ble Supreme Court has held in *Express Newspapers (Private) Ltd. and Anr. Vs. The Union of India (UOI) and Ors. AIR 1958 SC 578* that if any limitation on the exercise of the fundamental right under Art. 19(1)(a) does not fall within the four corners of Art. 19(2), it cannot be upheld. The Hon'ble Court further held that there can be no doubt that freedom of speech and expression includes freedom of propagation of ideas.

In *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors (1995) 5 SCC 139*, the Hon'ble Supreme Court held that:

“Article 19(1)(a) not only guarantees freedom of speech and expression, it also protects the rights of an individual to listen, read and receive the said speech”.

The automated removal of content created by a user is a clear restriction of this freedom of speech and expression and can only be done if it falls under reasonable restrictions imposed under Art. 19(2) of the Constitution. Hence the broad list of information as listed in Sub-Rule (2) of Rule 3 characterized as unlawful is ultra vires of the Constitution of India.

#### **D. The Draft Rules are beyond the rule making powers of the Government**

Central Government obtains the source of power to issue these rules from the provisions of the IT Act. The rule making power has to be strictly confined to the boundaries specified as per the Act and cannot result in expanding the scope of the Act. Chapter XII of the IT Act (as amended) provides exemption from liability of intermediaries in certain cases. This exemption is subject to certain conditions to be observed by the intermediaries. The Government obtains the source of power to issue these rules from two provisions of the Act :

Section 79(2)(c) requires the intermediary to observe “*due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.*”

Section 87(2)(zg)– states that rules may provide for “*the guidelines to be observed by the intermediaries under sub-section (2) of section 79*”

Thus the rule making power of the Central Government is limited to prescribing other guidelines in this behalf. These guidelines can only be related to “due diligence” to be observed by the intermediary while discharging its duties under the Act.

The duties of an intermediary under the Act are restricted to the following:



1. Under Section 67C of the IT Act, the intermediary is required to “*preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.*”
2. Section 69 of the Act contains the power to issue directions for interception or monitoring or decryption of any information through any computer resource. Under Section 69(3), “*The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1) extend all facilities and technical assistance to—*
  - (a) *provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or*
  - (b) *intercept, monitor, or decrypt the information, as the case may be; or*
  - (c) *provide information stored in computer resource.*”
3. Section 69A of the IT Act contains provisions for blocking public access of any information through any computer resource. Under this Section, the intermediary is required to comply with such directions issued by “*the Central Government or any of its officers specially authorised by it in this behalf*”.
4. Section 69B of the IT Act contains provisions for monitoring and collecting traffic data or information through any computer resource for cyber security. Section 69B(2) states that “*The intermediary or any person in-charge of the computer resource shall, when called upon by the agency authorised, provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.*”

The Central Government can prescribe guidelines only in respect of the above duties of the intermediaries. But these rules have widened the scope of the IT Act by legislating on information that can be posted by a user and listing a broad category of information that can be considered as unlawful. This is not connected to the duties to be discharged by the intermediaries under the Act in any way. Sub-rules (2) and (7) of Rule 3 of the Draft Rules go beyond controlling intermediaries and result in controlling the users who post content.

The Hon'ble Supreme Court has held in *State of Karnataka and Anr. Vs. Ganesh Kamath and Ors.* (1983) 2 SCC 40 that:

*“it is a well settled principle of interpretation of statutes that the conferment of rule-*

*making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent there with or repugnant thereto”.*

The Hon'ble Supreme Court has held in *Agricultural Market Committee Vs. Shalimar Chemical Works Ltd.* (1997)5 SCC 516 that:

*“The delegate which has been authorised to make subsidiary Rules and Regulations has to work within the scope of its authority and cannot widen or constrict the scope of the Act or the policy laid down thereunder. It cannot, in the garb of making Rules, legislate on the field covered by the Act and has to restrict itself to the mode of implementation of the policy and purpose of the Act.”*

In view of the law as laid down in the aforementioned judgments, the Central Government has acted beyond its powers vested by the IT Act in framing the Draft Rules.

The rule making power of the Central Government is limited to due diligence of the intermediary **while discharging his duties under this Act** and also prescribing other guidelines **in this behalf**. These guidelines can only be related to “due diligence” to be observed by the intermediary while discharging its duties under the Act. But the Draft Rules have widened the scope of the Act by listing a much broader list of information that can be considered as unlawful. The definition of “due diligence” should be limited to having a policy, enforcing that policy and expeditiously removing infringing material when ordered by a court of law or the appropriate government.

#### **E. Burden on the intermediary**

The Draft Rules try to broaden the scope of the IT Act by placing burdensome obligations and restrictions on the intermediaries to proactively monitor user generated content which is not warranted by the IT Act. As provided in Sub-Rule 9 of Rule 3, the intermediaries have to deploy tools for removing unlawful content. Thus, the rules purport to burden the intermediaries with the obligation of deciding the unlawfulness of any content posted online, thereby according a judicial role which could only be done by a competent court. The Act specifies offences in the nature of civil as well as criminal offences. These have to proceed before the concerned forum. The intermediary cannot be burdened with a policing effort.

The Draft Rules have in effect tried to circumvent the *Shreya Singhal* judgment, wherein the Court read down Section 79(3)(b) and Rule 3(4) of the Information Technology (Intermediaries

Guidelines) Rules, 2011, interpreting the actual knowledge requirement to only mean a court order and/ or an order by the appropriate government or its agency, which must strictly conform to the standards laid down in Art. 19(2) of the Constitution. The automated system replaces the notice and take down requirement from the 2011 Rules that was read down with an automated system in respect of a broad set of unlawful information.

## F. Privacy of users and traceability

Rule 3(5) of the Draft Rules places an obligation on intermediaries to provide information and assistance to government agencies concerning the security of the state, cyber security, and investigation or prosecution of offences. This rule seeks to amend Rule 3(7) of the Current Rules by inserting changes such as:

1. Imposition of a time limit of 72 hours for providing assistance to government agencies;
2. Requirement to provide assistance to ‘any government agency’ from the erstwhile ‘government agencies who are lawfully authorised’;
3. Requirement to provide assistance to government agencies for ‘security of the state’;
4. Any request for assistance made by government agencies can now be sent through electronic means in addition to written requests; and most crucially,
5. *“The intermediary shall enable tracing out of originator of information on its platform as required by government agencies who are legally authorised.”*

To address the most sensitive part of these proposed changes i.e. the traceability requirement, it is important to reproduce the definition of the term ‘originator’ as per Section 2(1)(za):

*“Originator means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated stores, or transmitted to any other person by does not include an intermediary”*

The most concerning aspect of this requirement is how it will affect intermediaries like WhatsApp and Signal who provide personal communication services (over the Internet) which are end-to-end encrypted i.e. wherein even the service provider does not have access to the content of messages / information which flows through their platform. For reference, *“WhatsApp’s end-to-end encryption ensures only you and the person you’re communicating with can read what’s sent, and nobody in between, not even WhatsApp. Your messages are secured with locks, and only the recipient and you have the special keys needed to unlock and read your messages. For added protection, every*

*message you send has an unique lock and key.”<sup>10</sup>*

Introducing a traceability requirement for end-to-end encrypted services will lead to breaking of such encryption and thus compromising the privacy of individuals making use of such services for their private communication.

In August of 2017, a nine-judge bench of the Supreme Court in *KS Puttaswamy v. UOI*<sup>11</sup> (“the Privacy Judgment”), held that *“the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution.”* The judgment comprises of six different opinions, but at various points, the judges have held that informational and communicational privacy forms a part of the overall privacy of a person and unauthorised use or use of such information without the informed consent of users violates their privacy.

In his judgment, F. Nariman J. has stated that one of the aspects that a fundamental right to privacy would cover in the Indian context would be *“Informational privacy which does not deal with a person’s body but deals with a person’s mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of this right”*.<sup>12</sup> Similarly, SK Kaul J. opined that, *“The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed. Thus, for e.g. , if the posting on social media websites is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it.”*<sup>13</sup>

DY Chandrachud J. (for himself and three other judges) in his judgment stated that, *“Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well.”*<sup>14</sup> While discussing the various types of privacy, he observed that communicational and informational privacy are a part of nine primary types of privacy<sup>15</sup> - *“communicational privacy which is reflected in enabling an individual to restrict access to communications or control the use of information which is communicated to*

10 Explanation of the end-to-end encryption used by WhatsApp on its service, available at <https://faq.whatsapp.com/en/android/28030015/>. Last accessed on 28 January 2019.

11 WP (Civil) No. 494 of 2012, available at [https://www.sci.gov.in/supremecourt/2012/35071/35071\\_2012\\_Judgement\\_24-Aug-2017.pdf](https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf). Last accessed on 28 January 2019.

12 Id., Para 81 of Justice Nariman’s judgment.

13 Id., Para 70 of Justice Kaul’s judgment.

14 Id., Para 3(H) of the Conclusion to Justice Chandrachud’s judgment.

15 Id., Para 142 Justice Chandrachud’s judgment.

*third parties” and “informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information.”*

In Puttaswamy, the court also established a four-pronged test for the legitimate invasion of the fundamental right to privacy:<sup>16</sup>

- a) The action must be sanctioned by law;
- b) The proposed action must be necessary in a democratic society for a legitimate state aim;
- c) The extent of such interference must be proportionate to the need for such interference. There should be a rational nexus between the objects and the means adopted to achieve them; and
- d) There must be procedural guarantees against abuse of such interference.<sup>17</sup>

Thus, any regulation proposed by the Government, which has the purport of violating the privacy of individuals needs to pass this four-pronged test enunciated by the Supreme Court in the Puttaswamy judgment. The traceability requirement proposed under the Draft Rules, will not be a proportionate or necessary measure if it has the implication of breaking end-to-end encryption on messaging services. The Draft Rules also do not provide any procedural guarantees against the possible abuse of a process like traceability of originator of information, as required by the test laid down in the Puttaswamy judgment.

Section 69 of the IT Act gives powers to authorised representatives of Central and State Governments to intercept, monitor, or decrypt information stored in any computer resource<sup>18</sup> in the interest of sovereignty or integrity of India, defence of India, security of the State, public order or for investigation of any offence (among other things). The Rules which lay down the procedure and safeguards for such interception, monitoring and decryption of information<sup>19</sup> (“the Interception Rules”) authorise the Ministry of Home Affairs and the Home Department of the Central and State Governments respectively as the competent government authorities to issue order for such interception of information.<sup>20</sup> The traceability requirement under Rule 3(5) of the Draft Rules, if it intends to break encryption or request intermediaries for decryption of information then such

16 Id., Justice Chandrachud’s judgment representing 4 judges [Conclusion Para 3(H)] clubbed with Justice Kaul’s judgment (at Para 71), which forms the majority opinion of the Puttaswamy case on this point.

17 Id., Para 71 of Justice Kaul’s judgment.

18 The definition of ‘computer resource’ as per Section 2(1)(k) of the IT Act is: computer resource means computer, computer system, computer network, data, computer data, base or software.

19 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, available at <http://meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf>. Last accessed on 28 January 2019.

20 Id. at Rule 3.

powers already exist under a separate provision of the parent statute (i.e. as per Section 69 of the IT Act). The scope of decryption cannot be enlarged in subordinate legislation under a different provision (i.e. Section 79 of the IT Act in relation to the Draft Rules). Any changes addressing the decryption of information will necessarily have to be amendments to either Section 69 of the IT Act or / and the Interception Rules notified therein. Delegated legislation cannot go against the substantive provisions of the statute and they must be read in context of the primary / legislative act. In *ITW Signode India Ltd. v. Collector of Central Excise* [(2004) 3 SCC 48],<sup>21</sup> the Hon'ble Supreme Court stated that, "It is a well-settled principle of law that in case of a conflict between a substantive act and delegated legislation, the former shall prevail inasmuch as delegated legislation must be read in the context of the primary / legislative act and not the vice-versa."

Similarly, Section 69B of the IT Act deals with monitoring and collection of traffic data or information for the enhancement of cyber security in the country. The term 'traffic data' as defined under the Section 69B<sup>22</sup> includes any data identifying or purporting to identify any person, location to or from which the communication is transmitted and includes communications origin, destination and time (among other things). The The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 provide the procedure and safeguards for monitoring of traffic data under Section 69B. These Rules authorize MeitY to pass an order for such monitoring. In as much as Rule 3(5) of the Draft Rules pertains to cyber security, it cannot override and enlarge the scope of Section 69B or the Rules framed under it.

Lastly, the Draft Rules seek to expand the powers of the Government for law enforcement by replacing the phrase 'government agencies who are lawfully authorised' to 'any government agency'. Such expansion of the scope of powers of the Government for investigation or prosecution purposes go beyond the scope of the Intermediaries Guidelines Rules under Section 79 of the IT Act and are changes that need to form a part of the parent legislation. As argued, specific provisions of the IT Act provide for procedural safeguards for enabling access to information by law enforcement agencies. These safeguards are missing in the Draft Rules. The Draft Rules potentially go beyond the scope of Section 79 and other core provisions of the IT Act such as Section 69 and 69B of the IT Act.

In *National Stock Exchange Member v. Union of India* [125 (2005) DLT 165]<sup>23</sup> the High Court of Delhi held that, *"...in every legal system there is a hierarchy of laws, and the general principle is that if there is a conflict between a norm in a higher layer of the hierarchy and a norm in a lower*

21 Available at <https://indiankanoon.org/doc/1305345/>. Last accessed on 29 January 2019.

22 See Explanation appended to Section 69B of the IT Act.

23 Available at <https://indiankanoon.org/doc/876340/>. Last accessed on 29 January 2019.



level of the hierarchy, then the norm in the higher layer prevails, and the norm in the lower layer becomes *ultra vires*” the court elaborated on the hierarchy of laws as: 1) The Constitution of India; 2) Statutory Law; 3) Delegated Legislation; and 4) Administrative Instructions.

Thus, it is clear that subordinate / delegated legislation cannot go beyond the scope of the substantive provisions of the main law and in the hierarchy of laws, statutory law will always prevail over delegated legislation.

The government should have an encryption policy, which is lacking at the moment. The government should stop trying to slip through a back door what cannot be done through the front door.

