# India’s Draconian Rules for Internet Platforms Threaten User Privacy and Undermine Encryption

## Description

INDIA: The Indian government’s new Intermediary Guidelines and Digital Media Ethics Code (“2021 Rules”) pose huge problems for free expression and Internet users’ privacy. They include dangerous requirements for platforms to identify the origins of messages and pre-screen content, which fundamentally breaks strong encryption for messaging tools. Though WhatsApp and others are challenging the rules in court, the 2021 Rules have already gone into effect.

Three UN Special Rapporteurs—the Rapporteurs for Freedom of Expression, Privacy, and Association—heard and in large part affirmed civil society’s criticism of the 2021 Rules, acknowledging that they did “not conform with international human rights norms.” Indeed, the Rapporteurs raised serious concerns that Rule 4 of the guidelines may compromise the right to privacy of every internet user, and called on the Indian government to carry out a detailed review of the Rules and to consult with all relevant stakeholders, including NGOs specializing in privacy and freedom of expression.

2021 Rules contain two provisions that are particularly pernicious: the Rule 4(4) Content Filtering Mandate and the Rule 4(2) Traceability Mandate.

## Content Filtering Mandate

Rule 4(4) compels content filtering, requiring that providers are able to review the content of communications, which not only fundamentally breaks end-to-end encryption, but creates a system for censorship. Significant social media intermediaries (i.e. Facebook, WhatsApp, Twitter, etc.) must “endeavor to deploy technology-based measures,” including automated tools or other mechanisms, to “proactively identify information” that has been forbidden under the Rules. This cannot be done without breaking the higher-level promises of secure end-to-end encrypted messaging.

Client-side scanning has been proposed as a way to enforce content blocking without technically breaking end-to-end encryption. That is, the user’s own device could use its knowledge of the unencrypted content to enforce restrictions by refusing to transmit, or perhaps to display, certain prohibited information, without revealing to the service provider who was attempting to communicate or

view that information. That's wrong. Client side-scanning requires a robot-spy in the room. A spy in a place where people are talking privately makes it not a private conversation. If that spy is a robot-spy like with client-side scanning, it is still a spy just as much as if it were a human spy.

As we explained last year, client-side scanning inherently breaks the higher-level promises of secure end-to-end encrypted communications. If the provider controls what's in the set of banned materials, they can test against individual statements, so a test against a set of size 1, in practice, is the same as being able to decrypt a message. And with client-side scanning, there's no way for users, researchers, or civil society to audit the contents of the banned materials list.

The Indian government frames the mandate as directed toward terrorism, obscenity, and the scourge of child sexual abuse material, but the mandate is actually much broader. It also imposes proactive and automatic enforcement of the 2021 Rule's Section (3)1(d)'s content takedown provisions requiring the proactive blocking of material previously held to be "information which is prohibited under any law," including specifically laws for the protection 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," and incitement to any such act. This includes the widely criticized Unlawful Activities Prevention Act, which has reportedly been used to arrest academics, writers and poets for leading rallies and posting political messages on social media.

This broad mandate is all that is necessary to automatically suppress dissent, protest, and political activity that a government does not like, before it can even be transmitted. The Indian government's response to the Rapporteurs dismisses this concern, writing "India's democratic credentials are well recognized. The right to freedom of speech and expression is guaranteed under the Indian Constitution."

The response misses the point. Even if a democratic state applies this incredible power to preemptively suppress expression only rarely and within the bounds of internationally recognized rights to freedom of expression, Rule(4)4 puts in place the tool kit for an authoritarian crackdown, automatically enforced not only in public discourse, but even in private messages between two people.

Moreover, rules like these give comfort and credence to authoritarian efforts to enlist intermediaries to assist in their crackdowns. If this Rule were available to China, word for word, it could be used to require social media companies to block images of Winnie the Pooh as it happened in China from being transmitted, even in direct "encrypted" messages.

Automated filters also violate due process, reversing the burden of censorship. As the three UN Special Rapporteurs made clear, a

> general monitoring obligation that will lead to monitoring and filtering of user-generated content at the point of upload … would enable the blocking of content without any form of due process even before it is published, reversing the well-established presumption that States, not individuals, bear the burden of justifying restrictions on freedom of expression.

