

## CUTS Webinar

# Discussing the Information Technology (Intermediary Guidelines) Rules, 2021 from the Lens of Consumer Welfare & EoDB

06 May 2021 • 04.30 pm - 06.00 pm (IST)

## Background

The recently released Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021<sup>1</sup> (rules), lays down guidelines for due diligence to be followed by intermediaries, which present a plethora of implementation challenges for intermediaries, and pose risks to consumer welfare. The rules make it mandatory for significant social media intermediaries to enable traceability of originators of certain objectionable content<sup>2</sup> and deploy technology-based measures, including automated tools or other mechanisms to identify certain kinds of problematic information proactively.<sup>3</sup>

It has been argued that enabling traceability of originators of the content may require intermediaries to break end-to-end encryption for compliance. This is likely to dilute consumers' privacy on encrypted instant messaging service providers, risking infringement of their fundamental right to privacy. Also, requiring intermediaries to deploy technology-based solutions for identifying problematic content would prompt them to process more consumer data for compliance, which may be contrary to the principles of data minimisation and limitation.

Such weakening of data protection and privacy risks may dent consumer's trust in digital technology-driven communication services. As found by the CUTS study 'Understanding Consumers Perspective on Encryption,'<sup>4</sup> consumers value the privacy of their communication and claim to be willing to pay INR 1 per for it. They are likely to reduce or completely stop exchanging certain kinds of information if privacy is compromised or even perceived to be at risk. Also, consumers were found to give equal importance to curbing the spread of problematic content and privacy and were unwilling to trade the latter for the former.

These risks emanating from compliance are further compounded by the rules requiring intermediaries to appoint a Chief Compliance Officer who may be made liable under applicable laws, including the Indian Penal Code, if the intermediary fails to observe due diligence under the rules.<sup>5</sup> Such a provision may force intermediaries to over-comply with the rules to safeguard

---

<sup>1</sup> Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at: [https://www.meity.gov.in/writereaddata/files/Intermediary\\_Guidelines\\_and\\_Digital\\_Media\\_Ethics\\_Code\\_Rules-2021.pdf](https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf)

<sup>2</sup> S. 4(2) of the Rules.

<sup>3</sup> S. 4(4) of the Rules.

<sup>4</sup> CUTS report on Understanding Consumers Perspective on Encryption, available at: <https://cuts-ccier.org/pdf/survey-finding-understanding-consumers-perspective-on-encryption.pdf>

<sup>5</sup> S. 4(1)(a), read with S. 7 of the Rules.

themselves from prosecution, resulting in excessive and additional data collection, monitoring/processing and content takedown. The short timeline available for implementing the requirement also remains an area of concern for intermediaries in this regard.

It also remains to be checked as to how and whether startups, who may fall in the category of significant data fiduciaries, would find the wherewithal to comply with such due diligence requirements. This may adversely impact the government's Startup India mission, thereby having a chilling effect on innovation.

Furthermore, the guidelines empower the executive, i.e., government and its agencies, to order intermediaries to take down content, and compel them to provide information and assistance for various purposes. However, the rules do not mandatorily require any judicial oversight while exercising these powers, thereby giving the state and its agencies arbitrary discretion.<sup>6</sup> This fuels risks of arbitrary censoring of content, thereby curbing consumers' access to information.

## About the Webinar

Given such possible adverse impact of the rules, the webinar seeks to discuss its relevant provisions from the lens of consumer welfare and ease of doing business. A reference would also be made to relevant intermediary guidelines in other jurisdictions, such as United States,<sup>7</sup> European Union,<sup>8</sup> Australia,<sup>9</sup> New Zealand,<sup>10</sup> Manilla Principles on Intermediary Liability,<sup>11</sup> etc. The following issues may be touched upon in the discussion.

- Traceability of originators of content: balancing the need for identifying the originator of problematic content and securing the privacy of chats of consumers.
- Proactive identification of problematic content: curbing the spread of problematic content, while respecting principles of data minimisation and limitation.
- Impact on startups: ensuring the growth of startups by reducing compliance burdens for continued innovation.
- Risks of over-compliance: penal provisions for failing to conduct due diligence leading to risks of over-compliance, which may harm consumer welfare.
- Judicial oversight: the need for mandatory judicial oversight in executive orders of content takedown.

---

<sup>6</sup> S. 3(1)(d) of the Rules.

<sup>7</sup> Section 512(c) of the Digital Millennium Copyright Act ("DMCA") and Section 230 of the Communications Decency Act ("CDA").

<sup>8</sup> Articles 12 to 15 of Directive 2000/31/EC of 8 June 2000 on electronic commerce; Directive 2001/29/EC on Copyright in the Information Society (as to copyright) and Directive 2004/48/EC on the Enforcement of Intellectual Property Rights (other than copyright); Regulation on Preventing the Dissemination of Terrorist Content Online; Code of conduct on countering illegal hate speech online

<sup>9</sup> Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill, 2019

<sup>10</sup> Harmful Digital Communications Act

<sup>11</sup> Available at: <https://manilaprinciples.org/index.html>

## Agenda

Time	Session	Speaker(s)
4.30pm to 4.35pm	Opening Remarks	<b>Bipul Chatterjee</b> , Executive Director, CUTS International
4.35pm to 4.40pm	Presentation	<b>Setu Bandh Upadhyay</b> , Consultant, CUTS International
4.40pm to 5.55pm	Panel discussion, including a question and answer session, moderated by <b>Amol Kulkarni</b> , Director – Research, CUTS International	<ul style="list-style-type: none"> <li>• <b>Amar Patnaik</b>, Hon. Member of Parliament (MP), &amp; Member, Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 (PDPB)</li> <li>• <b>Ritesh Pandey</b>, Hon. MP, &amp; Member, JPC on PDPB</li> <li>• <b>Rakesh Maheshwari</b>, Group Coordinator and Head- Cyber Law, Ministry of Electronics &amp; Information Technology (MeitY)</li> <li>• <b>Ashish Aggarwal</b>, Vice President – Public Policy, National Association of Software and Service Companies (NASSCOM)</li> <li>• <b>Daniel Castro</b>, Vice President, Information Technology &amp; Innovation Foundation (ITIF), and Director, Centre for Data Innovation</li> <li>• <b>Amber Sinha</b>, Executive Director, Centre for Internet and Society (CIS)</li> </ul>
5.55pm to 6.00pm	Closing Remarks	<b>Sidharth Narayan</b> , Assistant Policy Analyst, CUTS International