Our recommendations for Rule 3(5) of the Draft Rules are:

1. A requirement of traceability will be in violation of informational privacy, which has been recognized as a fundamental right by the Supreme Court in the Puttaswamy judgment. Thus, we recommend that such a provision should be removed from the Draft Rules.
2. Proposed changes in delegated legislation should not undermine substantive provisions of the IT Act (specifically, Section 69 and 69B of the IT Act). They should not go beyond the purport of their parent provision (Section 79 of the IT Act); and
3. The phrase ‘any government agency’ should be removed and the current language of ‘government agencies who are lawfully authorised’ should remain.
4. This Rule is beyond the ambit of Section 79 of the IT Act. Addition of a requirement of traceability in a subordinate legislation is beyond the rule-making power of the Government.

### **Local Office, Incorporation and Appointment of Nodal Officer**

Rule 3(7) of the Draft Rules requires all intermediaries with more than 5 million users in India to be incorporated, have a permanent registered office in India with a physical address and appoint a nodal officer and a senior functionary for 24-hour coordination with Law Enforcement Agencies (“LEA”). The Current Rules do not have such obligations.

There is ambiguity regarding the meaning of “users” under this Rule. This Rule applies to all intermediaries with more than 5 million (50 lakh) users in India. At present there is lack of clarity about what this number of users refers to i.e. whether it refers to daily, monthly or yearly users, or the number of total registered users. To understand the implication of this requirement, reference to the user base of popular messaging apps is pertinent. WhatsApp, India’s most popular chatting app, has around 200 million users in India. Relatively newer chatting applications Hike and ShareChat

have 100 million users<sup>24</sup> and 25 million users respectively.<sup>25</sup> The 5 million users specified in the Draft Rules represent a little more than 1% of the Internet user base in India<sup>26</sup> which might bring a substantial number of intermediaries under a new set of compliance requirements. This may cause many start-ups to bear the brunt of high costs stemming from incorporation under Companies Act, 2013.

The Draft Rules stipulate appointment of different officers to ensure compliance with the orders / requisitions by law enforcement agencies in accordance with provisions of law or rules. To meet this objective, Draft Rule 3(7) requires the intermediary to appoint a nodal officer and a senior functionary for 24-hour coordination with LEA. Draft Rule 3(12) also mandates the appointment of grievance officer to address the complaints against violation of Draft Rule 3. Multiple appointments may increase procedural burdens for intermediaries and create possibilities of overlap in their functions.

We recommend:

1. To avoid confusion created due to multiplicity of authorities, a single officer can be appointed to fulfil compliance with the obligations;
2. The provision requiring incorporation of intermediaries can lead to compliance burden and should be made voluntary for intermediaries; and
3. Vietnam recently passed the Cybersecurity Law, which requires intermediaries to set up physical offices in the form of a representative office or branch within the country's jurisdiction in order to fulfil their cybersecurity obligations. The law does not require incorporation. Such alternatives can be explored in India.

### **G. 'Unlawful Information' and 'Proactive Content Filtering'**

Rule 3(9) creates a positive obligation (by use of the words “shall” and “proactive monitoring”) on intermediaries to remove content. This implies that even without a court order, intermediaries have to actively search and filter content that is ‘unlawful’.

Online intermediaries are considered channels of distribution that play a merely neutral, technical and non-adjudicatory role. The Rule requires intermediaries to scrutinize user generated content and

24 Hike unbundles its messaging app to reach India's next wave of smartphone users, available at <https://techcrunch.com/2018/01/16/hike-unbundles-its-messaging-app/>. Last accessed on 30 January 2019.

25 ShareChat: The no-English social media app that Indian politicians are flocking to, available at <https://scroll.in/article/897154/sharechat-the-no-english-social-media-app-that-indian-politicians-are-flocking-to/>. Last accessed on 30 January 2019.

26 According to the Mobile Internet Report, IAMAI, 2017 there are 456 million mobile Internet users in India.



determine its legality - a task which must be undertaken by the judiciary considering that there are no clear standards of what is 'unlawful'. This provision of proactive content filtering is against the judgment in *Shreya Singhal v. Union of India*, wherein the Supreme Court had held that intermediaries are neutral platforms that do not need to exercise their own judgment to decide what constitutes legitimate content. The Council of Europe's recommendation on the role of Internet intermediaries asserts that that 'illegal content' should be determined either by law or by a judicial authority or other independent administrative authority whose decisions are subject to judicial review.<sup>27</sup> The Global Network Initiative (GNI) in its statement<sup>28</sup> on the 'Terrorist Content Regulation', EU's proposed law to prevent the dissemination of 'terrorist content', has highlighted how definitional issues are likely to lead to legal uncertainty as well as potentially overly-aggressive interpretations by companies that could result in the removal of content that should be protected.

The United Nations Special Rapporteur on the protection of the right to freedom of opinion and expression, right to privacy and protection of human rights and fundamental freedoms, in a letter to the Commission of the European Union, raised grave concerns about the 'Terrorist Content Regulation' that stipulates proactive monitoring of content using automated tools. The letter stated that a 'general monitoring obligation will lead to the monitoring and filtering of user generated content at the point of upload. This form of pre-screening would enable the blocking of content without any form of due process even before it is published, reversing the well established presumption that States, not individuals, bear the burden of justifying restrictions on freedom of expression.'<sup>29</sup>

Implementation of the Rule will lead to massive private censorship as intermediaries will over-censor content to retain their safe-harbour protection under Section 79 of the IT Act. We recommend that 'unlawful' content should be restricted to acts mentioned under Article 19 (2).

## H. Automated Tools

Rule 3(9) mandates deployment of technology based automated tools by intermediaries to

27 Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of Internet intermediaries, available at [www.coe.int/cm](http://www.coe.int/cm). Last accessed on 30 January 2019.

28 Statement on Europe's Proposed Regulation on Preventing the Dissemination of Terrorist Content Online, available at <https://globalnetworkinitiative.org/wp-content/uploads/2019/01/GNI-Statement-Proposed-EU-Regulation-on-Terrorist-Content.pdf>. Last accessed on 30 January 2019.

29 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, available at <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=24234>. Last accessed on 27 January 2019.

proactively monitor content. The Council of Europe in their latest recommendation on the role and responsibility of Internet intermediaries has mentioned that States should take into account the fact that automated means, which may be used to identify illegal content, currently have a limited ability to assess context. Such restrictions should not prevent the legitimate use of identical or similar content in other contexts.<sup>30</sup> The recommendation also states that any restriction of content should be carried out using the least restrictive technical means and should be limited in scope and duration to what is strictly necessary.

The recent letter<sup>31</sup> by Special Rapporteurs to the Commission of EU has also warned against the use of automated content tools to take down content. It states that due to AI's inadequate understanding of context, the use of automated tools comes with serious limitations and aggravates the risk of pre-publication censorship. It further mentions that even the use of algorithms with a very high accuracy rate potentially results in hundreds of thousands of wrong decisions leading to screening that is over-inclusive or under-inclusive.

Automated moderation systems that are in use today rely on keyword tagging which is then followed by human review. Even the most advanced automated systems cannot, at the moment, replace human moderators in terms of accuracy and efficiency. This is mainly because artificial intelligence is currently not mature enough to understand the nuances of human communication such as sarcasm and irony.<sup>32</sup> It should also be noted that global communication is influenced by cultural differences and overtones which an effective system of content moderation has to adapt to, and given the amateurish stage at which AI is at the moment, it may be short sighted to rely on this technology.

As our societies evolve and change, so does the definition of “grossly harmful / offensive content”. This implies that algorithms have to constantly understand nuanced social and cultural context that varies across regions. Research on AI has not yet produced any significant sets of data for this kind of understanding. The immediate result of using automated tools will be an increase in content takedowns and account suspensions which in turn will lead to over-censorship as has been seen around the world. Legitimate users (content creators) including journalists, human rights activists and dissidents will have their speech censored on a regular basis.

YouTube’s “Content ID” system for detecting content that infringes copyright has been deemed

30 See footnote 27.

31 See footnote 29.

32 Despite What Zuckerberg’s Testimony May Imply, AI Cannot Save Us, available at <https://www.eff.org/deeplinks/2018/04/despite-what-zuckerbergs-testimony-may-imply-ai-cannot-save-us/>. Last accessed on 30 January 2019.

notorious for over-censoring innocent material. Use of AI without human intervention for detecting hate speech, misinformation, disinformation, trolling, etc which is even more nuanced than identifying copyrighted material will be catastrophic for freedom of speech and expression on the Internet.

The key limitations of natural language processing tools are:<sup>33</sup>

1. Natural language processing (“NLP”) tools perform best when they are trained and applied in specific domains, and cannot necessarily be applied with the same reliability across different contexts;
2. Decisions based on automated social media content analysis risk further marginalizing and disproportionately censoring groups that already face discrimination. NLP tools can amplify social bias reflected in language and are likely to have lower accuracy for minority groups who are under-represented in training data;
3. Accurate text classification requires clear, consistent definitions of the type of speech to be identified. Policy debates around content moderation and social media mining tend to lack such precise definitions;
4. The accuracy and intercoder reliability challenges documented in NLP studies warn against widespread application of the tools for consequential decision-making; and
5. Text filters remain easy to evade and fall far short of humans’ ability to parse meaning from text.

Recognising the shortcomings of automated tools, Article 22(1) of the European Union’s General Data Protection Regulation states that *“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”*<sup>34</sup> Automated removal of content that falls under freedom of speech and expression would produce a legal effect and could significantly affect such a person.

We recommend that the requirement of deploying automated tools for proactive content filtering should be removed from the Draft Rules.

33 Mixed Messages? The Limits of Automated Social Media Content Analysis Presented at the 2018 Conference on Fairness, Accountability, and Transparency, Natasha Duarte Emma Llansó (Center for Democracy & Technology), Anna Loup (University of Southern California), available at <https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf>. Last accessed on 30 January 2019.

34 Article 22 of the European Union’s General Data Protection Regulation, available at <https://gdpr-info.eu/art-22-gdpr/>. Last accessed on 30 January 2019.

## I. Lack of safeguards

Section 69A of the IT Act provides for power to the Central Government to block public access of any information through any computer resource. The blocking of content can be resorted to by the Central Government in cases where it is necessary to do so in the interest of sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to the above. Thus, the blocking of sites are permitted only in the case of exemptions to Freedom of speech provided as per Article 19(2) of the Constitution of India.

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 have been notified by the Central Government to provide the procedure and safeguards for such blocking. These Rules provide a detailed procedure for blocking of access with a designated officer not below the rank of a Joint Secretary entrusted for the purpose of issuing direction for blocking.

It is clear from the provision of Section 69A that the legislature aimed to have sufficient safeguards in place for blocking of the content. These safeguards are not present in the Draft Rules. We recommend ensuring that these safeguards are not violated by any amendment to the Rules.

## J. Notice and Consent fatigue

Rule 3(4) of the Draft Rules requires intermediaries to notify their users ‘at least once every month’ of their privacy policies and user agreements, non compliance of which will result in termination of access and removal of non-compliant content. This requirement of monthly notification is an addition to the Current Rules and will lead to excessive communication from intermediaries to users. Such a notification requirement will lead to consent / user fatigue (excessive content / user notifications leads to dilution of meaningful and informed consent). Consent / user fatigue is a problem that was identified in the report of the ‘Committee of Experts under the Chairmanship of Justice BN Srikrishna’ (“the Report”) which was tasked to draft India’s Personal Data Protection Bill. The Report mentions that, “*There is undoubtedly some truth in excessive consent requirements desensitising individuals towards consent.*”<sup>35</sup> The Report points to a problem that user fatigue will result in desensitising individuals to privacy harms and will not achieve the goal of informed consent - “*...constant intimations for consent may affect user experience and desensitise individuals*

35 Last paragraph of Page 39 of the Srikrishna Report, available at [http://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf). Last accessed on 29 January 2019.

to privacy harms.”<sup>36</sup>

If the intent behind introducing this requirement is to meaningfully communicate to users their terms of use and privacy agreements, then mandatory monthly notifications will not solve this problem, rather it will prove to be a counter-productive tool and desensitise users to their obligations and possible privacy harms from using services. The issue of consent / user fatigue should be addressed by MeitY under the Personal Data Protection Bill and mechanisms such as better privacy policy designs and effective notification measures such as - dashboards may be looked at (as recommended by the Srikrishna committee in its Report)<sup>37</sup>

It is also important to point out that the notice and consent model could be used to disclaim liability on the part of the intermediaries, hence for meaningful communication of user agreements and privacy policies (notice requirements) the validity of consent must be carefully determined. “...consent should be freely given, informed and specific to the processing of personal data.”<sup>38</sup>

There is a concern that genuine messages regarding changes in the terms of service / privacy policy / other documents regarding conduct on the platform would get lost in the barrage of notifications regarding the requirement of compliance with the standard terms. Users are likely to start ignoring these notifications entirely, without having any knowledge about the differences regarding permissible content on different platforms.

We recommend that the requirement of monthly notification should be removed from the Draft Rules as it will not serve the purpose for which it is being introduced.

#### **K. Public health or safety**

Rule 3(2)(j) prohibits various alcohol and nicotine-based products. There is no known precedent for banning such categories of content altogether in any medium. There are certain restrictions on the display of such content in motion pictures and there are prohibitions in place against advertising such products, but such content is not banned altogether. The sub-clause, in its current form, can be interpreted to include activities that go beyond advertisement of such content, such a photograph containing consumption of alcohol by a user of a social media platform.

If this sub-clause is retained in any form, then the terms used in this sub-rule need to be changed in order to better reflect their intent, i.e. to ban only advertisement of these products,

<sup>36</sup> Id. at page 40.

<sup>37</sup> Id. at pages 38-39.

<sup>38</sup> Id. at page 26, last paragraph of the page.

Our recommendation is to remove this sub-clause entirely as it violates the freedom of speech and expression guaranteed under the Constitution of India.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018  
(Published by MeitY)

## Rule-Wise Comments

### Rule 3. Due Diligence observed by intermediary

#### Sub-Rule 1

The one size fits all treatment of intermediaries is problematic as the functions of each class of intermediaries like Telecom Service Providers, caching services and social media platforms are different. The obligations cast on each intermediary has to be based on its role and the kind of control it has over content.

