



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

META PLATFORMS INC. & WHATSAPP LLC v. UNION OF INDIA

A Case Commentary

- *Ms. Aashi Lalchand Khanchandani*

-

Case Title	: Meta Platforms Inc. & WhatsApp LLC v. Union of India
Citation	: S.L.P. (C) No. 9479 of 2025 (S.C.) (India)
Court	: Supreme Court of India
Bench	: Three-Judge Bench (Majority: 2:1)
Date of Judgment	: April 3, 2026
Area of Law	: Constitutional Law; Technology Law; Privacy and Digital Rights
Statutes Involved	: INDIA CONST. arts. 19(1)(a), 19(2), 21; Information Technology Act, No. 21 of 2000; IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Digital Personal Data Protection Act, No. 22 of 2023

1. INTRODUCTION

Since 2021, the regulation of encrypted digital communications in India has been characterized by ongoing constitutional disputes. The Ministry of Electronics and Information Technology issued the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 under the Information Technology Act, 2000,¹ with Rule 4(2) presenting

¹ Information Technology Act, No. 21 of 2000

the most significant challenge to platforms employing end-to-end encryption.² This provision required major social media intermediaries providing messaging services to facilitate identification of the “*first originator*” of any message upon request from a competent court or designated government authority. WhatsApp LLC, whose encryption architecture is inherently incompatible with retrospective originator tracing, contested the rule before the Delhi High Court in 2021.³ The dispute was ultimately adjudicated by a three-judge bench of the Supreme Court. The judgment delivered on April 3, 2026, which invalidated Rule 4(2) as unconstitutional, represents a significant development in Indian digital rights jurisprudence.

The case required the Court to consider three intersecting constitutional guarantees: the fundamental right to privacy under Article 21, as articulated in *K.S. Puttaswamy v. Union of India*,⁴ the right to freedom of speech and expression under Article 19(1)(a),⁵ and the State's authority to impose reasonable restrictions under Article 19(2).⁶ This commentary argues that, although the majority opinion of the Court reached the correct outcome, it is incomplete because it does not establish a constitutionally compliant framework for digital surveillance. This omission has resulted in a pressing regulatory gap that requires legislative intervention.

I. FACTS

1. WhatsApp LLC, part of Meta Platforms Inc., runs an end-to-end encrypted messaging service with over 500 million Indian users. Only communicating parties hold the cryptographic keys, so WhatsApp cannot read messages or identify message originators.
2. Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021—which falls under the Information Technology Act, 2000 required “*significant social media intermediaries*” that provide messaging services to enable the identification of the “*first originator*” of any information upon a court or government order.

² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2), G.S.R. 139(E)

³WhatsApp LLC v. Union of India, W.P. (C) No. 1121 of 2021

⁴ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

⁵ India Const. art. 19(1)(a).

⁶ India Const. art. 19(2).

3. WhatsApp challenged Rule 4(2) before the Delhi High Court in 2021, after which the case was referred to a division bench. The Supreme Court subsequently transferred the matter to itself and constituted a three-judge bench. The Union of India defended Rule 4(2) as necessary to trace sources of misinformation, incitement to violence, and child sexual abuse material.
- 4.

II. ISSUES

The courts framed three issues :

1. Whether Rule 4 (2) violates the fundamental right to privacy under Article 21 by compelling a misappropriate invasion of end-to-end encrypted communications?
2. Whether it imposes an unconstitutional chilling effect on freedom of speech and expression under Article 19(1)(a)?
3. Whether Rule 4(2) exceeds the rule-making authority granted by Section 87 of the Information Technology Act, 2000?

III. HOLDING

By a 2-1 majority, the Supreme Court struck down Rule 4(2) as unconstitutional under Articles 19(1)(a) and 21. The majority did not decide the ultra vires ground, finding the constitutional infirmity sufficient for relief.⁷

IV. REASONING

Proportionality and Privacy - The majority held that end-to-end encryption and the right to private communication are inseparable. Mandating originator traceability would create a permanent flaw in the encryption, exposing all users not just those under investigation—to surveillance. Such a systemic breach fails the necessity prong of the proportionality test from *K.S. Puttaswamy v. Union of India*.⁸

⁷ Supra note 4, slip op. at 2–3.

