

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

W.P. (C) No. _____ of 2021

IN THE MATTER OF:

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

...RESPONDENT


INDEX

S.No.	Particulars	Page Nos.
1.	Court Fees	1
2.	Notice of Motion	2 – 3
3.	Memo of Parties	4 – 5
4.	Synopsis with List of Dates and Events	6 – 12
5.	Writ Petition on behalf of Facebook, Inc. under Article 226 of the Constitution of India, 1950, for issuance of writ of mandamus or any other writ as deemed appropriate.	13 - 45

6.	<u>ANNEXURE-P-1:</u> Copy of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.	46 – 61
7.	<u>ANNEXURE-P-2:</u> Copy of the description of Messenger service on Petitioner’s website.	62
8.	<u>ANNEXURE-P-3:</u> Copy of Petitioner’s Messenger Help Centre webpage.	63 - 64
9.	<u>ANNEXURE-P-4:</u> Copy of Petitioner's safety guidelines.	65 – 70
10.	<u>ANNEXURE-P-5:</u> Copy of Petitioner's LEA request portal.	71
11.	<u>ANNEXURE-P-6:</u> Copy of the Information Technology (Intermediaries Guidelines) 2011.	72 – 75
14.	<u>ANNEXURE-P-7:</u> 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).	76 – 82
15.	<u>C.M. NO. OF 2021</u> Application under Section 151 Code of Civil Procedure, 1908, for interim relief along with affidavit.	83 – 93

16.	<u>C.M. NO.</u> <u>OF 2021</u> Application under Section 151 Code of Civil Procedure, 1908, praying for exemption from filing legible copies of dim annexures, proper left hand margin of documents and font size of annexures along with affidavit.	94 – 101
17.	<u>C.M. NO.</u> <u>OF 2021</u> Application under Section 151 Code of Civil Procedure, 1908 praying for exemption from filing apostilled petition, applications and affidavits along with affidavit.	102 – 109
18.	Vakalatnama along with Power of Attorney	110 - 118
19.	Proof of service	119

FILED THROUGH:



MR. AJIT WARRIER /MR. GAUHAR MIRZA
ENROL. NO.- [REDACTED]
SHARDUL AMARCHAND MANGALDAS & CO
ADVOCATES FOR THE PETITIONER
216, OKHLA INDUSTRIAL AREA, PHASE-III,
NEW DELHI-110020

EMAIL: [REDACTED]

PHONE [REDACTED]

DATE: 25 MAY 2021
PLACE: NEW DELHI

COURT FEES

Forbes^{INDIA}

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

IN THE MATTER OF:

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

NOTICE OF MOTION

To

1. Union of India

Through its Secretary

Ministry of Electronics & Information Technology,

Electronics Niketan, 6, CGO Complex,

Lodhi Road, New Delhi - 110023.

Email: webmaster@meity.gov.in

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

Petitioner, through



MR. AJIT WARRIER /MR. GAUHAR MIRZA

ENROL. NO.- [REDACTED]

SHARDUL AMARCHAND MANGALDAS & CO

ADVOCATES FOR THE PETITIONER

216, OKHLA INDUSTRIAL AREA, PHASE-III,

NEW DELHI-110020

EMAIL [REDACTED]

PHONE: [REDACTED]

DATE: 25 MAY 2021

PLACE: NEW DELHI

INDIA
Forbes

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

IN THE MATTER OF:

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

MEMO OF PARTIES

IN THE MATTER OF:

FACEBOOK, INC.

1 HACKER WAY, MENLO PARK, CALIFORNIA 94025,
USA

EMAIL 

...PETITIONER

VERSUS

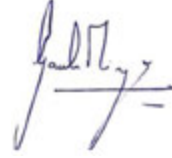
UNION OF INDIA

THROUGH ITS SECRETARY,
MINISTRY OF ELECTRONICS AND INFORMATION
TECHNOLOGY ELECTRONICS NIKETAN,
6, CGO COMPLEX, LODHI ROAD,
NEW DELHI - 110023.

EMAIL: webmaster@meity.gov.in

...RESPONDENT

Petitioner, through



MR. AJIT WARRIER /MR. GAUHAR MIRZA
ENROL. NO.- [REDACTED]
SHARDUL AMARCHAND MANGALDAS & CO
ADVOCATES FOR THE PETITIONER
216, OKHLA INDUSTRIAL AREA, PHASE-III,
NEW DELHI-110020
EMAIL [REDACTED]
PHONE: [REDACTED]

DATE: 25 MAY 2021

PLACE: NEW DELHI

INDIA
Forbes

SYNOPSIS

India's commitment to the fundamental rights of Indian citizens to privacy and freedom of speech is reflected in its Constitutional guarantees and in landmark decisions by the Hon'ble Supreme Court recognizing the rights to privacy and free speech over the internet.

Petitioner Facebook, Inc. ("**Petitioner**") is also committed to promoting the privacy and free speech of everyone who uses the Facebook service, which is reflected in its robust policies that adopt global best practices to protect user privacy and promote a safe online experience. Every day, people use Facebook to share their experiences, connect with friends and family, and build communities. Facebook is a service for more than two billion people, including millions of users in India, to freely express themselves across countries and cultures and in dozens of languages. Petitioner recognizes how important it is for Facebook to be a place where people feel empowered to communicate.

While Petitioner primarily offers a social media platform, it also provides the "Messenger" messaging service, which helps people stay close with those who matter most, from anywhere and on any device. Messenger offers a feature called Facebook Secret Conversations. As stated on Facebook's website: "*With secret conversations, you can send: Messages, Pictures, Stickers, Videos, Voice recordings. . . . A secret conversation in Messenger is encrypted end-to-end, which means the messages are intended just for you and the other person—not anyone else, including [Petitioner].*" (available at:

<https://www.facebook.com/help/messenger-app/1084673321594605>)

On 25 February 2021, the Central Government (“**Respondent**”) issued the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules 2021 (“**2021 Guidelines**”). Rule 4(2) imposes a new duty on “*significant social media intermediaries*” (“**SSMIs**”) “*providing services primarily in the nature of messaging*” to “*enable the identification of the **first originator** of the information on its computer resource*” in India as may be required by a valid order from a court or authorized government agency.

Impugned Rule 4(2) forces Petitioner to break end-to-end encryption on its Facebook Secret Conversations feature and undermines Constitutional guarantees of privacy and free speech. Indeed, since there is no way to predict which communications the Government will later seek to identify, intermediaries would have to build mechanisms to identify the first originator of *every* end-to-end encrypted communication sent on their services in India. Further, as the rule does not include any time limit, every such communication by every user in India will *forever* be linked to their identities -- including the vast majority of such communications which are sent by law-abiding Indian citizens.

Petitioner is constrained to challenge Rule 4(2) on the following principal grounds:

- Rule 4(2) violates the fundamental right to *privacy*, which includes the right to anonymity. The rule violates users’ right to remain anonymous and eliminates their ability to control

what information is disclosed to third parties, without satisfying *any*, let alone *all three*, of the mandatory requirements laid down in *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (“*Puttaswamy I*”) to justify an infringement of privacy:

- There is no valid statute authorizing the invasion of privacy. (*Ramlila Maidan Incident In re*, (2012) 5 SCC 1 at para 30).
- There is no guarantee against arbitrary State action, including no prior judicial review. (*Puttaswamy I* at para 310; *K.S. Puttaswamy v. UOI*, (2019) 1 SCC 1). The rule is not proportional, as the privacy infringement is not “*through the least restrictive alternatives.*” (*Kerala State Beverages (M&M) Corp. Ltd. v. P.P. Suresh*, (2019) 9 SCC 710 at para 30).
- Rule 4(2) violates users’ fundamental right to ***freedom of speech and expression***. The ability to exercise this right depends on the ability to maintain one’s privacy, which is necessary to protect people from retaliation for expressing unpopular but lawful opinions, challenging mainstream views, and even reporting unlawful activities. Rule 4(2) undermines privacy for users using encrypted messaging services and features in India, thereby chilling their lawful speech. (*Shreya Singhal v. Union of India*, (2015) 5 SCC 1 at para 90; *S. Khushboo v. Kanniammal*, (2010) 5 SCC 600 at para 47).