#### Sub-Rule 2

The rule lists a range of information that users are prevented from displaying, uploading, or sharing through an intermediary. The provision is against the dictum laid down by the Supreme Court in the *Shreya Singhal* judgment that “Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79”. The broad list of information deemed to be unlawful goes beyond the restrictions as per Article 19(2) and is unconstitutional. Moreover, the terms and expressions used are vague and ambiguous.

#### Sub-Rule 4

Rule 3(4) of the Draft Rules requires intermediaries to notify their users ‘at least once every month’ of their privacy policies and user agreements, non compliance of which will result in termination of access and removal of non-compliant content. This requirement of monthly notification is an addition to the Current Rules and will lead to excessive communication from intermediaries to users. Such a notification requirement will lead to consent / user fatigue (excessive content / user notifications leads to dilution of meaningful and informed consent).

It is our recommendation that the requirement of monthly notification should be removed from the Draft Rules as it will not serve the purpose for which it is being introduced.

**Sub-Rule 5**

The rule as explained earlier could result in violation of the right to privacy of users and thus should be removed.

**Sub-Rule 7**

The rule lacks clarity as to how the number of users is determined in the case of an intermediary as the users could be registered users or average active users per day / month / year. Moreover, the stipulation for incorporation of the entity puts onerous burden on the intermediary.

**Sub-Rule 8**

This Sub-Rule has been modified as per the judgment in *Shreya Singhal*. However, the norm for retention of records should be to keep the least amount of data and for the least amount of time based on the purpose for which the data is being kept. There should not be any requirement to store data any longer than necessary.

**Sub-Rule 9**

Automated tools, especially when these are mandated to filter content deemed illegal under the broad categories stipulated under Sub Rule 3, will lead to muzzling of free speech and result in chilling effect. This restriction is clearly violative of the fundamental right to freedom of speech and expression and goes beyond the restrictions that can be imposed under Article 19(2) as laid down in *Shreya Singhal v UOI* and *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors.*

Sub-Rule (9) of Rule 3, by providing for automated tools to filter content without laying down any procedures and safeguards, results in violation of a citizen's right to freedom of speech and expression.

**Sub-Rule 12**

The notifications to the designated agent may be restricted only to infringements in the case of Trademarks and Copyright, and in the case of other unlawful activities, when supported by an order from a competent court or appropriate Government.


**TRUE COPY**




MIT/79/050

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)<sup>1</sup> and the right to privacy under international law. The bench in *Puttaswamy* laid down the test for "**proportionality and legitimacy**"<sup>2</sup> 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<sup>3</sup> ("**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.<sup>4</sup>

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

<sup>1</sup> Justice K. S. Puttaswamy (Retd) & Another v. Union of India & Ors (2017), Writ Petition (Civil) 494 of 2012.

<sup>2</sup> Concurring opinion of Justice Sanjay Kishan Kaul, Paragraph 71, Page 37, *ibid*.

<sup>3</sup> International Principles on the Application of Human Rights to Communications Surveillance, <https://necessaryandproportionate.org/principles>.

<sup>4</sup> 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](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](http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf).

<sup>5</sup> 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](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<sup>6</sup> 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”.<sup>7</sup> 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

<sup>6</sup> 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/freedomofexpression/pages/callforsubmission.aspx>.

<sup>7</sup> 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),<sup>8</sup> 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<sup>9</sup> 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.**

<sup>8</sup> *Shreya Singhal v. Union of India*, Writ Petition (Criminal) No. 167 of 2012.

<sup>9</sup> 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*.**

## TRUE COPY

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.<sup>10</sup>

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.<sup>11</sup> These tools are far from being neutral, and in fact encode societal discrimination and unfairness into inscrutable systems.<sup>12</sup> As we have shown through previous research,<sup>13</sup> 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.

<sup>10</sup> 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/>.

<sup>11</sup> Safiyah Umoja Noble, *Algorithms of Oppression: How search engines reinforce racism*, 2018. New York University Press, New York.

<sup>12</sup> Virginia Eubanks, *Automating Inequality: How high tech tools profile, police, and punish the poor*, Page 190, January 2018. St. Martin’s Press, New York.

<sup>13</sup> 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](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240384).

MIT/79/084



## 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<sup>1</sup>

#### 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)<sup>2</sup>. 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,<sup>3</sup> to which this government has declared its commitment<sup>4</sup>.

<sup>1</sup> Authored by **Sarvjeet Singh** with assistance from **Yesha Tshering Paul** and inputs from **Shrutanjaya Bhardwaj**, **Smitha Krishna Prasad** and **Ujwala Uppaluri**.

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

<sup>3</sup> 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 violate 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,<sup>5</sup> and to make the social media platforms accountable under the law.<sup>6</sup> However, the proposed rules apply to all intermediaries<sup>7</sup> irrespective of their specific role or nature<sup>8</sup>.

“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.*<sup>9</sup>

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.<sup>10</sup> However, others have

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

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

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

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

<sup>8</sup> See Chinmayi Arun and Sarveet 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).

<sup>9</sup> The Information Technology Act, 2000, s. 2(1)(w).

<sup>10</sup> 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.<sup>11</sup>

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<sup>12</sup> 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”.<sup>13</sup> 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)<sup>14</sup> 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.<sup>15</sup> The power to make changes in policy is an essential function and cannot be delegated.

<sup>11</sup> Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

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

<sup>13</sup> 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/>.

<sup>14</sup> 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).

<sup>15</sup> 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](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.<sup>16</sup>

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.<sup>17</sup> Moreover, delegated legislation should conform to the parent statute and cannot exceed the scope of enabling act.<sup>18</sup>

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.<sup>19</sup>

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.<sup>20</sup>

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.<sup>21</sup> The current due diligence

<sup>16</sup> *Avinder Singh v. Punjab*, (1979) 1 S.C.C. 137.

<sup>17</sup> *Agriculture Market Committee v. Shalimar Chemical Works Ltd.*, (1977) 5 S.C.C. 516.

<sup>18</sup> See *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C. 641; *State of Karnataka v. Ganesh Kamath*, (1983) 2 S.C.C. 40. See also Ujjwala 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>.

<sup>19</sup> *K.T. Plantation Pvt. Ltd. v. State of Karnataka*, (2011) 9 S.C.C. 1.

<sup>20</sup> 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.

<sup>21</sup> 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 Sarvejit 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.<sup>22</sup> 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.<sup>23</sup> 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.<sup>24</sup>

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).

<sup>22</sup> *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 119.

<sup>23</sup> *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 122 and 124.3.

<sup>24</sup> *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).<sup>25</sup> 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.<sup>26</sup> Many of the terms listed under Rule 3(2) are subjective and not defined either in the current version of 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*.<sup>27</sup> Majority of the remaining terms are nebulous in nature<sup>28</sup> and provide no opportunity to know what is prohibited.<sup>29</sup> 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.<sup>30</sup>

<sup>25</sup> See Ujjwala 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>.

<sup>26</sup> *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.

<sup>27</sup> *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 85.

<sup>28</sup> *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 79.

<sup>29</sup> *Kartar Singh v. State of Punjab*, (1994) 3 S.C.C. 569, ¶¶ 130-131.

<sup>30</sup> 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”<sup>31</sup>, “obscene”<sup>32</sup>, “pornographic”<sup>33</sup>, and “pedophilic”<sup>34</sup>, Rule 3(2)(i) – “threatens the integrity, defense, security or sovereignty and of India”<sup>35</sup>, “friendly relations with foreign states”<sup>36</sup>, “public order”<sup>37</sup>, “incitement to commission of any cognizable offence”<sup>38</sup>, Rule 3(2)(j) – “threatens public health”<sup>39</sup> and “safety”<sup>40</sup> and Rule 3(2)(k) – “threatens critical information infrastructure”<sup>41</sup>. 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<sup>42</sup> and a threat to critical information infrastructure must meet the very high threshold of the security of state standard.

<sup>31</sup> Will fall under the “defamation” ground, the Constitution of India, 1950, art. 19(2).

<sup>32</sup> Will fall under the “decency or morality” ground, the Constitution of India, 1950, art. 19(2).

<sup>33</sup> Will fall under the “decency or morality” ground, the Constitution of India, 1950, art. 19(2).

<sup>34</sup> Will fall under the “decency or morality” ground, the Constitution of India, 1950, art. 19(2).

<sup>35</sup> 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).

<sup>36</sup> Will fall under the “friendly relations with foreign States” ground, the Constitution of India, 1950, art. 19(2).

<sup>37</sup> Will fall under the “public order” ground, the Constitution of India, 1950, art. 19(2).

<sup>38</sup> Will fall under the “incitement to an offence” ground, the Constitution of India, 1950, art. 19(2).

<sup>39</sup> 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”.

<sup>40</sup> 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”.

<sup>41</sup> Will fall under the “the security of the State” or presumably “public order” grounds, the Constitution of India, 1950, art. 19(2).

<sup>42</sup> See CHINMAYI ARUN, ARPITA BISWAS AND PARUL SHARMA, HATE SPEECH LAWS IN INDIA 14-16 (2018); Sarvejit 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<sup>43</sup>, 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”.

<sup>43</sup> 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<sup>44</sup> 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<sup>45</sup>, 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<sup>46</sup> 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*

<sup>44</sup> The Information Technology Act, 2000, s. 2(1)(za).

<sup>45</sup> 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.

<sup>46</sup> *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 in 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<sup>47</sup> 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.<sup>48</sup>

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

<sup>47</sup> The Information Technology Act, 2000, s. 2(1)(za).

<sup>48</sup> 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](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.<sup>49</sup>

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*<sup>50</sup>, 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,<sup>51</sup> 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<sup>52</sup>, 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

<sup>49</sup> 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).

<sup>50</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (Bobde, J., sep. op.).

<sup>51</sup> *Union of India v. Association for Democratic Reforms*, 2002 (3) S.C.R. 294.

<sup>52</sup> For an analysis of safeguards under Section 69 and Section 69B of the Information Technology Act, 2000 see Chinmayi Arun and Sarvejit 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*<sup>53</sup>, nor would it meet the new standard of proportionality adopted in respect of privacy in *Puttaswamy*<sup>54</sup>.

▫ **EXCESSIVE DELEGATION**

Sections 69 and 69B of the Act read with their respective subordinate legislations<sup>55</sup> 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 statute, can also be challenged for being contrary to other statutory provisions.<sup>56</sup> 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

<sup>53</sup> *State of Madras v. V.G. Row*, (1952) S.C.R. 597.

<sup>54</sup> *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).

<sup>55</sup> 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.

<sup>56</sup> *India Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 S.C.C. 641. See Ujjwala 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<sup>57</sup>, and this number is probably over 600 million currently<sup>58</sup>. 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.<sup>59</sup> The right to freedom of speech and expression includes the right to receive information<sup>60</sup>, and the court has held the right to a diverse media environment as an integral part of Article 19(1)(a) of the Constitution.<sup>61</sup> 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<sup>62</sup> 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

<sup>57</sup> 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>.

<sup>58</sup> 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](https://www.business-standard.com/article/current-affairs/india-is-adding-10-million-active-internet-users-per-month-google-118062700882_1.html).

<sup>59</sup> 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>.

<sup>60</sup> *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.

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

<sup>62</sup> 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.<sup>63</sup>

### 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<sup>64</sup>. 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<sup>65</sup> to 1 day. The

<sup>63</sup> 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).

<sup>64</sup> See Shrutanjaya Bhardwaj, *Comments on the Draft Intermediary Guidelines (Amendment) Rules, 2018*, 1 (Jan. 4, 2019).

<sup>65</sup> 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](http://meity.gov.in/sites/upload_files/dit/files/Clarification%2079rules(1).pdf). See Chinmayi Arun and

proposed rules should differentiate between content<sup>66</sup> 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<sup>67</sup>. 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.<sup>68</sup> This will lead to censorship and takedown of lawful speech.<sup>69</sup>

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).

<sup>66</sup> 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/>.

<sup>67</sup> Recent initiative in Europe have a different time periods ranging from 1 hour to

<sup>68</sup> 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).

<sup>69</sup> 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.<sup>70</sup> 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<sup>71</sup>. 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.<sup>72</sup> Moreover, since the proposed rule does not define “unlawful information or content” it suffers from vagueness and is void. The rule also

<sup>70</sup> See *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶ 115.

<sup>71</sup> See *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) S.C.C. OnLine S.C. 1642, ¶ 447(4)(f).

<sup>72</sup> *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.<sup>73</sup> 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.<sup>74</sup> Nevertheless, algorithmic blocking must be approached with circumspection and careful advance consideration.

---

<sup>73</sup> 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).

<sup>74</sup> *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.<sup>75</sup> These technologies are inaccurate<sup>76</sup> and prone to both over inclusive and under inclusive outcomes.<sup>77</sup> 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<sup>78</sup> and disproportionately affect marginalized speakers and communities<sup>79</sup>.

Finally, over-censorship, by which a great deal of lawful content is disabled, is a near certainty.<sup>80</sup> 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.<sup>81</sup>

<sup>75</sup> 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).

<sup>76</sup> 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>.

<sup>77</sup> 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/>.

<sup>78</sup> 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).

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

<sup>80</sup> 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>.

<sup>81</sup> 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.

PUBLIC COMMENTS ON DRAFT INTERMEDIARY GUIDELINES, 2018  
(Published by MeitY)

---

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





MIT/79/087

The spread of disinformation over social media platforms and other forms of unlawful activities a legitimate law and order concern, however the demands placed upon these platforms by the proposed The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 cast far too wide a net, will the dampen free and open discourse that is a hallmark of democracy and in its current avatar is likely to cause more harm than good.

Clause: 3(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 authorised.*

#### **UNNECESSARILY WIDE GAMUT:**

The nebulous category of “unlawful information”, which includes any content perceived as a threat to “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” brings us full circle to Shreya Singhal v. Union of India which brought up the unconstitutionality of Section 66A's similarly unclear list of offences. To hold an intermediary accountable for such a wide, easily-misused list of content is both an unreasonable demand on the resources of the intermediary as well as a worrying chokehold on free speech.

Since the core problem this act wishes to address is, as elucidated above, a law and order issue, the Intermediary Guidelines seem to cast a disproportionately wide net. Paired with another proposed bill, the Personal Data Protection Bill (2018) which mandates that data fiduciaries store a copy of personal data of Indian users in India, the government will be able to demand access to personal information of online media users for a wide range of perceived offences to the detriment of free and open discourse online.