## Traceability Mandate

The traceability provision, in Rule 4(2), requires any large social media intermediary that provides

messaging services to “enable the identification of the first originator of the information on its computer resource” in response to a court order or a decryption request issued under the 2009 Decryption Rules. The Decryption Rules allow authorities to request the interception or monitoring of any decrypted information generated, transmitted, received, or stored in any computer resource..

The Indian government responded to the Rapporteur report, claiming to honor the right to privacy:

> The Government of India fully recognises and respects the right of privacy, as pronounced by the Supreme Court of India in K.S. Puttaswamy case. Privacy is the core element of an individual’s existence and, in light of this, the new IT Rules seeks information only on a message that is already in circulation that resulted in an offence.

This narrow view of Rule (4)4 is fundamentally mistaken. Implementing the Rule requires the messaging service to collect information about all messages, even before the content is deemed a problem, allowing the government to conduct surveillance with a time machine. This changes the security model and prevents implementing strong encryption that is a fundamental backstop to protecting human rights in the digital age.

## The Danger to Encryption

Both the traceability and filtering mandates endanger encryption, calling for companies to know detailed information about each message that their encryption and security designs would otherwise allow users to keep private.  Strong end-to-end encryption means that only the sender and the intended recipient know the content of communications between them. Even if the provider only compares two encrypted messages to see if they match, without directly examining the content, this reduces security by allowing more opportunities to guess at the content.

It is no accident that the 2021 Rules are attacking encryption. Riana Pfefferkorn, Research Scholar at the Stanford Internet Observatory, wrote that the rules were intentionally aimed at end-to-end encryption since the government would insist on software changes to defeat encryption protections:

> Speaking anonymously to *The Economic Times*, one government official said the new rules will force large online platforms to “control” what the government deems to be unlawful content: Under the new rules, “platforms like WhatsApp can’t give end-to-end encryption as an excuse for not removing such content,” the official said.

The 2021 Rules’ unstated requirement to break encryption goes beyond the mandate of the Information Technology (IT) Act, which authorized the 2021 Rules. India’s Centre for Internet & Society’s detailed legal and constitutional analysis of the Rules explains: “There is nothing in Section 79 of the IT Act to suggest that the legislature intended to empower the Government to mandate changes to the technical architecture of services, or undermine user privacy.” Both are required to comply with the Rules.

There are better solutions. For example, WhatsApp found a way to discourage massive chain forwarding of messages without itself knowing the content. It has the app note the number of times a message has been forwarded inside the message itself so that the app can then change its behavior

based on this. Since the forwarding count is inside the encrypted message, the WhatsApp server and company don’t see it. So your app might not let you forward a chain letter, because the letter’s content shows it was massively forwarded, but the company can’t look at the encrypted message and know it’s content.

Likewise, empowering users to report content can mitigate many of the harms that inspired the Indian 2021 Rules. The key principle of end-to-end encryption is that a message gets securely to its destination, without interception by eavesdroppers. This does not prevent the recipient from reporting abusive or unlawful messages, including now-decrypted content and the sender’s information. An intermediary may be able to facilitate user reporting, and still be able to provide the strong encryption necessary for a free society. Furthermore, there are cryptographic techniques for a user to report abuse in a way that identifies the abusive or unlawful content without the possibility of forging a complaint and preserving the privacy of those people not directly involved.

The 2021 Rules endanger encryption, weakening the privacy and security of ordinary people throughout India, while creating tools which could all too easily be misused against fundamental human rights, and which can give inspiration for authoritarian regimes throughout the world. The Rules should be withdrawn, reviewed and reconsidered, bringing the voices of civil society and advocates for international human rights, to ensure the Rules help protect and preserve fundamental rights in the digital age.

By Katitza Rodriguez and Kurt Opsahl

**Category**

1. History-Archaeology-Past Mysteries
2. Main

**Tags**

1. Arménsko
2. Genocída
3. Masakr
4. Turecko

**Date Created**
07/26/2021