- Rule 4(2) is *ultra vires* the IT Act, as the IT Act does not vest Respondent with any power to impose a duty on intermediaries to build mechanisms that would allow the identification of the “*first originator*” of every communication in India on their platforms, and certainly not if it requires breaking end-to-end encryption as is the case with Rule 4(2). Rule 4(2) imposes a duty far beyond intermediaries’ “*due diligence*” obligations under the IT Act and would require Petitioner to change the fundamental nature of its platform.

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

LIST OF DATES

Date	Particulars
17 October 2000	The IT Act was notified.
2004	Petitioner began operating the Facebook service which provides a free and voluntary online social networking service that allows users to connect and share information with their friends and family.
5 February 2009	The Information Technology (Amendment) Act, 2008 (“ Amendment ”), 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.
11 April 2011	Respondent published the Prior Intermediaries Rules in the Official Gazette.
24 March 2015	The Hon’ble Supreme Court, in its decision in <i>Shreya Singhal</i> , ruled <i>inter alia</i> that Section 79 is an exemption provision under which intermediaries are entitled to exemption from liability provided that they observe due diligence and satisfy the conditions set forth in the Prior Intermediaries Rules. The Hon’ble Supreme Court further held that intermediaries may not be

	compelled to determine the lawfulness of content.
24 August 2017	The Hon'ble Supreme Court, in its decision in <i>Puttaswamy I</i> , ruled <i>inter alia</i> that the right to privacy is a fundamental right protected under Article 21 of the Constitution of India.
14 July 2018	Petitioner became the relevant data controller of the Facebook service with respect to India users under a change in the terms of service dated 19 April 2018, fully effective on or around 14 July 2018.
24 December 2018	Respondent published the Draft Information Technology [Intermediaries Guidelines (Amendment)] Rules, 2018 (“ Proposed Amendments ”). Respondent also commenced a consultative process by inviting comments and counter-comments to the Proposed Amendments.
24 December 2018 to 14 February 2019	Respondent received several comments and counter-comments from a variety of stakeholders, many of whom were, among other things, especially critical of requiring intermediaries to identify originator information. Among the comments was a letter from the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Professor

	David Kaye (“ David Kaye Letter ”), which highlighted concerns regarding the Proposed Amendments, including the dangers of requiring intermediaries to identify originator information.
25 February 2021	Respondent published the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Rules) in the Official Gazette. Part I and Part II of the Intermediary Rules, which includes Rule 4(2) violates the Constitution and the IT Act and is being challenged under the present petition.
25 May 2021	Being aggrieved by Impugned Rule 4(2), Petitioner has filed this Writ Petition on behalf of itself, and in a representative capacity for violation of the rights of many Indian users of Facebook under Article 14, 19 and 21 of the Constitution.

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

IN THE MATTER OF:

FACEBOOK, INC.

1 HACKER WAY, MENLO PARK,

CALIFORNIA 94025, USA ... 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 Facebook, Inc. (“**Petitioner**”) respectfully approaches this Hon’ble Court to challenge the validity of Impugned Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**Intermediary Rules**”). The Intermediary Rules were prescribed by Respondent on 25 February 2021 under the Information Technology Act, 2000 (“**IT Act**”). A copy of the Intermediary Rules and IT Act are enclosed herewith as **Annexure P-1** to this Petition.
2. Petitioner challenges Rule 4(2) on the grounds that, among other things, it (i) violates the fundamental privacy and free speech rights of Indian citizens by forcing intermediaries to build mechanisms so that, when ordered by Respondent, they can provide Respondent with the identity of the “*first originator*” of any information in India on end-to-end encrypted services; and (ii) exceeds the rulemaking authority granted to Respondent under the IT Act. Petitioner is therefore constrained to challenge Rule 4(2) as explained below.

BACKGROUND REGARDING PETITIONER

3. Petitioner is a company incorporated under the laws of the State of Delaware, United States of America. Petitioner is located at 1 Hacker Way, Menlo Park, California 94025, in the United States of America. Petitioner is the data controller for user-generated content appearing on the Facebook service, i.e., the website www.facebook.com and applications for mobile devices and tablets in India.
4. Petitioner provides Facebook, an online social networking service that gives people the power to build community and brings the world closer together. Users log into their Facebook accounts to create, upload, and share posts, comments, photos, videos, and other content directly onto Facebook. Every day, people use Facebook to share their experiences, connect with friends and family, and build communities. Facebook is a service for people to freely express themselves across countries and cultures and in dozens of languages. Petitioner recognizes how important it is for Facebook to be a place where people feel empowered to communicate.
5. Petitioner is committed to promoting the privacy and freedom of speech of everyone who uses the Facebook service. This is reflected in robust policies that adopt global best practices to protect user privacy and promote a safe online experience. Indeed, Facebook expressly prohibits users from sharing personal information without the user's consent, and provides users with a means to report when they believe that their privacy has been compromised. Users

are empowered to choose what to delete, share, and who to share it with, and are provided with tools to protect their privacy.

6. While Petitioner primarily offers a social media platform, it also provides the “Messenger” messaging service, which *“helps [people] stay close with those who matter most, from anywhere and on any device.”* (Available at: <https://www.facebook.com/messenger/about/>). Messenger provides a **“Secret Conversations”** feature. As stated on Facebook’s website: *“With secret conversations, you can send: Messages, Pictures, Stickers, Videos, Voice recordings. . . . A secret conversation in Messenger is encrypted end-to-end, which means the messages are intended just for you and the other person—not anyone else, including [Petitioner].”* (Available at: <https://www.facebook.com/help/messenger-app/1084673321594605>). A copy of the description of Messenger service on Petitioner’s website and the Messenger Help Centre webpage are enclosed herewith as **Annexure P-2** and **Annexure P-3** to this Petition.
7. Petitioner also recognizes the critical role of law enforcement authorities (“LEAs”) in keeping the general public safe and is committed to cooperating with LEAs in India in accordance with its policies and applicable law. To that end:

- i. Petitioner has a dedicated team that works closely with LEAs in India.
- ii. Petitioner has taken steps to provide Indian LEAs with training and information regarding the proper submission of requests.
- iii. Petitioner has well-documented, detailed guidelines for handling LEA requests (publicly available at <https://www.facebook.com/safety/groups/law/guidelines>).
- iv. Petitioner has a portal exclusively for LEAs to request information (available at <https://www.facebook.com/records>).

A copy of Petitioner's safety guidelines and LEA request portal are enclosed herewith as **Annexure P-4** and **Annexure P-5** to this Petition.

“DUE DILIGENCE” GUIDELINES FOR INTERMEDIARIES

8. Intermediaries like Petitioner are entitled to statutory immunity from liability for hosting third party content if certain “due diligence” guidelines are observed. Specifically, Section 79 of the IT Act — entitled “*INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN*

CASES” — provides that “*an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him*” if certain due diligence guidelines are observed. Until recently, these due diligence guidelines were set forth in the Information Technology (Intermediaries Guidelines) Rules, 2011, which were prescribed pursuant to Section 79(2). A copy of the Information Technology (Intermediaries Guidelines) Rules, 2011 is enclosed herewith as **Annexure P-6** to this Petition.

9. Respondent, the Union of India through its Secretary, the Ministry of Electronics and Information Technology (“MeitY”), is responsible for matters relating to cyber laws and the administration of the IT Act and other information technology related laws. Respondent is the “*State*” within the meaning of Article 12 of the Constitution. On 25 February 2021, Respondent prescribed the Intermediary Rules, which set forth the due diligence guidelines that intermediaries must observe to maintain their immunity under Section 79.

CHALLENGE TO IMPUGNED RULE 4(2)

10. Petitioner, by this writ petition, challenges Impugned Rule 4(2), requiring “*significant social media intermediaries*” (“SSMIs”) “*providing services primarily in the nature of messaging*” to enable the identification of the “*first originator*” of information in India on their platforms, when

requested in a valid order from a Court or authorized government agency under Section 69 of the IT Act.

11. 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.”