#### **DATA RETENTION IS ANTITHETICAL TO PRIVACY**

The amendment requires storage of content requested by law enforcement agencies for 180 days at first and then for as long as deemed necessary by a court or government agencies. By leaving the duration for storage of such data open-ended, the provision is runs contrary to the principle of ‘Storage Limitation’ recommended by the Srikrishna Committee.<sup>1</sup> Instead of providing for indefinite storage of data beyond 180 days the amendment should require a periodic authorization every 60 days by a court or government agency should the data be deemed valuable for an investigation. In the absence of such an authorization the data preservation request would automatically lapse.

---

<sup>1</sup> Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, “A Free and Fair Digital Economy Protecting Privacy, Empowering Indians,” p.60 available at: [http://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf).

Clause 3(5): *When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.*

#### **TRACEABILITY IS ANTITHETICAL TO PRIVACY**

The amendments require intermediaries – defined under Indian law to include ISPs as well as communication platforms – to trace the originator of information on their platform when served with an order by an authorised government agency.

On communications platforms this would entail examining a chain of forwards to track down the individual who composed the original message or first uploaded a media file in question. For end-to-end encrypted services, this is not technically feasible, since the communication service providers do not have access to the content of the messages.

While MEITY has insisted<sup>2</sup> that the traceability requirement does not automatically mean breaking encryption, there is little doubt that enforcement of these rules will mean that

---

<sup>2</sup> Ministry of E & IT (@GoI\_Meity), “[@DialogueIndia](https://twitter.com/GoI_Meity/status/1081505492059467776) We are asking to trace origin of messages which lead to unlawful activities without breaking encryption. [#SaferSocialMedia](https://twitter.com/GoI_Meity/status/1081505492059467776),” January 5, 2019, 1629 Hrs, available at: [https://twitter.com/GoI\\_Meity/status/1081505492059467776](https://twitter.com/GoI_Meity/status/1081505492059467776).

some companies would have to roll back encryption entirely. To be clear, traceability is incompatible with end-to-end encryption.

Encryption as a service is used by journalists and whistleblowers to legitimately protect their privacy and in that is an enabler of the right to privacy and the freedom of expression. Apart from protecting privacy, encryption also makes communications more secure and helps ensure integrity of information.

Moreover, in many cases traceability that requires service providers to roll back or reduce the strength of encryption over their services is also likely to be ineffective. For example content that poses a threat to public order and national security (such as fake news) can be created on platforms and on forums that are not subject to Indian law and then released on to popularly used platforms where they can go viral. In situations such as these, tracing the pathway through which the content was shared by well-meaning users is unlikely to result in the apprehension of the true authors of such content.



**Mozilla Headquarters**

331 E Evelyn Avenue  
Mountain View, CA 94041  
United States of America  
650.903.0800

MIT/79/071

To  
Mr. Ravi Shankar Prasad  
Minister of Electronics and Information Technology  
Government of India

31st January 2019

To the Hon'ble Minister Prasad,

Thank you for the opportunity to provide comment on the draft Information Technology (Intermediary Guidelines) Rules 2018, that are proposed to replace the rules notified in 2011.

Mozilla is a global community working together to build a better internet. As a mission-driven technology company, we are dedicated to promoting openness, innovation, and opportunity online. We are the creators of Firefox, an open source browser and the family of Firefox products, including Firefox Focus and Firefox Lite, as well as Pocket, used by hundreds of millions of individual internet users globally.

As we've highlighted before, illegal content is symptomatic of an unhealthy internet ecosystem. To that end, Mozilla recently adopted an addendum to our Manifesto, in which we affirmed our commitment to an internet that promotes civil discourse, human dignity, and individual expression. Our products, policies, and processes embody these principles. Ultimately, illegal content on the web – and substandard policy and industry responses to it – undermine the overall health of the internet and as such, are a core concern for Mozilla. We have been at the forefront of these conversations globally (most recently, in Europe), pushing for approaches that manage the harms of illegal content online within a rights-protective framework.

We support the consideration of measures to hold social media platforms to higher standards of responsibility. However, **in our filing below, we explain why the current draft rules are not fit-for-purpose and will have a series of unintended consequences on the health of the internet as a whole.** For the sake of the internet's future and Indian users, we urge you to abandon these proposed rules and begin afresh with public consultations on the appropriate way to counter harmful speech online.

Continued open and wide ranging consultation on this complex issue will be necessary if India is to have a future-proof framework for tackling illegal

content in India. **Over the coming weeks and months, we will remain focused on shaping more sustainable solutions to these concerns, and to build out a vision for what a better framework for the "duty of diligence" could look like.** We look forward to providing these inputs and hope that they will be helpful as you continue your important work. For any questions on the present filing, please do not hesitate to contact Mozilla's Policy Advisor Amba Kak at [amba@mozilla.com](mailto:amba@mozilla.com).

### **Summary of concerns and recommendations**

Our concerns with the current draft may be grouped into three broad categories:

- I. Dilution of intermediary liability protections and content filtering obligations
- II. Enhanced government surveillance
- III. Operational requirements

#### **I. Dilution of intermediary liability protections and content filtering obligations**

**Proactive takedown obligation creates a zero-tolerance approach to harmful content which will inevitably lead to over-censorship and chill free expression.**

- This new regime significantly rolls back the intermediary liability protections enshrined in Section 79 of the Information Technology Act, and affirmed by the *Shreya Singhal* judgment of the Indian Supreme Court. The Court had put forth both practical and principled objections to requiring private companies to decide the legality of content on internet-scale. The verdict clarified that platforms would only be expected to remove content when they are directed to do so by a court order. The draft rules turn this logic on its head, and introduce a mandate for companies to proactively take down "unlawful content" using automated means.
- The rules provide no definition of "unlawful" beyond relating it to broad categories like "public order", and "decency and morality". Faced with the threat of direct liability for content, these rules not only encourage but essentially compel companies to bypass due process and make rapid, non-transparent, and unaccountable decisions

about what content gets removed. Eventually, it is users who will be deterred from expressing themselves online.

- On any online platform where users can communicate without prior restraint, there will be a risk that some users abuse that privilege. It is this freedom to communicate without ex ante restraints has been integral to the creativity, collaboration, access to knowledge and innovation that has made the internet successful. Moreover, the goal of completely purging illegal content online is also at odds with the technical architecture of platforms. When operating at enormous scale, it is technically infeasible to expect that risk to be entirely nullified.

**Automated and machine-learning solutions should not be encouraged as a silver bullet to fight against illegal speech on the internet.**

- The draft rules include a mandate to deploy automated tools to filter content. As we have [argued in Europe](#), automated content filters are a crude control instrument, and are of limited use when assessing the legality of content where *context* is essential.
- In opting to encourage automated tools, the government is putting primacy on the speed and quantity, rather than the quality, of content removals. These are blunt and inappropriate metrics of success when critical fundamental rights are at stake. Filtering tools are only effective with respect to a small subset of illegal content like child pornography where the standard is well defined and universally recognized, and the corresponding harm to free expression is minimal.
- When deployed in the context of the broad and subjective grounds provided in these draft rules, the additional context is critical (for e.g. a culturally specific reference; or if the content was excerpted for the purpose of commentary; or if intended for a specific and limited audience). False positives, or inaccurate labelling of content as illegal by algorithms could mean the suppression of legal content. This directly harms the freedom of speech guaranteed to Indian citizens, is likely to cause a chilling effect on users and eventually, diminishes the vibrancy of the public sphere.

**One-size-fits-all obligations for (a) *all types of intermediaries* and (b) *all types of illegal content* are arbitrary and disproportionate.**

- (a) *All types of intermediaries*
  - The term "intermediaries" is defined to go far beyond just social media companies. From internet service providers, to browsers, to operating systems, it is hard to imagine any internet company that wouldn't fall within its scope. While these rules have been justified as a way to tackle "instances of misuse of social media", the broad definition goes far beyond the specific companies they refer to. As written, these rules apply indiscriminately to all intermediaries regardless of the role we play in the ecosystem. While the intention might be for selective enforcement, the legal risk applies to all.
  - For small, medium-sized, and start-up online services, these elaborate content control obligations will be disproportionately burdensome to implement. Liability protections have allowed entrepreneurs to host platforms without fear that their innovations would be crushed by a failure to police every action of their users. Imposing the obligations proposed in these new rules would place a tremendous and in many cases fatal burden on many online intermediaries, especially new companies. A startup's first move should not be to build filtering infrastructure and hire an army of lawyers.
- (b) *All types of illegal content*
  - Illegal content is of various kinds, ranging from child pornography to hate speech to copyright to defamation. The draft rules, however, ignore crucial differences and put a uniform requirement of automated proactive removal of all types of "unlawful" content.
  - Each kind of illegal content has widely differing impact on fundamental rights and should not receive the same legal and technical treatment. For example, while sexual abuse content inevitably has a grave impact on victims and might require urgent takedown, a potential violation of copyright instead



calls for a balanced investigation of the claims and counter-claims, and necessitates a less hurried approach. On the other hand, with alleged hate speech or misinformation, there may be much more serious implications on freedom of speech depending on the political and social impact of the content in question. A single legal standard is a blunt approach to address these important differences.

## II. Enhanced government surveillance

**A proactive filtering mandate would require all online intermediaries to embed monitoring infrastructure and carry out continuous surveillance of user activity.**

- The mandate to proactively filter unlawful content, in effect, requires companies to embed monitoring infrastructure in order to continuously surveil the activities of users. Note that the definition of intermediaries would include entities ranging from internet service providers to browsers and operating systems, all of which are uniquely placed to gather a range of sensitive personal data from users.
- Rather than ensuring privacy and data protection safeguards, the draft rules encourage continuous surveillance. This kind of bulk and unrestricted monitoring flies in the face of the Supreme Courts dictat in *Puttaswamy v Union of India*, which puts in place a requirement that any limitations on the fundamental right to privacy must be narrowly tailored and proportionate.

**Requiring encrypted services to store additional sensitive information for the sole purpose of government surveillance weakens overall security and contradicts the principles of data minimisation, endorsed in MEITY's draft data protection bill.**

- Under the draft rules, law enforcement agencies can demand that companies trace the originator of any information. Many popular services today deploy end-to-end encryption and do not store source information to enhance the security of their systems and the privacy they guarantee users. This would essentially be a mandate to collect



and store additional metadata about senders and receivers of content with the sole purpose being potential government surveillance requests.

- For users, the guarantees of both end-to-end encryption with minimal collection of metadata is an assurance of privacy and security in the products. Compelling companies to modify their infrastructure based on government requests undermines this trust and denies them the ability to provide secure products and services to their customers.
- This mandate also contradicts the principles of data minimization and privacy by design, endorsed in MEITY's draft data protection bill, which require that entities only store the personal data that they need to deliver the service.

### III. Operational requirements

**Operational obligations on global businesses (especially SMEs) are onerous and likely to spur market exit and deter market entry.**

- The proposed rules, amongst other requirements, put a blunt requirement on any service with more than 5 million users in India to incorporate in the country and set up a permanent office. This is a significant operational obligation being imposed on hundreds of services, with no justification for this standard, nor any time period for compliance.
- If the justification is better compliance with government orders, then we submit that mandatory incorporation in India is a disproportionate means to achieve this end. For companies looking to have global presence, India is a large market that cannot be ignored. The stakes are already large enough, and combined with an effective regulator, these fears of non-enforcement are unfounded. Moreover, the choice of where to incorporate has multiple business consequences. Especially for small and medium sized entities, forcibly requiring incorporation and setting up an office in India could mean additional financial burden and operational inconvenience that may cause retreat from the Indian market altogether.
- This raises fears of several smaller international companies closing themselves off to Indian users, while also deterring potential market

expansion of new players into India. Less diversity of services means less choices for users, less competition between services and eventually harms the vibrancy of the Indian digital ecosystem.

- Any move to require companies to incorporate in India, especially with such a minimal market presence, would not only set a dangerous example for other countries, but also other countries would likely reciprocate in kind, requiring Indian companies to incorporate in their jurisdictional borders, which would represent a heavy burden on Indian industry and limit the efficacy of the Digital India and Made in India initiatives.
- Finally, developers of free to download software cannot easily control their distribution. This is especially true for open source software, which anyone can copy and compile. Software developers could thus find themselves falling under the requirements (and sanctions) of these rules absent any volition or action on their part.

## Conclusion

As the creator of an open source browser, we are an online intermediary supported by a large number of Indian users and volunteers. If implemented in their current form, these rules would require us to embed an automated infrastructure for surveillance and censorship into our networks. This not only would contravene our core commitments to privacy and freedom of speech online, but also give us the impossible task of having to decide the legality of content at internet-scale.

We support the consideration of measures to hold social media platforms to higher standards of responsibility, and acknowledge that building rights-protective frameworks for tackling illegal content on the internet is a challenging task. On our part, we remain focused on building out a vision for what a better framework for the “duty of diligence” could look like. The current draft of the rules put forward by the Ministry, however, are not fit for purpose. For the sake of the internet's future and Indian users, we urge you to abandon these proposed rules and begin afresh with public consultations on the appropriate way to counter harmful speech online.





**Press Information Bureau**  
**Government of India**



Ministry of Electronics & IT

## Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Social media platforms welcome to do business in  
India but they need to follow the Constitution and  
laws of India

Social media platform can certainly be used for  
asking questions and criticise

Social media platforms have empowered ordinary  
users but they need accountability against its  
misuse and abuse

The new Rules empower ordinary users of social  
media, embodying a mechanism for redressal and  
timely resolution of their grievance

Rules about digital media and OTT focuses more  
on in house and self-regulation mechanism  
whereby a robust grievance redressal mechanism  
has been provided while upholding journalistic and  
creative freedom



The proposed framework is progressive, liberal and contemporaneous

It seeks to address peoples' varied concerns while removing any misapprehension about curbing creativity and freedom of speech and expression

The guidelines have been framed keeping in mind the difference between viewership in a theatre and television as compared to watching it on Internet

Posted On: 25 FEB 2021 2:44PM by PIB Delhi

Amidst growing concerns around lack of transparency, accountability and rights of users related to digital media and after elaborate consultation with the public and stakeholders, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 has been framed in exercise of powers under section 87 (2) of the Information Technology Act, 2000 and in supersession of the earlier Information Technology (Intermediary Guidelines) Rules 2011.