⁸ Supra note 5, at ¶ 645 (Chandrachud, J., concurring)

Chilling Effect on Speech -- The Court found the rule would drive users to self-censorship. Even if tracing never occurs, knowing messages could be attributed to their originator suppresses constitutionally protected expression online.⁹

Lack of a Precise Legal Framework - Rule 4(2) lacks independent judicial review, time limits, or sunset clauses. It creates an ongoing risk of mass surveillance without the safeguards traditionally required for State access to private communications.¹⁰

The dissenting judge would uphold the rule, arguing that identifying the originator unlike decrypting content is a proportionate restriction justified by the need to trace illegal content.¹¹

V. ANALYSIS

A. The Proportionality Approach Is Doctrinally Sound

The majority's key contribution is analyzing technical architecture, not just governmental intent. Proportionality under *Puttaswamy* requires courts to consider both the State's purpose and the structural impact of its methods.¹² A mechanism that cannot target only suspects but invades everyone's privacy is structurally disproportionate. This aligns with the approach in *Carpenter v. United States*, where the U.S. Supreme Court held that digital records warrant greater constitutional protection due to their scope and sensitivity.¹³

B. The Originator-Content Distinction Is Technically Indefensible

The dissent accepted the government's claim that tracing the sender, not content, falls outside core privacy rights. For end-to-end encryption, this is incorrect. Identifying a message's sender needs either plaintext metadata stored on each device or a key-escrow or hash-tagging system both structural backdoors. The EU's General Data Protection Regulation requires "*privacy by design*" to prevent such vulnerabilities that can be exploited by malicious actors, foreign states,

⁹ Supra note 4, slip op. at 9.

¹⁰ *Id* at 10–11.

¹¹ *Id* at 13 (dissent).

¹² Supra note 5, at ¶ 645.

¹³ *Carpenter v. United States*, 585 U.S. 296, 310 (2018).

and insiders beyond lawful orders.¹⁴ The majority's lack of technical detail leaves room for new legislation to label originator tracing as mere "*metadata*".

C. International Law Was Underused

Article 17 of the ICCPR and UN Human Rights Committee General Comment No. 16 set that systemic surveillance likely violates privacy rights. Puttaswamy advised referencing international norms for interpreting rights.¹⁵ Tying proportionality analysis to these would have made it harder for officials to bypass constitutional limits through new regulations. This was a missed chance.¹⁶

D. The Judgment's Central Weakness: No Filled Vacuum

A major concern is the majority's refusal to prescribe interim safeguards. In *People's Union for Civil Liberties v. Union of India* (1997)¹⁷, the Court set out procedural protections for telephone tapping independent review, time limits, and the destruction of irrelevant data pending legislation. The digital context needs similar measures. The Digital Personal Data Protection Act, 2023 does not address government access to personal data via intermediaries.¹⁸ Thus, the regulatory gap that invalidated Rule 4(2) persists. The Court had precedent and authority to provide interim safeguards. Its inaction has consequences.

VI. GAPS AND SUGGESTIONS

Three legislative reforms are urgent. First, the Digital Personal Data Protection Act, 2023 must be amended to include a chapter on State access to data held by intermediaries, requiring prior judicial authorization (except certified emergencies), specified grounds, and post-hoc independent review. Second, Section 69 of the Information Technology Act, 2000 which empowers the government to issue directions for interception, monitoring, or decryption of information needs statutory proportionality review, sunset clauses, and parliamentary reporting

¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 25, Apr. 27, 2016, 2016 O.J. (L 119) 1 (GDPR)

¹⁵ Supra note 5, at ¶ 309 (Nariman, J., concurring).

¹⁶ International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171; UN Human Rights Comm., General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (1988)

¹⁷ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301, ¶ 31

¹⁸ Digital Personal Data Protection Act, No. 22 of 2023, §§ 7–9

obligations.¹⁹ Third, the government should commission an independent technical body (including cryptologists, civil society, and retired judges) to assess whether any constitutionally permissible form of originator accountability exists without degrading the encryption architecture. These are not merely policy suggestions; the constitutional holding creates a positive legislative obligation, and future courts should hold Parliament to that duty.

CONCLUSION

Meta Platforms Inc. & WhatsApp LLC v. Union of India is constitutionally solid but incomplete for digital privacy. The majority rightly struck down originator traceability as a disproportionate invasion of privacy and chill on free speech. However, by not outlining any alternative or safeguards, the Court left a gap that the executive may exploit. As Justice Kaul noted in *Puttaswamy*, privacy is ***“the ultimate expression of the sanctity of the individual”***.²⁰ Protecting that sanctity in the digital age needs more than invalidation; it requires precise, constitutionally sound legislative action and demands the State justify any new surveillance as proportionate.

¹⁹ Information Technology Act, No. 21 of 2000, § 69

²⁰ *Supra* note 5, at ¶ 180 (Kaul, J., concurring).