12. Rule 4(2) infringes the rights of Petitioner under *inter alia* Article 14 of the Constitution, and the rights of Indian

citizens who use the Secret Conversations messaging feature under Articles 14, 19, and 21 of the Constitution. Further, Petitioner and these users have the same interest in this petition with respect to Rule 4(2). Petitioner craves leave of this Hon'ble Court to treat this petition as one filed not only on behalf of Petitioner itself but in a representative capacity on behalf of these users in India, in accordance with the principles set out in Order I Rule 8 of the Code of Civil Procedure 1908, as the Hon'ble Supreme Court has done in previous instances. (See, e.g., *Food Corp. of India Worker's Union v. Food Corp. of India & Ors.*, (1985) 2 SCC 294 at paras 2, 17).

13. This petition raises important questions of law regarding (i) the application of the rights of privacy and freedom of speech and expression guaranteed under the Indian Constitution along with the safeguards provided under Articles 14, 19, and 21, *i.e.*, the golden triangle, and (ii) the authority or lack of authority of Respondent under the IT Act to prescribe Rule 4(2).

GROUNDS

14. The law is well-settled that subordinate legislation like Rule 4(2) “must not be *ultra vires* the Constitution” or “*the parent Act under which it has been made.*” (*Bombay Dyeing and Mfg. v. Bombay Env. Action Grp.*, (2006) 3 SCC 434 at para 104). Indeed, the Hon'ble Supreme Court has observed that it is:

“well-recognized that subordinate legislation can be challenged under 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).”

(State of TN v. P. Krishnamurthy, (2004) 6 SCC 517 at paras 15-16).

15. Rule 4(2) requires SSIMs *“providing services primarily in the nature of messaging”* to enable the identification of the first originator of information in India on their platforms in response to a valid order issued by a Court or authorized government agency under section 69 of the IT Act.
16. At the outset, Petitioner respectfully submits that, while the Facebook social media platform includes a messaging service (Facebook Messenger, including the Secret Conversations end-to-end encrypted messaging feature),

Rule 4(2) does *not* apply to Petitioner because the Facebook service is *not* “*primarily in the nature of messaging*”, as is required to trigger Rule 4(2). Nevertheless, in the event it is determined that Petitioner is subject to Rule 4(2), Petitioner challenges Rule 4(2) on the grounds that it (a) violates the constitutional right to privacy; (b) violates the constitutional right to freedom of speech and expression; (c) is *ultra vires* the IT Act, and (d) violates the principle of data minimisation, all as more fully explained below.

A. Rule 4(2)’s Requirement to “*Enable the Identification of the First Originator of the Information*” in India Violates Users’ Fundamental Right to Privacy

17. The Hon’ble Supreme Court recognized the right to privacy as a fundamental right guaranteed under Article 21 of the Constitution. (*K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (“*Puttaswamy I*”) at paras 375, 644). The Hon’ble Supreme Court later affirmed that “[p]rivacy and confidentiality encompass a bundle of rights including the *right to protect identity and anonymity*”, and that “*privacy as anonymity*” is among the “*three key elements of informational privacy*”. “*Anonymity is where an individual seeks freedom from identification, even when and despite being in a public space*”. (*Central Public Information Officer v. Subhash Chandra Agarwal*, (2020) 5 SCC 481 at para 54, emphasis added).

18. The Hon'ble Supreme Court further recognized that conversations through electronic means (like Petitioner's platform), which are often of an intimate and confidential nature, (i) have become exceedingly common, (ii) form a crucial part of modern life, and (iii) are entitled to protection under Article 21 of the Constitution. (E.g., *People's Union for Civil Liberties v. Union of India & Anr.* (1997) 1 SCC 301 at para 18).
19. Here, Rule 4(2) undermines privacy, including anonymity. Indeed, since there is no way to predict which communications the Government will later seek to identify, Petitioner would have to build mechanisms to identify the first originator of *every* communication sent using Secret Conversations. Further, as the rule does not include any time limit, every such communication by every user in India must *forever* be linked to their identities — including the vast majority of such communications which are sent by law-abiding Indian citizens. Enabling the identification of the first originator of information sent through Secret Conversations in India breaks end-to-end encryption and the privacy principles underlying it.
20. In *Puttaswamy I*, the Hon'ble Supreme Court held that there can be no such intrusion into the fundamental right to privacy unless the State satisfies *all three* of the following requirements: (i) there must be a valid law justifying the encroachment on privacy; (ii) the law must be reasonable and “*guarantee against arbitrary State action*”, which,

among other things, emphasizes the importance of judicial review before the invasion of privacy occurs; and (iii) the means adopted by Parliament must be proportional to the object and needs of the law. (*Puttaswamy I* at paras 310, 325). As explained below, however, Rule 4(2) fails to satisfy *any* — much less all three — of the *Puttaswamy I* requirements.

1. Rule 4(2) Fails the Valid Law Requirement

21. There is no valid law authorizing Respondent to violate citizens' fundamental privacy rights by imposing a duty to enable the identification of first originators in India on end-to-end encrypted services. It is well settled that any restrictions on fundamental rights must be by way of a statute enacted by Parliament. (See, e.g, *Ramlila Maidan Incident In re*, (2012) 5 SCC 1 at para 30). As discussed above, neither the IT Act (nor any other statute) imposes such a duty on intermediaries. Moreover, Rule 4(2) is not a valid law because it exceeds the scope of the IT Act and Respondent's rule-making powers. (See *Indian Young Lawyers Ass'n v. State of Kerala*, (2019) 11 SCC 1 at paras 137-140; *Global Energy Ltd. v. CERC*, (2009) 15 SCC 570 at para 25; *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). Thus, Rule 4(2) fails to satisfy the first *Puttaswamy I* requirement.

2. Rule 4(2) Fails to Guarantee Against Arbitrary State Action

22. Rule 4(2) is neither reasonable nor guarantees against arbitrary State action. Indeed, it grants the Government the power to link every communication to the user who made that communication without *prior judicial review* to guarantee against arbitrary State action. In *Puttaswamy I*, the Hon'ble Supreme Court emphasized the importance of such judicial review to guarantee against arbitrary State action:

“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.)

23. Further, in *K.S. Puttaswamy v. UOI*, (2019) 1 SCC 1 (*“Puttaswamy II”*), the Hon'ble Supreme Court again highlighted the importance of judicial scrutiny occurring *before* any invasion of privacy occurs. In that case, the petitioner challenged the constitutionality of Section 33(2) of the Aadhaar Act, which allowed the Government to direct disclosure of personal information in the interest of national security so long as the directions (i) were issued by a Joint Secretary in the Central Government, and (ii) received prior

approval of an Oversight Committee consisting of the Cabinet Secretary, Secretary to the Government of India in the Department of Legal Affairs, and the Secretary to the Department of Electronics and Information Technology. Despite all of the Act's oversight provisions, the Hon'ble Supreme Court held Section 33(2) *unconstitutional* for failure to provide safeguards sufficient to protect the fundamental right to privacy. In reaching its decision, the Hon'ble Supreme Court explained the importance of the Government obtaining *prior judicial approval* to guard against 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).

24. Requiring prior judicial review for electronic searches is consistent with the legal standard for physical searches under Section 93 of the Code of Criminal Procedure, 1973, which requires judicial approval *prior* to the Government's execution of a search warrant. Indeed, even before the Hon'ble Supreme Court recognized that privacy was a fundamental right, an eight-member bench concluded that the *“issue of a search warrant is normally the judicial function of the Magistrate. When such judicial function is interposed between the individual and the officer's*

authority for search, no circumvention thereby of the fundamental right is to be assumed.” (MP Sharma v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300, at para 17, emphasis added). The need for judicial scrutiny to protect the fundamental right to privacy is no different for searches of electronic information, especially given Indian citizens’ ever-increasing reliance on electronic platforms to communicate and store their most private and sensitive information.

25. Accordingly, because Rule 4(2) enables the Government to order certain SSIMs to enable the identification and disclosure of the first originators of communications in India on their end-to-end encrypted messaging services without *any* judicial oversight — much less *prior* judicial oversight — it is unreasonable and fails to guarantee against arbitrary State action. Rule 4(2) therefore fails the second *Puttaswamy I* requirement.