While finalizing these Rules, both the Ministries of Electronics and Information Technology and Ministry of Information and Broadcasting undertook elaborate consultations among themselves in order to have a harmonious, soft-touch oversight mechanism in relation to social media platform as well as digital media and OTT platforms etc.

Part- II of these Rules shall be administered by Ministry of Electronics and IT, while Part-III relating to Code of Ethics and procedure and safeguards in relation to digital media shall be administered by the Ministry of Information and Broadcasting.

### Background:

The Digital India programme has now become a movement which is empowering common Indians with the power of technology. The extensive spread of mobile phones, Internet etc. has also enabled many social media platforms to expand their footprints in India. Common people are also using these platforms in a very significant way. Some portals, which publish analysis about social media platforms and which have not been disputed, have reported the following numbers as user base of major social media platforms in India:

- WhatsApp users: 53 Crore
- YouTube users: 44.8 Crore
- Facebook users: 41 Crore
- Instagram users: 21 Crore
- Twitter users: 1.75 Crore



These social platforms have enabled common Indians to show their creativity, ask questions, be informed and freely share their views, including criticism of the Government and its functionaries. The Government acknowledges and respects the right of every Indian to criticize and disagree as an essential element of democracy. India is the world's largest open Internet society and the Government welcomes social media companies to operate in India, do business and also earn profits. However, they will have to be accountable to the Constitution and laws of India.

Proliferation of social media, on one hand empowers the citizens then on the other hand gives rise to some serious concerns and consequences which have grown manifold in recent years. These concerns have been raised from time to time in various forums including in the Parliament and its committees, judicial orders and in civil society deliberations in different parts of country. Such concerns are also raised all over the world and it is becoming an international issue.

Of late, some very disturbing developments are observed on the social media platforms. Persistent spread of fake news has compelled many media platforms to create fact-check mechanisms. Rampant abuse of social media to share morphed images of women and contents related to revenge porn have often threatened the dignity of women. Misuse of social media for settling corporate rivalries in blatantly unethical manner has become a major concern for businesses. Instances of use of abusive language, defamatory and obscene contents and blatant disrespect to religious sentiments through platforms are growing.

Over the years, the increasing instances of misuse of social media by criminals, anti-national elements have brought new challenges for law enforcement agencies. These include inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, financial frauds, incitement of violence, public order etc.

It was found that currently there is no robust complaint mechanism wherein the ordinary users of social media and OTT platforms can register their complaint and get it redressed within defined timeline. Lack of transparency and absence of robust grievance redressal mechanism have left the users totally dependent on the whims and fancies of social media platforms. Often it has been seen that a user who has spent his time, energy and money in developing a social media profile is left with no remedies in case that profile is restricted or removed by the platform without giving any opportunity to be heard.

### **Evolution of Social Media and Other Intermediaries:**

- If we notice the evolution of social media intermediaries, they are no longer limited to playing the role of pure intermediary and often they become publishers. These Rules are a fine blend of liberal touch with gentle self-regulatory framework. It works on the existing laws and statutes of the country which are applicable to content whether online or offline. In respect of news and current affairs publishers are expected to follow the journalistic conduct of Press Council of India and the Programme Code under the Cable Television Network Act, which are already applicable to print and TV. Hence, only a level playing field has been proposed.

### **Rationale and Justification for New Guidelines:**

These Rules substantially empower the ordinary users of digital platforms to seek redressal for their grievances and command accountability in case of infringement of their rights. In this direction the following developments are noteworthy:



- The Supreme Court in suo-moto writ petition (Prajawala case) vide order dated 11/12/2018 had observed that the Government of India may frame necessary guidelines to eliminate child pornography, rape and gangrape imageries, videos and sites in content hosting platforms and other applications.
- The Supreme Court vide order dated 24/09/2019 had directed the Ministry of Electronics and Information Technology to apprise the timeline in respect of completing the process of notifying the new rules.
- There was a Calling Attention Motion on the misuse of social media and spread of fake news in the Rajya Sabha and the Minister had conveyed to the house on 26/07/2018, the resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law. He had conveyed this after repeated demands from the Members of the Parliament to take corrective measures.
- The Ad-hoc committee of the Rajya Sabha laid its report on 03/02/2020 after studying the alarming issue of pornography on social media and its effect on children and society as a whole and recommended for enabling identification of the first originator of such contents.

### **Consultations:**

- The Ministry of Electronics and Information Technology (MEITY) prepared draft Rules and invited public comments on 24/12/2018. MEITY received 171 comments from individuals, civil society, industry association and organizations. 80 counter comments to these comments were also received. These comments were analyzed in detail and an inter-ministerial meeting was also held and accordingly, these Rules have been finalized.

### **Salient Features**

#### **Guidelines Related to Social Media to Be Administered by Ministry of Electronics and IT:**

- **Due Diligence To Be Followed By Intermediaries:** The Rules prescribe due diligence that must be followed by intermediaries, including social media intermediaries. In case, due diligence is not followed by the intermediary, safe harbour provisions will not apply to them.
- **Grievance Redressal Mechanism:** The Rules seek to empower the users by mandating the intermediaries, including social media intermediaries, to establish a grievance redressal mechanism for receiving resolving complaints from the users or victims. Intermediaries shall appoint a Grievance Officer to deal with such complaints and share the name and contact details of such officer. Grievance Officer shall acknowledge the complaint within twenty four hours and resolve it within fifteen days from its receipt.
- **Ensuring Online Safety and Dignity of Users, Specially Women Users:** Intermediaries shall remove or disable access within 24 hours of receipt of complaints of contents that exposes the private areas of individuals, show such individuals in full or partial nudity or in sexual act or is in the nature of impersonation including morphed images etc. Such a complaint can be filed either by the individual or by any other person on his/her behalf.
- **Two Categories of Social Media Intermediaries:** To encourage innovations and enable growth of new social media intermediaries without subjecting smaller platforms to significant compliance requirement, the Rules make a distinction between social media intermediaries and significant social media intermediaries. This distinction is based on the number of users on the social media platform. Government is empowered to notify the threshold of user base that will distinguish between social media intermediaries and significant social media intermediaries. The Rules require the significant social media intermediaries to follow certain additional due diligence.
- **Additional Due Diligence to Be Followed by Significant Social Media Intermediary:**
  - Appoint a **Chief Compliance Officer** who shall be responsible for ensuring compliance with the Act and Rules. Such a person should be a resident in India.



- Appoint a **Nodal Contact Person** for 24x7 coordination with law enforcement agencies. Such a person shall be a resident in India.
- Appoint a **Resident Grievance Officer** who shall perform the functions mentioned under Grievance Redressal Mechanism. Such a person shall be a resident in India.
- Publish a **monthly compliance report** mentioning the details of complaints received and action taken on the complaints as well as details of contents removed proactively by the significant social media intermediary.
- Significant social media intermediaries providing services primarily in the nature of messaging shall enable **identification of the first originator of the information** that is required only for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material punishable with imprisonment for a term of not less than five years. **Intermediary shall not be required to disclose the contents of any message** or any other information to the first originator.
- Significant social media intermediary shall have a physical contact address in India published on its website or mobile app or both.
- **Voluntary User Verification Mechanism:** Users who wish to verify their accounts voluntarily shall be provided an appropriate mechanism to verify their accounts and provided with demonstrable and visible mark of verification.
- **Giving Users An Opportunity to Be Heard:** In cases where significant social media intermediaries removes or disables access to any information on their own accord, then a prior intimation for the same shall be communicated to the user who has shared that information with a notice explaining the grounds and reasons for such action. Users must be provided an adequate and reasonable opportunity to dispute the action taken by the intermediary.
- **Removal of Unlawful Information:** An intermediary upon receiving actual knowledge in the form of an order by a court or being notified by the Appropriate Govt. or its agencies through authorized officer should not host or publish any information which is prohibited under any law in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries etc.
- The Rules will come in effect from the date of their publication in the gazette, except for the **additional due diligence for significant social media intermediaries**, which shall **come in effect 3 months after** publication of these Rules.

### **Digital Media Ethics Code Relating to Digital Media and OTT Platforms to Be Administered by Ministry of Information and Broadcasting:**

There have been widespread concerns about issues relating to digital contents both on digital media and OTT platforms. Civil Society, film makers, political leaders including Chief Minister, trade organizations and associations have all voiced their concerns and highlighted the imperative need for an appropriate institutional mechanism. The Government also received many complaints from civil society and parents requesting interventions. There were many court proceedings in the Supreme Court and High Courts, where courts also urged the Government to take suitable measures.

Since the matter relates to digital platforms, therefore, a conscious decision was taken that issues relating to digital media and OTT and other creative programmes on Internet shall be administered by the Ministry of Information and Broadcasting but the overall architecture shall be under the Information Technology Act, which governs digital platforms.



Ministry of Information and Broadcasting held consultations in Delhi, Mumbai and Chennai over the last one and half years wherein OTT players have been urged to develop “self-regulatory mechanism”. The Government also studied the models in other countries including **Singapore, Australia, EU and UK** and has gathered that most of them either have an institutional mechanism to regulate digital content or are in the process of setting-up one.

**The Rules establish a soft-touch self-regulatory architecture and a Code of Ethics and three tier grievance redressal mechanism for news publishers and OTT Platforms and digital media.**

Notified under section 87 of Information Technology Act, these Rules empower the Ministry of Information and Broadcasting to implement Part-III of the Rules which prescribe the following:

- **Code of Ethics for online news, OTT platforms and digital media:** This Code of Ethics prescribe the guidelines to be followed by OTT platforms and online news and digital media entities.
- **Self-Classification of Content:** The OTT platforms, called as the publishers of online curated content in the rules, would **self-classify the content into five age based categories-** U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult). Platforms would be required to implement **parental locks for content classified as U/A 13+ or higher**, and **reliable age verification mechanisms for content classified as “A”**. The publisher of online curated content shall prominently **display the classification rating** specific to each content or programme together with a content descriptor informing the user about the nature of the content, and advising on viewer description (if applicable) at the beginning of every programme enabling the user to make an informed decision, prior to watching the programme.
- Publishers of news on digital media would be required to observe **Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act** thereby providing a **level playing field between the offline (Print, TV) and digital media**.
- A **three-level grievance redressal mechanism** has been established under the rules **with different levels of self-regulation**.
  - Level-I: Self-regulation by the publishers;
  - Level-II: Self-regulation by the self-regulating bodies of the publishers;
  - Level-III: Oversight mechanism.
- **Self-regulation by the Publisher:** Publisher shall appoint a Grievance Redressal Officer based in India who shall be responsible for the redressal of grievances received by it. The officer shall take decision on every grievance received by it within 15 days.
- **Self-Regulatory Body:** There may be one or more self-regulatory bodies of publishers. Such a body shall be headed by a retired judge of the Supreme Court, a High Court or independent eminent person and have not more than six members. Such a body will have to register with the Ministry of Information and Broadcasting. This body will oversee the adherence by the publisher to the Code of Ethics and address grievances that have not been resolved by the publisher within 15 days.
- **Oversight Mechanism:** Ministry of Information and Broadcasting shall formulate an oversight mechanism. It shall publish a charter for self-regulating bodies, including Codes of Practices. It shall establish an Inter-Departmental Committee for hearing grievances.

\*\*\*\*\*

RKJ/M





(Release ID: 1700749) Visitor Counter : 6021

Read this release in: Marathi , Hindi , Gujarati , Odia , Telugu , Malayalam



Share your ideas & suggestions for  
**Mann Ki Baat**  
on 30th May, 2021

Click Here or  
Dial 1800 11 7800 (Toll-Free)

The phone lines shall remain open  
from 5th to 28th May, 2021

Download PIB APP



## RTI and Contact Us

WHO'S WHO AT PIB

Telephone Number of Regional Branch Offices of  
PIB

Information Manual

Transparency Audit

Internal Complaints Committee

Work Allocation

Telephone Nos of PIB Officers of Hqrs

Public Grievance Officer

CPIOs Appellate Authority List

Citizen Charter

Allocation Budget

Liaison Officer

Web Info Manager

## GOI Links

Ministry of Information and Broadcasting

Ministry of Agriculture & Farmers Welfare

Ministry of Textiles

Ministry of Commerce & Industry

Ministry of Defence

Ministry of Finance

Ministry of Health and Family Welfare



Ministry of Home Affairs

Ministry of Housing and Urban Affairs

Ministry of Human Resource Development

**178**

[More](#)

[Tenders](#)

[Archives](#)

[Terms & Conditions](#)

[Copyright Policy](#)  
[Help](#)

[Privacy Policy](#)

[Hyperlinking Policy](#)

Site is hosted by National Informatics Centre (NIC). Information is provided and updated by Press Information Bureau "A" wing, Shastri Bhawan, Dr. Rajendra Prasad Road, New Delhi – 110001, Phone: 23389338.

**Visitor Counter:** 110983

Last Updated On: **22 May 2021 18:43:00 PM**



*R+L*

  
**TRUE COPY**





# भारत का राजपत्र The Gazette of India

सी.जी.-डी.एल.-अ.-26022021-225497  
CG-DL-E-26022021-225497

असाधारण  
EXTRAORDINARY

भाग II—खण्ड . —उप-खण्ड (ii)  
PART II—Section 3—Sub-section (ii)

प्राधिकार से प्रकाशित  
PUBLISHED BY AUTHORITY

सं. 869]  
No. 869]

नई दिल्ली, शुक्रवार, फरवरी 26, 2021/ फाल्गुन 7, 1942  
NEW DELHI, FRIDAY, FEBRUARY 26, 2021/ PHALGUNA 7, 1942

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

अधिसूचना

नई दिल्ली, 25 फरवरी, 2021

का.आ. 942(अ).—सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 के नियम 2 के उप-नियम (1) के खंड (फ) द्वारा प्रदत्त शक्ति का प्रयोग करते हुए केंद्र सरकार एक महत्वपूर्ण सोशल मीडिया मध्यवर्ती माने जाने के लिए एतद्वारा सोशल मीडिया मध्यवर्ती के लिए सीमा के रूप में पचास लाख भारत में पंजीकृत उपयोगकर्ता खाते विनिर्दिष्ट करती है।

[फा. सं.16(4)/2020-सीएलईएस]

डॉ. राजेंद्र कुमार, अपर सचिव

## MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY NOTIFICATION

New Delhi, the 25th February, 2021

S.O. 942(E).—In exercise of power conferred by clause (v) of sub-rule (1) of rule 2 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Central Government hereby specifies fifty lakh registered users in India as the threshold for a social media intermediary to be considered a significant social media intermediary.

