

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 714
TO BE ANSWERED ON: 24.07.2026

**LEGAL AND POLICY FRAMEWORK FOR USERNAME
FEATURES ON MESSAGING PLATFORMS**

714. SMT. JEBI MATHER HISHAM:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether Government has examined the legal implications of the proposed username feature announced by WhatsApp;
- (b) whether any legal provision under the existing Information Technology framework empowers the Government to seek modifications or safeguards before the rollout of such features;
- (c) whether Government has conducted any assessment of the likely impact of anonymous or pseudonymous usernames on cybercrime investigations and law enforcement;
- (d) whether any consultation has been held with intermediaries, cybersecurity experts and other stakeholders on this issue; and
- (e) the details of the policy measures proposed to ensure that technological innovations do not compromise user safety or the constitutional right to informational privacy?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (e): The policies of the Government are aimed at fostering technological innovation while ensuring an Open, Safe and Trusted and Accountable Internet for all users, including women and children, through an appropriate legal and regulatory framework.

The Government is committed to ensure that the Internet in India is free from any form of unlawful acts, content or information.

Emerging Platform Features

The Government keeps track of technological developments on digital platforms. This includes new features introduced by intermediaries, from the perspective of user safety, cyber security and compliance with the applicable legal framework.

Upon reports regarding the proposed username feature on WhatsApp, the Government immediately engaged with the concerned messaging platforms and conveyed its concerns regarding the potential safety and security implications associated with the proposed feature. They were asked to defer the rollout of the feature in view of the concerns relating to the associated user safety, security implications and the applicable legal and regulatory framework.

The objective was to ensure that the feature does not facilitate cyber crimes such as digital arrest fraud, impersonation and other online offences.

Legal & Regulatory Framework

The Information Technology Act, 2000 (“IT Act”) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules, 2021”) prescribe due diligence obligations for intermediaries, including social media intermediaries. These include obligations relating to preventing the use of digital platforms for unlawful activities, including the dissemination of information involving impersonation, deepfakes, misleading information, obscenity and other harmful content.

These also include obligations relating to grievance redressal, cooperation with law enforcement agencies, and taking expeditious action on unlawful content as per the provisions of law, including compliance with lawful directions issued under the applicable legal framework.

The existing legal framework contains appropriate provisions to address unlawful activities facilitated through digital platforms. The IT Act provides punishment for various cyber offences such as privacy violations (section 66E), publishing or transmitting obscene or sexually explicit content (sections 67, 67A, 67B), identity theft (section 66C), cheating by personation (section 66D). It also empowers Police to investigate offences (section 78), enter public place and search and arrest suspected person (section 80).

Where any feature or its misuse results in violation of the provisions of the IT Act or the Rules made thereunder, appropriate action may be taken in accordance with the provisions of the IT Act and other applicable laws, based on the facts and circumstances of each case.

Intermediaries are also required, under the IT Rules, 2021, not to knowingly deploy, install or modify the technical configuration of a computer resource in a manner that circumvents any law for the time being in force.

In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, they lose their exemption from third party information provided under section 79 of the IT Act. They are liable for consequential action or prosecution as provided under any extant law.

The Government continuously assesses emerging cyber risks, including risks arising from impersonation, phishing, online fraud and other cyber offences. Such assessments are undertaken through regular interactions with relevant stakeholders, including intermediaries, law enforcement agencies, cyber security agencies and domain experts, as considered necessary.

The Government follows a consultative approach in addressing emerging technology and cyber security issues. Consultations with intermediaries and other stakeholders are held from time to time, as and when required.

The existing legal framework seeks to balance technological innovation with user safety, cyber security, privacy and other rights guaranteed under the Constitution. The IT and the rules made thereunder constitute a dynamic legal framework and are reviewed from time to time. Amendments are undertaken, as and when considered necessary, to address emerging issues in

cyberspace, technological advancements, evolving cyber threats, and changing regulatory requirements.

Further, the Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.

The 'National Cyber Crime Reporting Portal' (NCRP) (<https://cybercrime.gov.in>) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children.

Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.