3. Rule 4(2) Is Not Proportional

26. According to the Hon’ble Supreme Court, an infringement of a fundamental right is not proportional unless it occurs “*through the least restrictive alternatives.*” (*Kerala State Beverages (M&M) Corp. Ltd. v. P.P. Suresh*, (2019) 9 SCC 710 at para 30). Rule 4(2) fails the proportionality requirement for the following reasons.
27. *First*, to identify the first originator of information on its end-to-end encrypted Secret Conversations feature in India,

Petitioner would have to create a mechanism that permits such identification for *any* such communication in response to a Government direction. This mechanism would permit the identification of such communications sent by *any* user in India, including the vast majority who use this messaging feature lawfully. This would contravene the Hon'ble Supreme Court's precedent that Government surveillance must be limited to only 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 at paras 32, 33; see also *Malak Singh v. State of P&H*, (1981) 1 SCC 420 at para 6; *Puttaswamy II* at para 183).

28. An unconstitutional invasion of privacy can occur even where the activity sought to be surveilled occurs in "public" places. For example, in a recent case, the Hon'ble Supreme Court rejected the Government's attempts to install CCTV cameras at the entrances of bars and other public places of entertainment, despite the Government's interest in controlling crime and protecting women from exploitation. The Hon'ble Supreme Court found that even surveillance of public behavior in public places constitutes an unlawful invasion of privacy, in violation of *Puttaswamy I*. (*Indian Hotels & Restaurant Ass'n (AHAR) v. State of Maharashtra*, (2019) 3 SCC 429 at para 104). Here, requiring Petitioner to enable the identification of the first originator on its messaging service constitutes a substantially greater invasion of privacy than the surveillance at issue in *Indian*

Hotels. A mechanism that permits the identification of the end-to-end encrypted communications of all users — the vast majority of whom are law-abiding Indian citizens — does not satisfy the “least restrictive” means requirement.

29. **Second**, by requiring Petitioner to enable the identification of the first originator of information in India on its end-to-end encrypted messaging feature, Rule 4(2) will diminish user privacy and chill lawful speech because users will be concerned that their private communications could be demanded by and disclosed to the Government at any time. Imposing such a requirement could, for example, risk (a) exposing activists to retaliation for espousing certain views or speaking out in favor of or against certain politicians or policies, (b) subjecting journalists to retaliation for investigating socially or politically divisive issues, and (c) publicly exposing sensitive personal information like Aadhaar, financial, sexual orientation, religious, or health information. It is respectfully submitted that the Government cannot invade law abiding citizens’ fundamental rights merely in the hope of investigating more potential criminals. Indeed, as the Hon’ble Supreme Court explained, “*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 at paras 83, 84).
30. **Third**, imposing such a requirement on intermediaries must be the “*least restrictive*” measure available to the

Government to achieve its goals. Rule 4(2), however, fails to do so, as it infringes the privacy of even those users who are using end-to-end encrypted messaging services and features lawfully. Indeed, as there is no way to predict which communications the Government will later seek to identify, intermediaries would have to build the ability to identify the first originator of *every* such communication sent on their services in India.

31. Accordingly, Rule 4(2)'s requirement that messaging services must enable the identification of first originators of information in India is disproportionate, as it does not achieve Government's goals "*through the least restrictive alternatives.*" Rule 4(2) therefore fails the third *Puttaswamy I* requirement.
32. In sum, Respondent must satisfy *all three* of the *Puttaswamy I* requirements before it can justify violating Indian users' fundamental right to privacy. Rule 4(2), however, fails to satisfy *any* of the requirements and therefore should be struck down.

B. Rule 4(2) Violates the Right to Freedom of Speech and Expression

33. As the Hon'ble Supreme Court has repeatedly recognized, freedom of speech and expression is a fundamental right guaranteed under Article 19(1)(a) of the Constitution. Indeed, the Constitution's framers "*recognised the importance of safeguarding [the right to freedom of speech*

*and expression] since the free flow of opinions and ideas is essential to sustain the collective life of the citizenry.” (S. Khushboo v. Kanniamal & Anr., (2010) 5 SCC 600 at paras 45, 47; see also Shreya Singhal v. Union of India, (2015) 5 SCC 1 (“**Shreya Singhal**”), at paras 10, 90). This right includes “freedom not only for the thought that we cherish, but also for the thought that we hate.” (Naraindas Indurkha v. State of M.P., (1974) 4 SCC 788 at para 23).*

34. The Hon’ble Supreme Court has further observed that the fundamental right to freedom of speech and expression includes “*the right to propagate one’s views through the print media or through any other communication channel*”, and that “*any attempt to deny the same must be frowned upon unless it falls within the mischief of Article 19(2) of the Constitution.*” (*LIC v. Manubhai D. Shah*, (1992) 3 SCC 637 at para 8).
35. The ability to exercise one’s freedom of speech and expression, however, is dependent in large part on the ability to maintain one’s privacy. This is because privacy protects people from retaliation for expressing unpopular but lawful opinions, challenging mainstream views, and even reporting unlawful activities. Identifying the first originator of end-to-end encrypted information in India, however, undermines privacy and impedes freedom of expression. Indeed, as observed by Professor David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,

online privacy is crucial to safeguarding freedom of speech because it allows people to “*to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.*” See page 4 of the letter submitted by Professor Kaye, a copy of which is annexed herewith as **Annexure P-7** to this petition.

36. Moreover, while *reasonable* limitations on the fundamental right to freedom of speech and expression may be permissible, Rule 4(2) *unreasonably* intrudes upon this right for several reasons.
37. *First*, the Hon’ble Supreme Court has repeatedly found that a law violates the fundamental right to freedom of speech and expression if it chills lawful speech. (E.g., *Shreya Singhal* at paras 10, 90; *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632 at para 22; *S. Khushboo* at para 47). As discussed above, because Rule 4(2) infringes users’ ability to speak privately, it necessarily *chills even lawful speech*. Every communication by every user in India using the Secret Conversations feature will forever be linked to their identities, depriving them of their privacy, and depriving them of their desire and ability to speak and express themselves freely. Indeed, once users become aware that the Government can identify the first originator of every communication, these users — including the vast majority who are law abiding Indian citizens — will be discouraged from speaking freely for fear that their lawful private conversations will be traced, exposed, disclosed to others,

or, worse, subject them to retaliation, which is antithetical to free speech and end-to-end encryption.

38. ***Second***, Rule 4(2) unreasonably restricts the right to free speech and expression for many of the same reasons that it violates the right to privacy (discussed above). In short: (i) no valid law authorizes Rule 4(2) because it is *ultra vires* the IT Act; (ii) Rule 4(2) fails to provide constitutionally adequate safeguards to guarantee against arbitrary Government action because it permits the Government to order intermediaries to identify first originators of communications in India without any, let alone prior, judicial review; and (iii) Rule 4(2) is disproportionate because it is not the “*least restrictive*” means available, especially given its unlimited scope and massive infringement of fundamental rights.
39. Accordingly, because Rule 4(2) violates the fundamental right to freedom of speech and expression, it should be struck down.

C. Rule 4(2)’s Requirement to “*Enable the Identification of the First Originator of the Information*” in India is *Ultra Vires* the IT Act

40. Subordinate legislation is *ultra vires* the parent statute if it travels beyond, and does not conform with, the parent statute. (E.g., *Kunj Behari Lal Butail v. State of H.P.*, (2000) 3 SCC 40 at para 14; *ADM (Rev.) Delhi Admn v. Sri Ram* (2000) 5 SCC 451 at para 16). “*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.” (State of Karnataka v. Ganesh Kamath (1983) 2 SCC 402 at para 7).

41. Here, the scope of Respondent’s authority to prescribe the Intermediary Rules is defined by Sections 69A and 79(2) of the IT Act. However, as discussed below, neither section empowers Respondent to create a rule requiring the ability to identify the first originators of information in India on messaging services that protect communications with end-to-end encryption.
42. Section 69A empowers the Central Government to (i) order an “*intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource*”, and (ii) prescribe “*procedures and safeguards subject to which such blocking for access by the public may be carried out*”. Requiring SSIMs to identify the first originator of end-to-end encrypted information in India, however, is neither a blocking order nor a procedure or safeguard subject to which a blocking order may be carried out. Therefore, Rule 4(2) exceeds the scope of Respondent’s rule-making authority under Section 69A.