[F. No. 16(4)/2020-CLES]

Dr. RAJENDRA KUMAR, Addl. Secy.

1257 GI/2021

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064  
and Published by the Controller of Publications, Delhi-110054.

SURENDER  
MAHADASAM  
Digitally signed by SURENDER  
MAHADASAM  
Date: 2021.02.26 17:48:05  
+05'30'

TRUE COPY

**Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**

REFERENCE:  
OL IND 3/2019

14 February 2019

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 34/18.

In this connection, I make reference to the call for public comments by the Ministry of Electronics and Information to **The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018** (“the proposed Amendment”).

I welcome the opportunity to submit this comment to the proposed Amendment, reviewed in light of international human rights standards on the right to freedom of opinion and expression, and I stand ready to engage further with your Excellency’s Government on this matter.

According to the information received:

On 26 July 2018, the Honorable Minister for Electronics and Information Technology proposed an amendment to the Information Technology (Intermediaries Guidelines) Rules established under Section 79 of the Information Technology Act.

Section 79 states that an intermediary “shall not be liable for any third party information, data, or communication link made available or hosted by him” provided that the intermediary, *inter alia*, “observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.”

On 24 December 2018, the Ministry of Electronics and Information announced its proposal for The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (“the proposed Amendment”). The proposal purportedly addresses the need to combat the misuse of social media platforms and the spread of “fake news.”

The proposed Amendment would impose additional obligations on intermediaries to prohibit online content and provide assistance to Government investigations into online content.

In particular, intermediaries would be required to, *inter alia*, prohibit an expanded range of online content, assist the Government in tracing prohibited information to

their originator, establish physical presence and personnel dedicated to law enforcement cooperation, remove illegal online content within twenty-four hours, retain user data, and proactively monitor and filter online content.

Before explaining my concerns with the proposed Amendment, I wish to remind your Excellency's Government of its obligations under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), acceded by India on 10 April 1979. Article 19(1) of the Covenant establishes "the right to hold opinions without interference." The right to hold opinions is so fundamental that it is "a right to which the Covenant permits no exception or restriction" (CCPR/C/GC/34). Accordingly, this right is not simply "an abstract concept limited to what may be in one's mind," and may include activities such as research, online search queries, and drafting of papers and publications"(A/HRC/29/32).

Article 19(2), in combination with Article 2 of the Covenant, establishes State Parties' obligations to respect and ensure the right "to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Since Article 19(2) "promotes so clearly a right to information of all kinds," this indicates that "States bear the burden of justifying any withholding of information as an exception to that right" (A/70/361). The Human Rights Committee has also emphasized that limitations should be applied strictly so that they do "not put in jeopardy the right itself" (CCPR/C/GC/34). The General Assembly, the Human Rights Council and the Human Rights Committee have concluded that permissible restrictions on the Internet are the same as those offline.

Article 19(3) establishes a three-part test for permissible restrictions on freedom of expression:

First, restrictions must be "provided by law." In evaluating the *provided by law* standard, the Human Rights Committee has noted that any restriction "must be made accessible to the public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly" (CCPR/C/GC/34). Moreover, it "must not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution" (CCPR/C/GC/34).

Second, restrictions must only be imposed to *protect legitimate aims*, which are limited to those specified under Article 19(3), that is "for respect of the rights or reputations of others" or "for the protection of national security or of public order (*ordre public*), or of public health and morals". The term "rights...of others" under Article 19(3)(a) includes "human rights as recognized in the Covenant and more generally in international human rights law" (CCPR/C/GC/34).

Third, restrictions must be *necessary to protect one or more of those legitimate aims*. The requirement of necessity implies an assessment of the proportionality of restrictions, with the aim of ensuring that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons" (A/70/361). The ensuing

interference with third parties' rights must also be limited and justified in the interest supported by the intrusion. Finally, the restriction must be "the least intrusive instrument among those which might achieve the desired result" (CCPR/C/GC/34).

In light of these standards, the proposed Amendment raises the following concerns:

**Draft Rule 3(1): Additional prohibitions on online content**

The existing Rule 3(1) requires intermediaries to prohibit, *inter alia*, information that is "grossly harmful, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging," or that "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order."

The proposed Amendment would also require intermediaries to prohibit the "host[ing], display[ing], upload[ing], modify[ing], publish[ing], transmit[ing], updat[ing] or shar[ing]" of information that "threatens public safety" or "threatens critical information infrastructure."

The Human Rights Committee has concluded that, under Article 19 of the ICCPR, "[a]ny restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3." Accordingly, Rule 3(1) and any proposed changes must be compatible with the criteria of legality, legitimacy and necessity.

While public order and national security are legitimate grounds for restriction, the existing and proposed Rule 3(1) may impose disproportionate restrictions on freedom of expression. Existing Rule 3(1) criteria, such as the prohibition of information that is "racially, ethnically objectionable, disparaging," are vaguely formulated and prone to highly subjective interpretation, creating uncertainty about how intermediaries should restrict such content. The proposed Amendment exacerbates this vagueness and uncertainty, expanding the range of prohibited information to include information that "threatens public safety" and "critical information infrastructure."

In my June 2018 report to the Human Rights Council, I cautioned that vaguely formulated standards like draft Rule 3(1) "involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability" (A/HRC/38/35). They also "involve the delegation of regulatory functions to private actors that lack basic tools of accountability," and "whose motives are principally economic" (A/HRC/38/35). Since decisions regarding the lawfulness of expression involve "[c]omplex questions of fact and law," I urge Your Excellency's Government to ensure that public institutions retain the authority to adjudicate these questions. In particular, restrictions on online content should only be imposed "pursuant

to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy” (A/HRC/38/35).

### **Draft Rule 3(5): Mandatory assistance orders**

Rule 3(5) of the proposed Amendment would require intermediaries to provide “information or assistance” as asked by “any government agencies who are lawfully authorized,” including by “enabl[ing] tracing of originator of information on its platform as required by government agencies who are legally authorised.”

Under draft Rule 3(5), authorized government agencies may seek such information and assistance for the “investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto.”

I am concerned that compliance with this draft Rule will require intermediaries to match the identity of users to the information at issue, which may in turn necessitate the circumvention of encryption and other digital security measures. As I have explained in my June 2015 report to the Human Rights Council, encryption and anonymity technologies establish a “zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks” (A/70/361). As a result, restrictions on these technologies must meet the well-known three-part test” established under Article 19(3).

Laws that mandate or effectively require decryption may compel intermediaries to introduce security vulnerabilities or otherwise weaken encryption in a manner that undermines encryption and digital security protocols for all users across the platform. Even in cases where mandatory decryption orders are targeted at an individual account for a specific investigation, the ensuing security and privacy risks to large numbers of users may disproportionately chill and hinder their exercise of freedom of expression. The prospect that such decryption measures may be sought on vaguely formulated grounds under draft Rule 3(5), such as for the protection of “cyber security” and any related matters, heightens the disproportionality of such measures.

### **Draft Rule 3(7): Mandatory incorporation and appointment of personnel**

Draft Rule 3(7) requires intermediaries with “more than fifty lakh users in India,” or on the list of intermediaries notified by the government, to be incorporated in India according to the Companies Act, and to have a permanent registered office in India with physical address. Furthermore, under Rule 3(7), intermediaries must appoint a “nodal person of contact” and “alternate senior designated functionary” in order to ensure “24x7 coordination with law enforcement agencies.”

While I appreciate that this proposed rule change may be an effort to enhance the accountability of intermediaries to local users, I am concerned that the burden of incorporation and associated compliance measures would outweigh its purported

objectives. The requirement to establish a permanent registered office and appoint compliance personnel within an unspecified timeline is likely to impose costs that may unduly restrict the creation and operation of small, medium-sized or non-profit intermediaries. The potentially disproportionate impact on these intermediaries may contribute to the dominance of major, multi-national platforms in the country and diminish media pluralism. The Human Rights Committee has found that “undue media dominance or concentration by privately controlled media groups in monopolistic situations ... may be harmful to a diversity of sources and views” (CCPR/C/GC/34). The potential effects of Draft Rule 3(7) would run counter to the State’s duty to take “appropriate action” to prevent undue dominance and ensure media pluralism (A/HRC/38/35).

**Draft Rule 3(8): 24-hour window for content removals and data retention requirements**

Draft Rule 3(8) requires intermediaries to remove or disable access to unlawful content within 24 hours upon receiving a court order or notification from the appropriate Government or its agency. In addition, intermediaries must retain such information and associated records for at least one hundred and eighty days for “investigation purposes” or “for such longer period a may be required by the court or by government agencies.”

I am concerned that the twenty-four hour rule provides extremely limited opportunity for review or appeal of removal orders, whether before a judicial body or other relevant appeals mechanisms. In my June 2018 report to the Human Rights Council, I warned against domestic requirements “to monitor and rapidly remove user-generated content,” which establish “punitive frameworks likely to undermine freedom of expression even in democratic societies” (A/HRC/38/35). Furthermore, the lack of independent and external review or oversight of government-issued orders would effectively confer significant discretion on government authorities to restrict online content based on vague criteria, raising concerns of due process and increasing the risk of government overreach. Consistent with this past reporting, I urge Your Excellency’s Government to refrain from adopting a model of regulation “where government agencies, rather than judicial authorities, become the arbiters of lawful expression” (A/HRC/35/22).

The proposed data retention requirements also raise necessity and proportionality concerns. These requirements effectively compel intermediaries to create databases of personal and sensitive information about users that are readily accessible to the government for an unspecified range of “investigative purposes.” I have observed that broad data retention mandates heighten the risk of government access to user data that violates “established due process standards, such as the need for individualized suspicion of wrongdoing” (A/HRC/35/22). These mandates also render users vulnerable to security breaches and unauthorized third-party access. Additionally, I am concerned that Rule 3(8)’s data retention requirements, together with the proposals for proactive monitoring of online content and closer cooperation between intermediaries and law enforcement, will create a broad and intrusive surveillance regime that chills the exercise of the right to seek, receive and impart information on internet platforms.



### **Draft Rule 3(9): Automated content monitoring and removals**

Draft Rule 3(9) states that an “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 content.”

I am concerned that this proposed rule change would impose an affirmative obligation on intermediaries to regularly monitor content and restrict content at the point of upload, based on their own determinations of legality under highly subjective criteria (such as threats to “public safety” and “critical information infrastructure” as outlined above). As I discussed above, content review systems deployed by private intermediaries, which lack the due process safeguards and democratic legitimacy of the judicial process, are ill-equipped to make such determinations. The threat of criminal or civil penalties is also likely to incentivize intermediaries to err on the side of caution and restrict content that is perfectly legitimate or lawful.

Overreliance on automated tools would exacerbate these concerns. Automation tools range from keyword filters and spam detection tools to hash-matching algorithms (which filter images based on their unique digital “fingerprint”) and Natural Language Processing tools (which parse different features of text to determine whether it is a targeted category of speech).<sup>1</sup> These tools have become useful means of parsing text, images and video based on highly specific and objective criteria (such as matching the digital “fingerprints” of images to those of images already deemed unlawful). However, when applied to evaluations of online content that require an understanding of context or an assessment of highly subjective criteria (such as hate speech or libel), automated tools are prone to unreliable and discriminatory outcomes. In my September 2018 report to the General Assembly, I explained that these tools are still largely unable to meaningfully process “widespread variation of language cues, meaning and linguistic and cultural particularities” (A/73/348). Automated content moderation tools may also be “grounded in datasets that incorporate discriminatory assumptions” about race, gender and other protected characteristics, creating a high risk that such tools will remove content “in accordance with biased or discriminatory concepts” (A/73/348).

As a result, overreliance on automated tools may both overlook content susceptible to lawful restriction under Article 19(3) and increase censorship of legitimate expression. Inherent difficulties in scrutinizing and explaining the logic of automated tools further problematize their use in regulating contested areas of expression (A/73/348).

I urge the your Excellency’s Government to ensure that any amendment to its rules on intermediary liability addresses these concerns and is consistent with Article 19 of the ICCPR and related human rights standards.

<sup>1</sup> CTR. FOR DEMOCRACY & TECH., MIXED MESSAGES?: THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 1, 9 (2017), <https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf>.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting website within 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye  
Special Rapporteur on the promotion and protection of the right to freedom of opinion  
and expression



**TRUE COPY**

**IN THE HON'BLE HIGH COURT OF DELHI  
(EXTRAORDINARY WRIT JURISDICTION)**

**I.A. NO. \_\_\_\_\_ OF 2021**

**IN**

**WRIT PETITION (CIVIL) NO. \_\_\_\_ OF 2021**

**IN THE MATTER OF:**

**WHATSAPP LLC**

**...PETITIONER**

**VERSUS**

**UNION OF INDIA**

**...RESPONDENT**

**APPLICATION FOR INTERIM RELIEF**

**TO**

THE HON'BLE CHIEF JUSTICE AND THE  
HON'BLE COMPANION JUDGES OF THE  
HON'BLE HIGH COURT OF DELHI;

THE HUMBLE PETITION ON BEHALF OF  
PETITIONER ABOVE NAMED

**MOST RESPECTFULLY SHOWETH:**

1. That Petitioner, by way of the accompanying Writ Petition under Article 226 of the Constitution, prays for a Writ of Mandamus or any other appropriate writs seeking a declaration that (i) Impugned Rule 4(2) of the Information

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**Intermediary Rules**”) is unconstitutional, *ultra vires* the Information Technology Act, 2000 (“**IT Act**”), and illegal as to end-to-end encrypted messaging services; and (ii) criminal liability may not be imposed for non-compliance with Impugned Rule 4(2), and any attempt to impose criminal liability for non-compliance with Impugned Rule 4(2) is unconstitutional, *ultra vires* the IT Act, and illegal.

