Explainer:

May 26, 2021

#Indian Government defence of Information Technology Rules places privacy and digital security at risk

On May 26, 2021, the Indian government issued a press release in response to a legal challenge filed by WhatsApp against the traceability mandate under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. We appreciate the government's intention to reassure users that it is committed to protecting the right to privacy. However, this attempt is premised on legally unsound principles and technically inaccurate explanations.

We disagree with the claim that the measures imposed by the rules will not impact users or the functioning of end-to-end encrypted messaging services. A defining feature of end-to-end encrypted services, such as WhatsApp and Signal, is that no party other than the sender and the intended recipients, including the service provider, can access the content or discern who sent which message to whom. In order to implement traceability to identify the "first originator" of content, end-to-end encrypted services will have to fundamentally re-design their architecture to eliminate this feature. As a direct result, the core promise of privacy and security of such messaging platforms will be compromised, leading to a chilling effect on free expression. Therefore, traceability will irreversibly transform the functioning of end-to-end encrypted services, and jeopardize users' privacy and freedom of expression.

The government's assertion that traceability constitutes a reasonable restriction to the right to privacy fails the necessity and proportionality test, laid down by the Indian Supreme Court in the *Puttaswamy* judgement, to assess whether a restriction to the right to privacy is reasonable. The traceability mandate imperils the human rights of millions of users for the mere possibility of identifying a few miscreants online. This possibility is slim because bad actors will swiftly shift to other platforms, or devise their own, whereas the public at large will be deprived of secure spaces online. Traceability impedes users' rights to a greater extent than necessary to achieve the stated objectives, and the relevant provision in the rules is devoid of any material safeguards against abuse, which is a necessary element of the test. The mandate treats all users as potential criminal suspects, against the basic principle of presumption of innocence and international human rights

For More Information
Please visit
www.accessnow.org

Media Contact:
Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director,
Access Now
Tel: +91 9717653293; or 1-888-414-010
email: press@accessnow.org
Twitter: @accessnow

standards. The government's insistence on ending traceability has to be seen against the broader context of shrinking civic space, where exceptions carved out in laws are weaponised and selectively applied against dissenters and at-risk communities.

A necessary consequence of the traceability requirement is onerous data retention obligations on the intermediary. Intermediaries will have to create and store information that has so far been unavailable even to service providers, in order to assist government agencies - going against data minimization principles. The press release indicates that intermediaries have the ability to devise methods of implementing traceability that protect privacy while still enabling access to information pertaining to end-to-end encrypted communications. This is not technologically feasible. End-to-end encryption is undermined the moment something is linked to a message that the service provider can track. End-to-end encryption with scope for exceptional access is no longer end-to-end encryption. That is simply how the math enabling the technology works, not a choice that intermediaries make. A single vulnerability created to enable traceability will expose the platform and its users to manipulation by malicious actors. Public interest can be preserved without infringing privacy and security, but not by weakening end-to-end encryption.

The rules were not, as the government claims, framed in consultation with stakeholders. The rules, in their current form, are drastically different from the draft on which comments were invited in 2018, and well beyond what the executive branch can issue as subordinate rules without proposing a new bill to Parliament. The traceability mandate in the 2018 draft, among other things, was widely criticized. The current version of the rules did not undergo any public consultation. It carries dangerous new provisions that were completely absent in the 2018 draft, or even more problematic versions of provisions that were criticized in the earlier draft. This is against the government's own pre-legislative consultation policy. The policy requires that subordinate rules be placed in the public domain for at least 30 days prior and that a summary of comments be published.

We urge the government to reconsider the enforcement of these rules as they are prejudicial to the fundamental right to privacy and freedom of expression guaranteed by the Indian Constitution. A sustained, public and multi-stakeholder consultation is an essential prerequisite to the enactment of a framework that has such a profound effect on human rights. Since the rules also carry provisions that are beyond the scope of the parent legislation, they must also be made subject to parliamentary scrutiny.

We call on intermediaries to implement measures to protect privacy, free expression and security, and push back on overbroad, unlawful requests and regulatory mandates. Intermediaries must follow due procedure under applicable laws and international human rights standards in assessing

requests from government agencies. Companies must share, transparently and publicly, details of the number and the nature of requests for information or directions for content moderation received from government agencies, the grounds on which the requests were made, and the manner in which the company responded, including the information that was disclosed.

[*This brief was prepared by Namrata Maheshwari, with inputs from Ria Singh Sawhney and Raman Jit Singh Chima*]