43. Section 79(2) requires an intermediary to observe “*due diligence while discharging his duties under this Act and also observe(s) such other guidelines as the Central Government may prescribe in this behalf*”. However, this provision does not authorize Respondent to require intermediaries to build mechanisms to identify the first originator of information in India on their end-to-end encrypted messaging services and features for the following principal reasons.
44. **First**, the law is clear that the Central Government **cannot** undertake essential legislative functions, as such functions, “*which consists in declaring [...] policy and making it a binding rule of conduct*”, are reserved exclusively for Parliament. (See *In re Delhi Laws Act, 1912, Ajmer-Merwara (Extension of Laws) Act, 1947*, 1951 SCR 747 at para 311). Only after “*a policy is laid down and a standard established by statute*” — which are “*declared with sufficient clearness*” — can subordinate legislation (like Rule 4(2)) be promulgated consistent with such policy and standard. (See *Id.* at paras 308, 326, emphasis added).
45. Accordingly, Respondent cannot require intermediaries to enable the identification of the first originator of every communication in India on their end-to-end encrypted services and features absent vesting of a specific power in the IT Act itself. Section 79(2), however, neither contains a specific provision to that effect nor evinces Parliamentary intent to require intermediaries to enable identification of

the first originator of every such communication in India. Respondent therefore cannot impose such a requirement via Rule 4(2). (See, e.g., *Kunj Behari Lal Butail* at para 14 [“*[A] delegated power to legislate by making rules ‘for carrying out the purposes of the Act’ is a general delegation without laying down any guidelines; it cannot be so exercised as to bring into existence substantive rights or obligations or disabilities not contemplated by the provisions of the Act itself.*”).

46. **Second**, Rule 4(2)’s requirement far exceeds intermediaries’ due diligence obligations under the IT Act. Rule 4(2) would require that SSIMs create mechanisms to be able to identify the end-to-end encrypted communications of all of their users when requested by the Government. Indeed, by requiring SSIMs to create the ability to identify originators on end-to-end encrypted services and features, Rule 4(2) imposes significant *new* obligations on intermediaries that are absent in, and far exceed their obligations under, the IT Act. Moreover, enabling the identification of the first originator of such communications in India, in an effort to comply with Rule 4(2), would require Petitioner to make fundamental product changes to its messaging service. Forcing an intermediary to make such changes goes well beyond the “due diligence” measures as contemplated by Section 79(2).
47. **Finally**, 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*”. However, ***no other nation on earth*** has imposed a requirement like Rule 4(2). Thus, by imposing this requirement — which creates a substantial *disharmony* with the laws of the rest of the world — Respondent has violated Parliament’s express intent in enacting the IT Act.

48. Accordingly, because Rule 4(2) is *ultra vires* the express language and intent of the IT Act, it should be invalidated.

D. Rule 4(2) Violates the Principle of Data Minimisation.

49. “*Data minimisation*” is the principle that, where feasible, an online service should only collect and store user data that is necessary to provide its services. The aim of this principle is to reduce the risks of unauthorized access to such data. The Hon’ble Supreme Court, in Sikri, J.’s majority judgment in *Puttaswamy II*, explained that only by “*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 further observed that the statute at issue in that case was unconstitutional for violating, among other things, the principle of data minimisation. (*Id.* at para 510.4).

50. Here, to the extent that identifying the first originator of end-to-end encrypted information in India requires an intermediary to store additional data that is not necessary to provide its service, it contravenes the principle of data minimization.
51. Finally, Petitioner respectfully submits that criminal liability may not be imposed for non-compliance with Rule 4(2), and that doing so would be unconstitutional and *ultra vires* the IT Act.
52. Petitioner has not filed any other petition regarding the subject matter of the present Petition in either this Hon'ble Court or in any other High Court or before the Hon'ble Supreme Court of India. Petitioner reserves the right, and may humbly request leave of this Hon'ble Court, to add or amend any of the aforementioned grounds at a later stage, or to challenge any of the other Intermediary Rules, if and as appropriate.
53. Petitioner has no alternative remedy, much less an equally efficacious remedy, with respect to the subject matter of the present Petition. Further, adjudication by this Hon'ble Court in exercise of its extraordinary powers under Article 226 of the Constitution of India is necessary and warranted because Rule 4(2), among other things, (i) violates the fundamental rights to privacy and freedom of speech and expression, thereby raising substantial questions of law and public

importance; (ii) violates Article 14 of the Constitution; and (iii) is *ultra vires* the IT Act, the parent statute under which Rule 4(2) was prescribed. The fundamental rights of Petitioner's users in India are at stake, and Rule 4(2) is likely to have a far reaching consequence in India.

54. The annexures filed along with the present petition are the true copies of their respective originals.

PRAYER

55. In light of the above grounds, challenges, and submissions made in this Petition, Petitioner most respectfully beseeches this Hon'ble Court and seeks as under:

- a. Issue a writ of mandamus or any other appropriate writ, direction, or order to declare that (i) Impugned Rule 4(2) of the Intermediary Rules, with respect to end-to-end encrypted messaging services and features, is illegal and violative of Articles 14, 19(1)(a), 19(1)(g), and 21 of the Constitution and *ultra vires* the IT Act, and (ii) criminal liability may not be imposed for non-compliance with Impugned Rule 4(2), as doing so would be unconstitutional, *ultra vires* the IT Act, and illegal; and
- b. Issue an appropriate writ, order, or direction or such other appropriate remedy to do complete justice in the facts and circumstances of the present case.

- 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

INDIA


M/S. SHARDUL AMARCHAND MANGALDAS & CO.,

ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216,

OKHLA INDUSTRIAL ESTATE, PHASE-III,

NEW DELHI -110020

EMAIL:



MOB



PLACE: NEW DELHI

DATE: 25 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

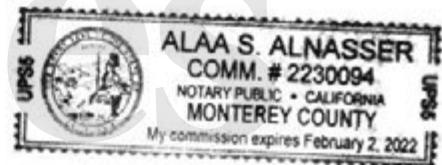
County of Alameda

Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (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:**

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

AFFIDAVIT ON BEHALF OF PETITIONER

I, Sandeep Solanki, aged about 43 years, son of Mr. Natvar M. Solanki, Power of Attorney holder of Petitioner, Facebook, Inc. ("Facebook"), residing at [REDACTED] do hereby solemnly affirm and state as under:

1. I am the Power of Attorney Holder of Facebook and am duly authorized and competent to swear this affidavit on behalf of Facebook. 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.

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 [REDACTED]
[REDACTED], ON THIS 21TH 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 at [REDACTED]
on this 21th 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

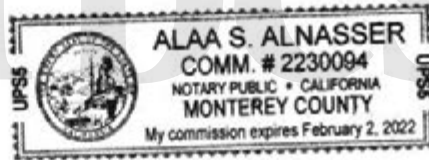
County of Alameda

Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solauki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (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

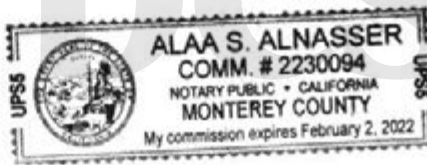
County of Alameda

Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (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 mentions 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:

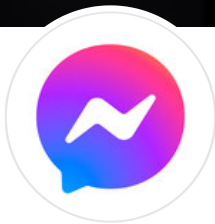
Classification decisions shall take account of the degree and nature of violence in a work.



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

Dr. RAJENDRA KUMAR, Addl. Secy.

//TRUE COPY//



Messenger

@messenger · Product/Service

Send Message

Home

About

Photos

Videos

More

Like



GENERAL

11,356,191 people like this

12,817,168 people follow this

Product/service · App Page

ADDITIONAL CONTACT INFO

<https://www.messenger.com/>

disclaimer@fb.com

Send message

MORE INFO

About

Messenger from Facebook helps you stay close with those who matter most, from anywhere and on any device.