2. Petitioner provides WhatsApp, a state-of-the-art end-to-end encrypted messaging service that allows people to communicate privately and securely. WhatsApp is used by more than 2 billion people throughout the world, including hundreds of millions of users in India. Due largely to Petitioner’s end-to-end encryption, users trust that they can communicate securely and privately with everyone — from friends and loved ones to medical providers, crisis support hotlines, and financial institutions — without anyone, including Petitioner, listening to or monitoring their conversations.
3. The facts of the case and the contents of the accompanying Petition are not repeated hereinafter for the sake of brevity and the same should be read as part and parcel of the present application.
4. Impugned Rule 4(2) requires that significant social media intermediaries “*providing services primarily in the nature of messaging shall enable the identification of the first originator of the information*” in India on their messaging services when required by an order under Section 69 of the

IT Act or a court order. The Petition has demonstrated a strong *prima facie* case that this Impugned Rule violates the fundamental rights of the hundreds of millions of WhatsApp users in India and Petitioner, and is *ultra vires* its parent statute, manifestly arbitrary, and illegal. The balance of convenience is also in favour of Petitioner and against Respondent.

5. Impugned Rule 4(2) is expected to become effective on May 26, 2021, at which point government agencies and instrumentalities of the State, are expected to make demands that Petitioner provide the identity of the first originator of information in India on its end-to-end encrypted platform, in violation of the fundamental rights of both the Petitioner and its Indian users. Non-compliance with such orders could result in the loss of the safe harbor immunity under Section 79 of the IT Act and criminal prosecution and liability.
6. Further, compliance with Impugned Rule 4(2) would force Petitioner to break end-to-end encryption on WhatsApp, and alter the fundamental nature of the service that people love and use today in India and across more than 100 countries. Thus, both non-compliance and compliance with Impugned Rule 4(2) will cause irreparable harm to the fundamental rights of Petitioner and its users and Petitioner's reputation.
7. No demonstrable harm will be caused to anyone if the operation of Impugned Rule 4(2) is stayed pending adjudication of this Petition.

8. Accordingly, Petitioner most respectfully submits that the operation of Impugned Rule 4(2) should be stayed during the pendency of the accompanying Petition as the Impugned Rule is without the authority of law, imposes onerous and constitutionally invalid obligations upon Petitioner, and violates the fundamental rights of hundreds of millions of WhatsApp users throughout the country.
9. This application is made bona fide and in the interest of justice.

### **PRAYER**

It is, therefore, most respectfully prayed that this Hon'ble Court may be pleased to:

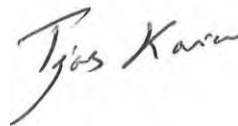
- a. Restrain Respondent and any other Government or law enforcement agency from taking any coercive steps against Petitioner and its employees in exercise of the powers purportedly conferred by Impugned Rule 4(2) during the pendency of the accompanying Petition;
- b. *Ex-parte ad-interim* stay (i) the operation of Impugned Rule 4(2) as to Petitioner and its employees during the pendency of the accompanying Petition, and (ii) the imposition of criminal liability on Petitioner and its employees for non-compliance with Impugned Rule 4(2) during the pendency of the accompanying Petition; and

C. Pass any further orders that this Hon'ble Court may deem fit and proper in light of the facts and circumstances of the present case.

FOR WHICH ACT OF KINDNESS THE PETITIONER SHALL AS DUTY  
BOUND FOREVER PRAY

  
PETITIONER

FILED THROUGH



M/S. SHARDUL AMARCHAND MANGALDAS  
& CO., ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216, OKHLA  
INDUSTRIAL ESTATE, PHASE-III, NEW

DELHI -110020

EMAIL: TEJAS.KARIA@AMSSHARDUL.COM

PAVIT.KATOCH@AMSSHARDUL.COM

MOB: 9871790537

PLACE: NEW DELHI  
DATE: 21 MAY 2021

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

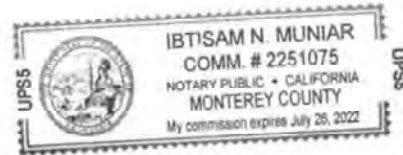
State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

HN



IBTISAM N. MUNIAR (Notary)

(Seal)

## Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document



IN THE HIGH COURT OF DELHI AT NEW DELHI

CIVIL WRIT JURISDICTION

CM NO. OF 2021

IN

WRIT PETITION (CIVIL) NO. OF 2021

IN THE MATTER OF:

WHATSAPP LLC

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

**AFFIDAVIT ON BEHALF OF PETITIONER**

I, Brian Hennessy, son of Mark Hennessy, aged about 41 years, Power of Attorney holder of the Petitioner, WhatsApp LLC ("**WhatsApp**"), having its office at 1601 Willow Road, Menlo Park, California 94025, USA, do hereby solemnly affirm and state as under: :

1. I am the Power of Attorney Holder of WhatsApp and am duly authorized and competent to swear this affidavit on behalf of WhatsApp. I am acquainted with the facts of the present case as derived from the official records maintained in the usual and ordinary course of business, and therefore competent to affirm this affidavit.
2. I have read and understood the contents of the accompanying application and state that the facts stated therein are true to the best of my knowledge and the submissions made therein are based on

legal advice received and believed by me to be true and correct. The contents of the affidavit are true to my personal knowledge.

3. I adopt the contents of the accompanying application part and parcel of my affidavit, the same not being reproduced herein for the sake of brevity.

SOLEMNLY AFFIRMED AT 22401 SAN VICENTE AVENUE, SAN JOSE, CALIFORNIA 95120, USA ON THIS 21ST DAY OF MAY 2021.



DEPONENT

**VERIFICATION**

I, the Deponent above named, do hereby verify the contents of the aforesaid Affidavit are true and correct based on the records and no part of it is false and nothing material has been concealed therefrom.

Verified by me at 22401 San Vicente Avenue, San Jose, California 95120, USA on this 21st day of May 2021.



DEPONENT

## Jurat

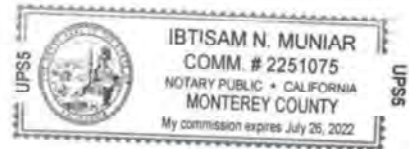
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibti Sam N. Muniar (Notary)

(Seal)

Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

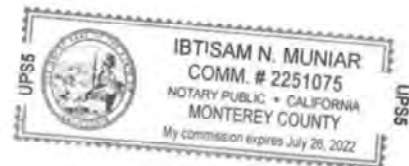
State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibtisam N. Muniar (Notary)



(Seal)

### Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document

IN THE HON'BLE HIGH COURT OF DELHI  
(EXTRAORDINARY WRIT JURISDICTION)

I.A. NO. \_\_\_\_\_ OF 2021

IN

WRIT PETITION (CIVIL) NO. \_\_\_\_ OF 2021

**IN THE MATTER OF:**

WHATSAPP LLC

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

**APPLICATION ON BEHALF OF THE PETITIONER  
UNDER SECTION 151 OF THE CODE OF CIVIL  
PROCEDURE, 1908 FOR EXEMPTION FROM FILING  
THE LEGIBLE COPIES OF THE DIM ANNEXURES,  
PROPER LEFT HAND MARGIN OF DOCUMENTS AND  
FONT SIZE OF ANNEXURES**

**MOST RESPECTFULLY SHOWETH:**

1. The accompanying Writ Petition (“**Petition**”) has been filed to challenge the validity of Impugned Rule 4(2) of the Information Technology (Intermediary Guidelines and

Digital Media Ethics Code) Rules, 2021 (“**Intermediary Rules**”).

2. That the contents of the Petition are not being reproduced herein, for the sake of brevity. However, the same may be read as part of this Application.
3. In view of the exigency in the matter, the Petitioner is praying for an exemption from filing the legible copies of the dim annexures, proper left hand margin of documents, and proper font size of annexures.
4. Petitioner submits that no prejudice will be caused to Respondents if the application is allowed.
5. This application is bonafide and in the interest of justice.

### **PRAYER**

In view of the facts and circumstances stated hereinabove, it is most respectfully prayed that this Hon'ble Court may kindly be pleased to:

- A. Exempt the Petitioner from filing the legible copies of the dim annexures, proper left hand margin of documents and proper font size of annexures filed along with the Petitioner; and

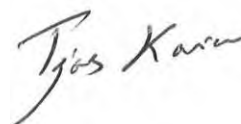
- B. Pass any further orders that this Hon'ble Court may deem fit and proper in light of the facts and circumstances of the present case.

FOR WHICH ACT OF KINDNESS THE PETITIONER SHALL AS DUTY  
BOUND FOREVER PRAY



PETITIONER

FILED THROUGH



M/S. SHARDUL AMARCHAND MANGALDAS

& CO., ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216, OKHLA

INDUSTRIAL ESTATE, PHASE-III, NEW

DELHI -110020

EMAIL: TEJAS.KARIA@AMSSHARDUL.COM

PAVIT.KATOCH@AMSSHARDUL.COM

MOB: 9871790537

PLACE: NEW DELHI

DATE: 21 MAY 2021

## Jurat

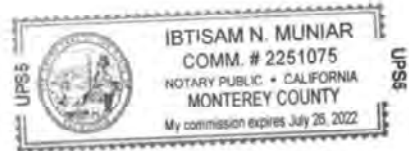
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibtisam N. Muniar (Notary)

(Seal)

## Description of Attached Document

\_\_\_\_\_  
Title or Type of Document\_\_\_\_\_  
Number of Pages\_\_\_\_\_  
Date of Document



IN THE HIGH COURT OF DELHI AT NEW DELHI

CIVIL WRIT JURISDICTION

CM NO. OF 2021

IN

WRIT PETITION (CIVIL) NO. OF 2021

IN THE MATTER OF:

WHATSAPP LLC

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

**AFFIDAVIT ON BEHALF OF PETITIONER**

I, Brian Hennessy, son of Mark Hennessy, aged about 41 years, Power of Attorney holder of the Petitioner, WhatsApp LLC ("**WhatsApp**"), having its office at 1601 Willow Road, Menlo Park, California 94025, USA, do hereby solemnly affirm and state as under: :

1. I am the Power of Attorney Holder of WhatsApp and am duly authorized and competent to swear this affidavit on behalf of WhatsApp. I am acquainted with the facts of the present case as derived from the official records maintained in the usual and ordinary course of business, and therefore competent to affirm this affidavit.
2. I have read and understood the contents of the accompanying application and state that the facts stated therein are true to the best of my knowledge and the submissions made therein are based on

legal advice received and believed by me to be true and correct. The contents of the affidavit are true to my personal knowledge.

3. I adopt the contents of the accompanying application part and parcel of my affidavit, the same not being reproduced herein for the sake of brevity.

SOLEMNLY AFFIRMED AT 22401 SAN VICENTE AVENUE, SAN JOSE, CALIFORNIA 95120, USA ON THIS 21ST DAY OF MAY 2021.



DEPONENT

**VERIFICATION**

I, the Deponent above named, do hereby verify the contents of the aforesaid Affidavit are true and correct based on the records and no part of it is false and nothing material has been concealed therefrom.

Verified by me at 22401 San Vicente Avenue, San Jose, California 95120, USA on this 21st day of May 2021.



DEPONENT

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

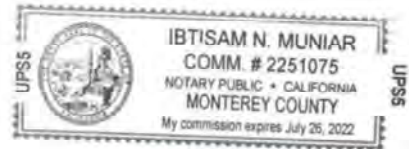
County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibtisam N. Muniar

(Notary)



(Seal)

## Description of Attached Document

\_\_\_\_\_  
Title or Type of Document\_\_\_\_\_  
Number of Pages\_\_\_\_\_  
Date of Document

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

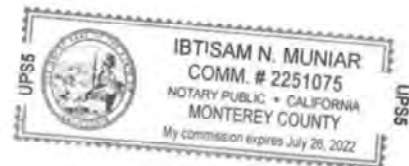
State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibtisam N. Muniar (Notary)



(Seal)

Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document

**IN THE HON'BLE HIGH COURT OF DELHI  
(EXTRAORDINARY WRIT JURISDICTION)**

**I.A. NO. \_\_\_\_\_ OF 2021**

**IN**

**WRIT PETITION (CIVIL) NO. \_\_\_\_ OF 2021**

**IN THE MATTER OF:**

**WHATSAPP LLC**

**...PETITIONER**

**VERSUS**

**UNION OF INDIA**

**... RESPONDENT**

**APPLICATION UNDER SECTION 151 OF THE CODE OF  
CIVIL PROCEDURE 1908, PRAYING FOR EXEMPTION  
FROM FILING APOSTILLED PETITION,  
APPLICATIONS AND AFFIDAVITS**

**MOST RESPECTFULLY SHOWETH:**

1. The accompanying Writ Petition (“**Petition**”) has been filed to challenge the validity of Impugned Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**Intermediary Rules**”)
2. That the contents of the Petition are not being reproduced herein, for the sake of brevity. However, the same may be read as part of this Application.
3. Petitioner’s authorised signatory currently resides in the State of California, United States, where stay-at-home orders have been issued in response to the COVID-19 outbreak therefore

the Petition, accompanying applications, and supporting affidavits could not be apostilled due to the social distancing requirements of such stay-at-home orders, and due to the Secretary of State's delay in processing apostille requests. The Secretary of State in California is operating at limited capacity due to COVID-19 related restrictions, and therefore, is processing apostille requests at a much slower pace than usual.

4. That under the present exigent circumstances, Petitioner respectfully requests that this Hon'ble Court grant Petitioner an exemption from filing apostilled versions of its Petition, accompanying applications and supporting affidavits.
5. Petitioner undertakes to duly furnish apostilled versions of its Petition, accompanying applications, and supporting affidavits as and when it becomes reasonably safe and possible to do so.
6. Petitioner submits that no prejudice will be caused to Respondent if the present Application is allowed.
7. The present Application is made *bona fide* and in the interests of justice and equity.

### **PRAYER**

In view of the foregoing facts and circumstances, it is therefore most respectfully prayed that this Hon'ble Court may be graciously pleased to:-

- A. exempt the Petitioner from filing the apostilled version of Petition, accompanying applications, and supporting affidavits; and

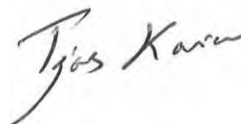
- B. Pass any further orders that this Hon'ble Court may deem fit and proper in light of the facts and circumstances of the present case.

FOR WHICH ACT OF KINDNESS THE PETITIONER SHALL AS DUTY  
BOUND FOREVER PRAY



PETITIONER

FILED THROUGH



M/S. SHARDUL AMARCHAND MANGALDAS  
& CO., ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216, OKHLA  
INDUSTRIAL ESTATE, PHASE-III, NEW

DELHI -110020

EMAIL: TEJAS.KARIA@AMSSHARDUL.COM

PAVIT.KATOCH@AMSSHARDUL.COM

MOB: 9871790537

PLACE: NEW DELHI

DATE: 21 MAY 2021

## Jurat

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

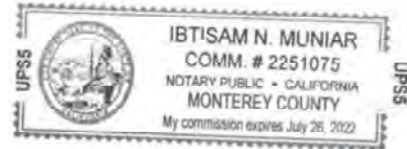
State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

IB



IBTISAM N. MUNIAR (Notary)

(Seal)

### Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document



IN THE HIGH COURT OF DELHI AT NEW DELHI

CIVIL WRIT JURISDICTION

CM NO. OF 2021

IN

WRIT PETITION (CIVIL) NO. OF 2021

IN THE MATTER OF:

WHATSAPP LLC

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

**AFFIDAVIT ON BEHALF OF PETITIONER**

I, Brian Hennessy, son of Mark Hennessy, aged about 41 years, Power of Attorney holder of the Petitioner, WhatsApp LLC ("**WhatsApp**"), having its office at 1601 Willow Road, Menlo Park, California 94025, USA, do hereby solemnly affirm and state as under: :

1. I am the Power of Attorney Holder of WhatsApp and am duly authorized and competent to swear this affidavit on behalf of WhatsApp. I am acquainted with the facts of the present case as derived from the official records maintained in the usual and ordinary course of business, and therefore competent to affirm this affidavit.
2. I have read and understood the contents of the accompanying application and state that the facts stated therein are true to the best of my knowledge and the submissions made therein are based on

legal advice received and believed by me to be true and correct. The contents of the affidavit are true to my personal knowledge.

3. I adopt the contents of the accompanying application part and parcel of my affidavit, the same not being reproduced herein for the sake of brevity.

SOLEMNLY AFFIRMED AT 22401 SAN VICENTE AVENUE, SAN JOSE, CALIFORNIA 95120, USA ON THIS 21ST DAY OF MAY 2021.



DEPONENT

**VERIFICATION**

I, the Deponent above named, do hereby verify the contents of the aforesaid Affidavit are true and correct based on the records and no part of it is false and nothing material has been concealed therefrom.

Verified by me at 22401 San Vicente Avenue, San Jose, California 95120, USA on this 21st day of May 2021.



DEPONENT

## Jurat

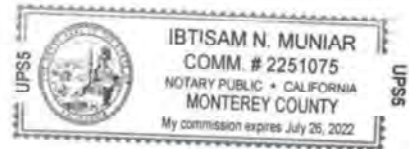
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibti Sam N. Muniar (Notary)

(Seal)

Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document

## Jurat

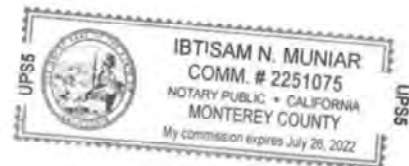
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_

Ibtisam N. Muniar (Notary)

(Seal)

## Description of Attached Document

\_\_\_\_\_  
Title or Type of Document\_\_\_\_\_  
Number of Pages\_\_\_\_\_  
Date of Document

**IN THE HIGH COURT OF DELHI AT NEW DELHI****CIVIL WRIT JURISDICTION****WRIT PETITION (CIVIL) NO.      OF 2021****IN THE MATTER OF:****WHATSAPP LLC****...PETITIONER****VERSUS****UNION OF INDIA****... RESPONDENT****VAKALATNAMA**

KNOW ALL to whom this shall come that I, Brian Hennessy, Power of Attorney holder of the Petitioner, WhatsApp LLC (formerly known as WhatsApp Inc.), a limited liability company registered under the laws of the State of Delaware, U.S.A. and having its registered office at 1601 Willow Road, Menlo Park, California 94025 (U.S.A.), appoint Mr. Tejas Karia (G/1390/2000) and Mr. Pavit Singh Katoch (KAR/1712/2007) of M/s. SHARDUL AMARCHAND MANGALDAS & CO., ADVOCATES & SOLICITORS, Amarchand Towers, 216, Okhla Industrial Estate, Phase-III, New Delhi -110020 (Tel: 41590700: 40606060 Fax: 26924900) to be the Advocates for me

in the abovementioned case, to do all the following acts, deeds, and things, or any of them, that is to say:

1. TO ACT, appear, and plead in the abovementioned case in this Court or any other Tribunal/Court in which the same may be tried or heard in the first instance, or in Appeal, Letters Patent Appeal, Review, Revision of Execution, or in any other stage of its progress until its final decision;
2. TO PRESENT Petitions, Caveats, Pleadings, Appeals, Letters Patent Appeal, Petitions for Appeal to Supreme Court, Cross-Objections, or Petitions for Execution, Review, Revision, Withdrawal, Compromise, or other Petitions, Affidavits, or other documents as shall be deemed necessary or advisable for the prosecution of the said cause in all of its stages;
3. TO WITHDRAW or compromise the said cause, or submit to arbitration any differences or disputes that shall arise touching or in any manner relating to the said cause;
4. TO RECEIVE monies and grant receipts thereof and to do all other acts and things which may be necessary to be done for the progress and in the course of the prosecution of the said cause;
5. TO EMPLOY any other Legal Practitioner authorising them to exercise the power and authority hereby conferred on the Advocates whenever they may think fit to do so;

AND I/WE hereby agree to ratify whatever acts of the Advocates or their substitute/s responsible for the result of the said cause, in consequence of their absence from the Court when the said cause is called up for hearing.

AND I/WE hereby agree that in the event of the whole or any part of the fees agreed by me/us to be paid to the Advocates remaining unpaid, they shall be entitled to withdraw from the prosecution of the said cause until the same is paid.

IN WITNESS WHEREOF I/WE hereunto set my/our hand to the present content, which has been explained to and understood by me/us, on this 21st day of May 2021.

Accepted subject to the terms regarding fees payable to M/s.

SHARDUL AMARCHAND MANGALDAS & CO.

  
Client

Signature:  
Name: Tejas D. Karia  
Advocate  
Enrolment No.: G/1390/2000

Signature identified by  
Signature:  
Name:  
Advocate Enrolment  
No.:

M/s Shardul Amarchand Mangaldas & Co.



## Jurat

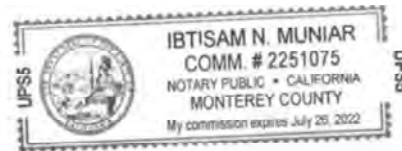
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Santa Clara

Subscribed and sworn to (or affirmed) before me this 21<sup>st</sup> day of May, 2021,  
by Brian Hennessy, proved to me on the basis of satisfactory evidence  
to be the person(s) who appeared before me.

Signature \_\_\_\_\_



ibtisam N. Muniar (Notary)

(Seal)

Description of Attached Document

\_\_\_\_\_  
Title or Type of Document

\_\_\_\_\_  
Number of Pages

\_\_\_\_\_  
Date of Document



**BY THIS POWER OF ATTORNEY** made on November 14, 2019, **WHATSAPP INC.**, a Delaware Limited Liability company whose address is 1601 Willow Road, Menlo Park, CA 94025 (the "**Company**") **HEREBY**:

1. Appoints Brian Hennessy, s/o Mark Hennessy, Director and Associate General Counsel of WhatsApp Inc., whose business address is 1601 Willow Road, Menlo Park, CA 94025 ("the Attorney") as its and lawful attorney to act on behalf of the Company and in its name to execute, sign and/or deliver any documents (including without limitation any agreements, instruments, contracts, documents, acts of deeds, complaints, suits, affidavits, petitions, and any other documents required in the prosecution or defense of legal proceedings) for use in the territories of India only.
2. Declares that all documents, acts and things which shall be executed or done by the Attorney by virtue of this Power of Attorney shall be as good, valid and effectual to all intents and purposes whatsoever as if they had been executed or done by the Company.
3. Ratifies and confirms and agrees to ratify and confirm from time to time and at all times whatever the Attorney shall do or purport to do or cause to be done by virtue of this Power of Attorney.
4. Declares that this Power of Attorney shall be valid from the date hereof until such time as it is expressly revoked by the Company (whichever the earlier) **PROVIDED ALWAYS** that the Power of Attorney shall expire automatically upon the Attorney ceasing to be an employee of Facebook, Inc. or any of its subsidiaries.
5. Declares that this Power of Attorney is in addition to, and not in supersession of, any other authorization in favour of the Attorney.
6. Declares that this Power of Attorney shall in all respects be governed by and construed in accordance with the laws of the state of California.

IN WITNESS WHEREOF the Company has duly executed this Power of Attorney on the date first above written.

Signed for and on behalf of

WHATSAPP INC.


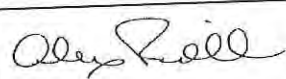


**David W. Kling**

Secretary of WhatsApp Inc.

# State of California Secretary of State

This Certificate is not valid for use anywhere within the United States of America, its territories or possessions.

<b>APOSTILLE</b> (Convention de La Haye du 5 octobre 1961)			
<b>1. Country:</b> Pays / País:	United States of America		
<b>This public document</b> Le présent acte public / El presente documento público			
<b>2. has been signed by</b> a été signé par ha sido firmado por	K. D. Strand Kiar		
<b>3. acting in the capacity of</b> agissant en qualité de quien actúa en calidad de	Notary Public, State of California		
<b>4. bears the seal / stamp of</b> est revêtu du sceau / timbre de y está revestido del sello / timbre de	K. D. Strand Kiar , Notary Public, State of California		
<b>Certified</b> Attesté / Certificado			
<b>5. at</b> à / en	Los Angeles, California	<b>6. the</b> le / el día	18th day of November 2019
<b>7. by</b> par / por	Secretary of State, State of California		
<b>8. N°</b> sous n° bajo el número	22112		
<b>9. Seal / stamp:</b> Sceau / timbre: Sello / timbre:		<b>10. Signature:</b> Signature: Firma:	

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

This Apostille does not certify the content of the document for which it was issued.

To verify the issuance of this Apostille, see: [apostille-search.sos.ca.gov/](http://apostille-search.sos.ca.gov/).

This certificate does not constitute an Apostille under the Hague Convention of 5 October 1961, when it is presented in a country which is not a party to the Convention. In such cases, the certificate should be presented to the consular section of the mission representing that country.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

Cette Apostille ne certifie pas le contenu de l'acte pour lequel elle a été émise.

Cette Apostille peut être vérifiée à l'adresse suivante: [apostille-search.sos.ca.gov/](http://apostille-search.sos.ca.gov/).

Ce certificat ne constitue pas une Apostille en vertu de la Convention de La Haye du 5 Octobre 1961, lorsque présenté dans un pays qui n'est pas partie à cette Convention. Dans ce cas, le certificat doit être présenté à la section consulaire de la mission qui représente ce pays.

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado y, en su caso, la identidad del sello o timbre del que el documento público esté revestido.

Esta Apostilla no certifica el contenido del documento para el cual se expidió.

Esta Apostilla se puede verificar en la dirección siguiente: [apostille-search.sos.ca.gov/](http://apostille-search.sos.ca.gov/).

Este certificado no constituye una Apostilla en virtud del Convenio de La Haya de 5 de octubre de 1961 cuando se presenta en un país que no es parte del Convenio. En estos casos, el certificado debe ser presentado a la sección consular de la misión que representa a ese país.



# CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

CIVIL CODE § 1189

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California )

County of San Mateo )

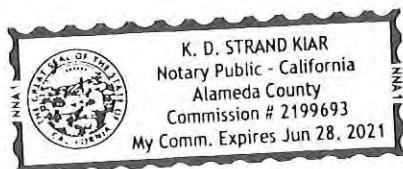
On Nov 14, 2019 before me, K. D. Strand Kiar, Notary Public  
Date Here Insert Name and Title of the Officer

personally appeared David W. Kling  
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.



Signature [Signature]  
Signature of Notary Public

Place Notary Seal Above

## OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

### Description of Attached Document

Title or Type of Document: POA - Document Date: Nov 14, 2019  
Number of Pages: 1 Signer(s) Other Than Named Above: \_\_\_\_\_

### Capacity(ies) Claimed by Signer(s)

Signer's Name: David W. Kling  
☒ Corporate Officer — Title(s): Secretary  
☐ Partner — ☐ Limited ☐ General  
☐ Individual ☐ Attorney in Fact  
☐ Trustee ☐ Guardian or Conservator  
☐ Other: \_\_\_\_\_  
Signer Is Representing: WhatsApp Inc

Signer's Name: \_\_\_\_\_  
☐ Corporate Officer — Title(s): \_\_\_\_\_  
☐ Partner — ☐ Limited ☐ General  
☐ Individual ☐ Attorney in Fact  
☐ Trustee ☐ Guardian or Conservator  
☐ Other: \_\_\_\_\_  
Signer Is Representing: \_\_\_\_\_

**From:** [Katoch, Pavit Singh](#)  
**To:** ["webmaster@meity.gov.in"](mailto:webmaster@meity.gov.in)  
**Cc:** [Karia, Tejas](#)  
**Subject:** RE: WhatsApp LLC v. Union of India - Delhi High Court  
**Date:** Tuesday, 25 May 2021 9:10:47 PM  
**Attachments:** [WhatsApp LLC v. Union of India.pdf](#)  
**Importance:** High

---

## **PROOF OF SERVICE**

To,

1. Union of India  
Through the Secretary  
Ministry of Electronics and IT  
Electronics Niketan, 6, CGO Complex,  
Lodhi Road, New Delhi 110 003  
Email: [webmaster@meity.gov.in](mailto:webmaster@meity.gov.in)

### **RE: WHATSAPP LLC v. UNION OF INDIA – Delhi High Court**

Dear Sir,

We represent the Petitioner, WhatsApp LLC in the captioned matter.

Please see attached a copy of the writ petition that we are filing, which is served on you by way of present email. The Petition is accompanied by an application for interim relief.

Please note that the present email shall be submitted before the Hon'ble Court as proof of advance service to the Union of India. Request you to take note of the same.

Best Regards,

**Pavit Singh Katoch, Advocate (KAR/1712/2007)**

**On behalf of Shardul Amarchand Mangaldas & Co.  
Advocates for the Petitioner, WhatsApp LLC**