//TRUE COPY//



Messages

Sending Messages, Photos and Videos

Messenger Contacts

Secret Conversations

Group Conversations

Voice and Video Calling

Messenger Kids

Secret Conversations

What can I send in a secret conversation in Messenger?

With secret conversations, you can send:

- Messages
- Pictures
- Stickers
- Videos
- Voice recordings

Secret conversations don't support:

- Group messages
- Gifs
- Voice or video calling
- Payments

A secret conversation in Messenger is encrypted end-to-end, which means the messages are intended just for you and the other person—not anyone else, including us. Keep in mind that the person you're messaging could choose to share the conversation with others (ex: a screenshot). Learn [how to start a secret conversation](#).

Was this information helpful?

Yes No

[View full article](#)
[Share article](#)

How do I verify that my secret conversation in Messenger is encrypted?

All secret conversations in Messenger are encrypted. Your messages will be encrypted whether or not you compare device keys.

Both you and the other person in the secret conversation have device keys that you can use to verify that the messages are end-to-end encrypted. You can see your device keys on any device where you're using secret conversations. Each of your devices will have its own device keys.

View conversation device key

To view a conversation's device keys:

- 1 Open a secret conversation with someone.
- 2 Click their name at the top.
- 3 Click **Your Keys**.

Verify the conversation

To verify the conversation is encrypted, compare the device key that appears under your friend's name with the their keys on their device to make sure they match. You can compare devices in person, or via screenshot.

Example: On your device, your friend Anna's device keys are 123. On Anna's device, her keys should also be 123.

Was this information helpful?

Yes No

[View full article](#)

[Share article](#)

Can I use multiple devices for secret conversations in Messenger?

A [secret conversation in Messenger](#) is encrypted end-to-end, which means the messages are meant only for you and the other person and not anyone else, including us.

You can use more than one mobile device for secret conversations. To add a new device, just [install the Messenger app](#) and sign into Messenger on that device.

When you sign into a new mobile device:

- You won't see the messages from previous secret conversations on the new device.
- You'll receive a notice in past secret conversations letting you and the other participants know you're on a new device.
- Once the device is added, you'll see new messages in secret conversations on all active devices.

Learn how to [start a secret conversation](#). You can also [set messages to disappear](#) in a secret conversation.


Was this information helpful?

Yes No

[View full article](#)

[Share article](#)

Why am I seeing more than one Messenger conversation with the same person?

If you start a secret conversation with someone you already have a regular Messenger conversation with, you'll see two different conversations in your mobile app. Secret conversations have a padlock icon  by the person's profile picture.

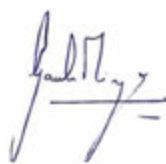
Learn how to [start a secret conversation on the Messenger app](#) for mobile.

Was this information helpful?

Yes No

[View full article](#)

[Share article](#)



//TRUE COPY//

Information for Law Enforcement Authorities



These operational guidelines are for law enforcement officials seeking records from Facebook and Instagram. For private party requests, including requests from civil litigants and criminal defendants, please visit the [Help Center](#). Users seeking information on their own accounts can access Facebook's "Download Your Information" feature from their [account settings](#). This information may change at any time.

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: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.
- 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 message headers and IP addresses, 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 messages, photos, videos, timeline posts, and location information.
- We interpret the national security letter provision as applied to Facebook to require the production of only 2 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. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure

of the contents of an account. Further information can be found [here](#).

Authenticity Policy

People on Facebook are required to use the name they go by in everyday life on their account's main profile, and must not maintain multiple accounts. Operating fake accounts, pretending to be someone else, or otherwise misrepresenting your authentic identity is not allowed, and we will act on violating accounts. Please see our Account Integrity and Authentic Identity policies [here](#).

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 through the [Law Enforcement Online Request System](#), or mail 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 through the [Law Enforcement Online Request System](#). Note: We will not review or respond to requests submitted by non-law enforcement officials. Users aware of an emergency situation should immediately and directly contact local law enforcement officials.

Child Safety Matters

We report all apparent instances of child exploitation appearing on our site 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 Center 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 (and include relevant NCMEC report identifiers) in the request to ensure that we are able to address these matters expeditiously and effectively.

Data Retention and Availability

We will search for and disclose data 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.

Details about data and account deletion can be found in our [Data Policy](#), [Statement of Rights and Responsibilities](#), and [Help Center](#).

Form of Requests

We will be unable to process overly broad or vague requests. All requests must identify requested records with particularity, including the specific data categories requested and date limitations for the request, as well as include:

- The name of the issuing authority and agent, email address from a law-enforcement domain, and direct contact phone number.
- The email address, phone number (+XXXXXXXXXX), user ID number (<http://www.facebook.com/profile.php?id=1000000XXXXXXXX>) or username (<http://www.facebook.com/username>) of the Facebook profile.

User Consent

If a law enforcement official is seeking information about a Facebook 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. For account content, such as messages, photos, videos and timeline posts, users can access Facebook's ["Download Your Information" feature from their account settings](#). Users can also view recent IP addresses in their account settings under "Security Settings" > "Where You're Logged In". Users do not have access to historical IP information without legal process.

Notification

Our policy is 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. We will also provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing

violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Testimony

Facebook nor Instagram provides expert testimony support. In addition, Facebook and Instagram 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, Facebook, Instagram and our users, and emergency requests.

Human Rights Due Diligence

In line with our commitments as a member of the Global Network Initiative and our [Corporate Human Rights Policy](#), we also conduct a careful review of each law enforcement request to disclose user data for consistency with international human rights standards.

Victim and Survivor Support

We know law enforcement often works with victims or other members of the community that need support navigating social media and understanding how to stay safe online. [Here](#) is a list of resources that can help you offer support to them.

Submission of Requests

Online

Law enforcement officials may use the [Law Enforcement Online Request System](#) for the submission, tracking and processing of requests.

Please note:

1. Law enforcement officials seeking account records from Facebook or Instagram must

address their request to Facebook Inc.

2. A government-issued email address is required to access the Law Enforcement Online Request System.

Mail

United States mailing address:

1601 Willow Road, Menlo Park CA 94025

Attention: Facebook Security, Law Enforcement Response Team

Law enforcement officials who do not submit requests through the [Law Enforcement Online Request System](#) should expect longer response times.

Notes

- 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.

INDIA
Forbes



Our family of companies:



[About](#)

[Create Ad](#)

[Create Page](#)

[Developers](#)

[Careers](#)

[Privacy](#)

[Cookies](#)

[Ad Choices](#)

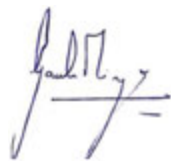
[Terms](#)

[Help](#)

Facebook © 2021

[English \(US\)](#) 

INDIA
Forbes



//TRUE COPY//

Law Enforcement Online Requests



Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

[Request Access](#)

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Law Enforcement Guidelines](#).

English (UK) हिन्दी বাংলা العربية المल्याळം ಕನ್ನಡ ગુજરાતી తెలుగు मराठी বাংলা தமிழ் +

Sign Up Log In Messenger Facebook Lite Watch People Pages Page categories Places Games Locations Marketplace Facebook Pay Groups
Jobs Oculus Portal Instagram Local Fundraisers Services Voting Information Centre About Create ad Create Page Developers Careers Privacy
Cookies AdChoices Terms Help

Facebook © 2021

//TRUE COPY//

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 explicit or implicit 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 hosing, 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//

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).¹ 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.

¹ 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


INDIA
//TRUE COPY//
Forbes

IN THE HON'BLE HIGH COURT OF DELHI
(EXTRAORDINARY WRIT JURISDICTION)

C.M. NO. OF 2021

IN

WRIT PETITION (CIVIL) NO. ____ OF 2021

IN THE MATTER OF:

FACEBOOK, INC.

...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
THE PETITIONER ABOVE NAMED

MOST RESPECTFULLY SHOWETH:

1. That by way of the accompanying Writ Petition under Article 226 of the Constitution of India, Petitioner is seeking

issuance of a Writ of Mandamus or any other appropriate writ, direction, or order to declare that (i) Impugned Rule 4(2) of the Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**Intermediary Rules**”) is, with respect to end-to-end encrypted messaging services and features, illegal and violative of Articles 14, 19(1)(a), 19(1)(g) and 21 of the Constitution and *ultra vires* the Information Technology Act, 2000 (“**IT Act**”), and (ii) criminal liability may not be imposed for non-compliance with Impugned Rule 4(2), as doing so would be unconstitutional, illegal, and *ultra vires* the IT Act.

2. Petitioner offers the Facebook social media platform to users throughout the world, including many users in India. Facebook is a free and voluntary online social networking service that allows its users to connect and share information online. While Petitioner primarily offers a social media platform, it also provides the “Messenger” messaging service, which helps people stay close with those who matter most, from anywhere and on any device. Messenger offers a feature called Facebook Secret Conversations. As stated on Facebook’s website: “*With secret conversations, you can send: Messages, Pictures, Stickers, Videos, Voice recordings. . . . A secret conversation in Messenger is encrypted end-to-end, which means the messages are intended just for you and the other person—not anyone else, including [Petitioner].*”
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 shall be read as part and parcel of the present application.

4. The Intermediary Rules were notified by Respondent on 25 February 2021 in supersession of the Information Technology (Intermediaries Guidelines) Rules, 2011. Impugned Rule 4(2) is expected to become effective on 26 May 2021, at which time government agencies may make demands that Petitioner provide the identity of the first originator of information in India with respect to communications on Petitioner's end-to-end encrypted Secret Conversations messaging feature.
5. In light of the Constitutional and other challenges raised in the accompanying Petition and the serious issues of law and public importance arising therefrom, Petitioner has a strong *prima facie* case, and the balance of convenience is also in favour of Petitioner and against Respondent.
6. Specifically, the Petition demonstrates that Impugned Rule 4(2) violates the constitutional rights of Petitioner, as well as the fundamental rights to privacy and free speech of Indian citizens who use the Secret Conversations messaging feature. Indeed, compliance with Impugned Rule 4(2) would force Petitioner to break end-to-end encryption with regard to communications on its Secret Conversations messaging feature, and alter the fundamental nature of this feature. Thus, Impugned Rule 4(2) will cause irreparable

harm to the Constitutional rights of Petitioner and its users who send such communications.

7. Further, Impugned Rule 4(2) is *ultra vires* the IT Act and far exceeds the rulemaking authority granted to Respondent under the IT Act. Impugned Rule 4(2) has been framed under sections 69A and 79 of the IT Act. Respondent's rule-making authority under such provisions is limited to "*carry[ing] out the provisions of IT Act*" and laying down "*guidelines to be observed by intermediaries*". The power to create new and more onerous obligations, beyond the provisions of sections 69A and 79, has not been conferred upon Respondent by the Legislature.
8. In addition, if an interim stay of Impugned Rule 4(2) is not granted, Petitioner would be subject to grave and irreparable harm and prejudice, as it would (i) expose Petitioner to loss of immunity for hosting content under Section 79 of the IT Act; (ii) expose Petitioner and its employees to potential criminal liability in case of any perceived non-compliance with Impugned Rule 4(2), which has no foundational basis in the IT Act, the parent statute; and (ii) impose additional obligations on Petitioner to build new mechanisms and processes which would require a significant investment of time and money, and which would change the fundamental nature of the Secret Conversations messaging feature that Petitioner offers to its users in India.
9. Accordingly, Petitioner most respectfully submits that the operation of Impugned Rule 4(2) ought to be stayed *qua*

Petitioner with respect to its end-to-end encrypted messaging feature, as it is not only without the authority of law but also imposes onerous and unconstitutional obligations on Petitioner and infringes the fundamental rights of the many users of such messaging feature throughout the country.

10. This application is made bonafide and in the interest of justice.

PRAYER

It is, therefore, most respectfully prayed that this Hon'ble Court may be pleased to:

- a. Issue an ex-parte ad interim order staying the operation of Impugned Rule 4(2) of the Intermediary Rules *qua* Petitioner with respect to its end-to-end encrypted messaging feature, during the pendency of the accompanying Petition, as the rule is unconstitutional, *ultra vires* the IT Act, and illegal;
- b. During the pendency of the accompanying Petition, prohibit the imposition of any criminal liability, and restrain Respondent and any other Government or law enforcement agency from taking any coercive action, against Petitioner and its employees for any perceived non-compliance with Impugned Rule 4(2), as doing so would be unconstitutional, *ultra vires* the IT Act, and illegal; 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

INDIA


M/S. SHARDUL AMARCHAND MANGALDAS & CO.,

ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216,

OKHLA INDUSTRIAL ESTATE, PHASE-III,

NEW DELHI -110020

EMAI



MOB



PLACE: NEW DELHI

DATE: 25 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 Alameda

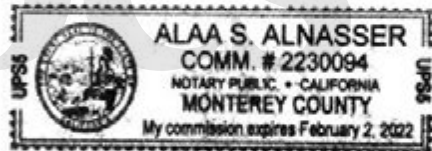
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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

C.M No. _____ of 2021

IN

WRIT PETITION (CIVIL) NO. _____ OF 2021

IN THE MATTER OF:

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

AFFIDAVIT ON BEHALF OF PETITIONER

I, Sandeep Solanki, aged about 43 years, son of Mr. Natvar M. Solanki, Power of Attorney holder of Petitioner, Facebook, Inc. ("Facebook"), residing at [REDACTED]

do hereby solemnly affirm and state as under:

1. I am the Power of Attorney Holder of Facebook and am duly authorized and competent to swear this affidavit on behalf of Facebook. 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.

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 [REDACTED] U.S.A. ON THIS 21TH 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 at [REDACTED] on this 21th 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 Alameda

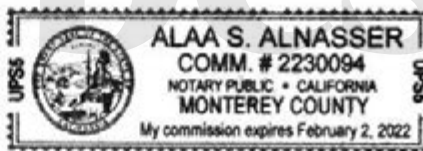
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature 

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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 Alameda

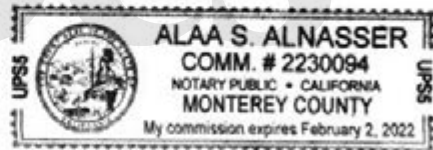
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Sobnki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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)**

C.M. NO. OF 2021

IN

WRIT PETITION (CIVIL) NO. ____ OF 2021

IN THE MATTER OF:

FACEBOOK, INC.

...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.

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 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 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

INDIA
Shardul
Forbes

M/S. SHARDUL AMARCHAND MANGALDAS & CO.,

ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216,

OKHLA INDUSTRIAL ESTATE, PHASE-III,

NEW DELHI -110020

EMAIL

[REDACTED]

[REDACTED]

MOB:

[REDACTED]

PLACE: NEW DELHI

DATE: 25 MAY 2021

[REDACTED]

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

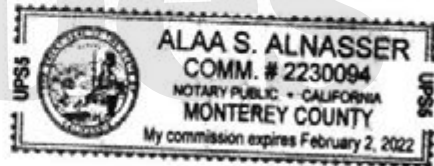
County of Alameda

Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (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

C.M No. _____ of 2021

IN

WRIT PETITION (CIVIL) NO. _____ OF 2021

IN THE MATTER OF:

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

AFFIDAVIT ON BEHALF OF PETITIONER

I, Sandeep Solanki, aged about 43 years, son of Mr. Natvar M. Solanki, Power of Attorney holder of Petitioner, Facebook, Inc. ("Facebook"), residing at _____

do hereby solemnly affirm and state as under:

1. I am the Power of Attorney Holder of Facebook and am duly authorized and competent to swear this affidavit on behalf of Facebook. 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.

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 [REDACTED]

[REDACTED] ON THIS 21TH 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 at [REDACTED]
on this 21th 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 Alameda

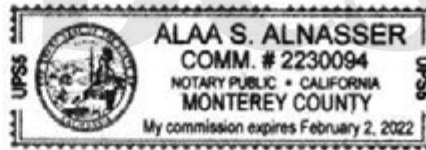
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature 

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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 Alameda

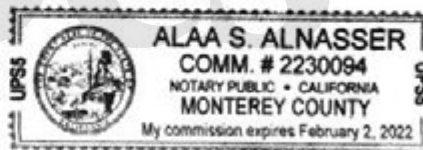
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Sobnki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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)**

C.M. NO. OF 2021

IN

WRIT PETITION (CIVIL) NO. ____ OF 2021

IN THE MATTER OF:

FACEBOOK, INC.

...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.
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 pleadings & affidavits 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, applications and affidavits.
5. Petitioner undertakes to duly furnish apostilled versions of its petition, applications and 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 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, applications and 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

INDIA


M/S. SHARDUL AMARCHAND MANGALDAS & CO.,

ADVOCATES FOR THE PETITIONER

AMARCHAND TOWERS, 216,

OKHLA INDUSTRIAL ESTATE, PHASE-III,

NEW DELHI -110020

EMAIL

[REDACTED]

[REDACTED]

MOB

[REDACTED]

PLACE: NEW DELHI
DATE: 25 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 Alameda

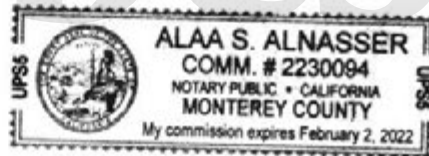
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021.
by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature 

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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

C.M No. _____ of 2021

IN

WRIT PETITION (CIVIL) NO. _____ OF 2021


IN THE MATTER OF:

FACEBOOK, INC.

...PETITIONER

UNION OF INDIA VERSUS INDIA
 ... RESPONDENT

AFFIDAVIT ON BEHALF OF PETITIONER

I, Sandeep Solanki, aged about 43 years, son of Mr. Natvar M. Solanki, Power of Attorney holder of Petitioner, Facebook, Inc. ("Facebook"), residing at 

do hereby solemnly affirm and state as under:

1. I am the Power of Attorney Holder of Facebook and am duly authorized and competent to swear this affidavit on behalf of Facebook. 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.

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 [REDACTED]

[REDACTED] ON THIS 21TH 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 at [REDACTED]

on this 21th 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 Alameda

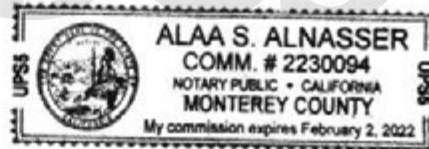
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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 Alameda

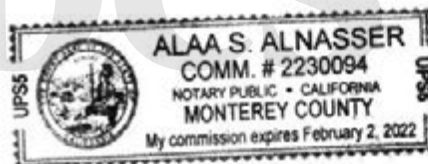
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature 

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



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:

FACEBOOK, INC.

...PETITIONER

VERSUS

UNION OF INDIA

... RESPONDENT

VAKALATNAMA

KNOW ALL to whom this shall come that I, Sandeep Solanki, Power of Attorney holder of the Petitioner, Facebook Inc., a company registered under the laws of the State of Delaware, U.S.A. and having its registered office at 1 Hacker Way, Menlo Park, California 94025 (U.S.A.), appoint Mr. Ajit Warriar

 and Mr. Gauhar Mirza 

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.

INDIA
Forbes

Signature: 
Name: AJIT WARRIER

Advocate

Enrolment No.: 

Signature identified by
Signature: 

Name: GAUHAR MIRZA

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 Alameda

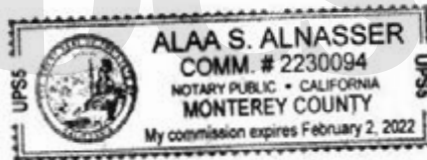
Subscribed and sworn to (or affirmed) before me this 21st day of May, 2021, by Sandeep Solanki, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature [Handwritten Signature]

Alaa S. Alnasser (Notary)

(Seal)

INDIA
Forbes



Description of Attached Document	
_____	Title or Type of Document
_____	Number of Pages
_____	Date of Document

POWER OF ATTORNEY

KNOW ALL MEN BY THESE PRESENTS THAT Facebook, Inc. having its office at 1601 Willow Road, Menlo Park, California 94025, United States of America, (“**Company**”) **HEREBY APPOINTS** Sandeep Solanki, 41, son of Natvar M. Solanki, having office at 1601 Willow Road, Menlo Park, California 94025, United States of America, as its Attorney (“**Attorney**”) to do or execute any or all acts, matters, deeds or things, for and on behalf of the Company, in connection with, and/or in relation to, the following matters, namely:

1. To commence, institute, verify, file, carry on, continue, prosecute, answer and/or discontinue proceedings before the District Courts, High Courts and the Supreme Court of India of India and to sign, verify and execute any or all Petitions, Vakalatnamas (Authority Letter), Affidavits, Appeals, Applications or documents of whatever description that may be necessary for the purpose of filing or defending any proceedings; and to appoint any or all Advocates, Pleaders, or Counsel; and to file any or all Appeals, Revisions, Reviews, or Special Leave Petitions before the Supreme Court of India, or in any other proceeding of any kind whatsoever arising therefrom and/or connected therewith, and suffer orders, judgments or decrees given or pronounced in said proceedings.

Facebook
Legal
Litigation
PSG

2. To state, settle, adjust, compound, submit to arbitration/mediation and/or compromise the abovementioned proceedings, accounts, claims or demands whatsoever in such manner in all respects as the Attorney shall think fit.
3. To sign, affirm and verify complaints, written statements, petitions, claims and objections; compromise decree and applications of all kinds; to file all such documents in any court, tribunal, regulatory body, office or with any person; and to return any necessary papers in court as regards to the above mentioned proceedings.
4. To perform all such acts or things, including appearing before any court, tribunal, or notary public, and accepting notices or services or writ or summons or other legal process that may be served upon the Company in connection with the above mentioned proceedings.
5. To apply for certified copies of judicial records of the above mentioned proceedings.

THE COMPANY HEREBY AGREES that all acts, deeds and things done by the Attorney whether jointly or severally, shall be construed as acts, deeds and things done by the Company. We hereby undertake to ratify and confirm all and whatever the Attorney shall do by virtue of the powers hereby given.

Facebook
Legal
Litigation

PSG

This Power of Attorney is granted until January 31, 2023 and may be revoked at any time by the Company by written notice of revocation of this Power of Attorney.

IN WITNESS WHEREOF, we have signed this Special Power of Attorney at 1601 Willow Road on this 24th day of May, 2018.

SIGNED and DELIVERED by:

For Facebook, Inc.

Signature: Paul S. Grewal



Name: Paul Grewal

Designation: VP and Deputy General Counsel



**State of California
Secretary of State**

This Certificate is not valid for use anywhere within the United States of America, its territories or possessions.

APOSTILLE (Convention de La Haye du 5 octobre 1961)			
1. Country: Pays / País:	United States of America		
This public document Le présent acte public / El presente documento público			
2. has been signed by a été signé par ha sido firmado por	Michelle Payomo Blacklock		
3. acting in the capacity of agissant en qualité de quien actúa en calidad de	Notary Public, State of California		
4. bears the seal / stamp of est revêtu du sceau / timbre de y está revestido del sello / timbre de	Michelle Payomo Blacklock , Notary Public, State of California		
Certified Attesté / Certificado			
5. at à / en	Sacramento, California	6. the le / el día	25th day of May 2018
7. by par / por	Secretary of State, State of California		
8. N° sous n° bajo el número	71053		
9. Seal / stamp: Sceau / timbre: Sello / timbre:		10. Signature: 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: www.sos.ca.gov/business/notary/apostille-search/.

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: www.sos.ca.gov/business/notary/apostille-search/.

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: www.sos.ca.gov/business/notary/apostille-search/.

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.



ACKNOWLEDGMENT

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

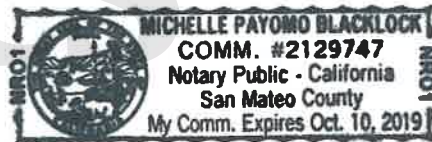
On May 24, 2018 before me, Michelle Payomo Blacklock ^{Notary Public}
(insert name and title of the officer)

personally appeared Paul Grewal
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 MB Blacklock (Seal)



PROOF OF SERVICE

Forbes ^{INDIA}