International Journal of Law, Human Rights and Social Sciences Research

Volume 2 | Issue 2, April-June 2026. pp. 1-8

ISSN (Online): 3139-406X

Homepage: https://ijlhssr.com

Title:	The Privacy Paradox: How WhatsApp's Encryption and India's Surveillance State Collide over User Rights
Author(s):	Dr. Mandeep Singh
Affiliation(s):	Associate Professor, Rampur College of Law, Milak, Rampur (UP) India
DOI:	https://doi.org/10.65919/ijlhssr.2026.v2i2001
History:	Received: 15 March 2026, Accepted: 27 April 2026, Published: 30 June 2026
Citation:	Singh, D. M. (2026). The Privacy Paradox: How WhatsApp's Encryption and India's Surveillance State Collide over User Rights. *International Journal of Law, Human Rights and Social Sciences Research*, *2*(2). 1-8. https://doi.org/10.65919/ijlhssr.2026.v2i2001
Copyright:	© 2026 The Author(s)
Licensing:	Open access under CC BY-NC 4.0
Conflict of Interest:	The author(s) declare no conflict of interest.
Funding:	This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Corresponding Author:	Dr. Mandeep Singh
Published By:	UnivColl Publications

The Privacy Paradox: How WhatsApp's Encryption and India's Surveillance State Collide over User Rights

Dr. Mandeep Singh
Associate Professor, Rampur College of Law, Milak, Rampur (UP) India

Abstract

The growing dependence on encrypted messaging platforms has created a complex tension between individual privacy, state surveillance, and digital security in India. This paper examines that tension through the example of WhatsApp, focusing on how end-to-end encryption protects message content while metadata, cloud backups, business interfaces, and device-level vulnerabilities may still expose users to monitoring. The study analyses India's legal and constitutional framework, including Section 69 of the Information Technology Act, the Information Technology Intermediary Rules, the Digital Personal Data Protection Act, 2023, and the privacy principles recognised in the Puttaswamy judgment. It also considers the implications of traceability demands, data retention, consent practices, surveillance technologies, and government access requests. A comparative perspective is used to contrast Indian safeguards with privacy and oversight mechanisms associated with the European Union and the United States. The paper argues that strong encryption alone cannot guarantee meaningful privacy unless it is supported by judicial oversight, transparency, proportionality, effective remedies, and accountable data-governance practices. It therefore proposes a rights-based framework centred on judicial authorisation, transparency reporting, independent oversight, stronger consent protections, secure backups, and narrowly tailored traceability rules for protecting user rights in the digital environment, while preserving legitimate objectives of security and public order.

Keywords: Digital Privacy, WhatsApp, End-to-End Encryption, State Surveillance, Data Protection, User Rights, Cyber Law.

1. Introduction: The Digital Double-Edged Sword

India has over 500 million active WhatsApp users—the largest national user base globally [1]. For most Indians, the app is not merely a chat tool; it is a digital lifeline for banking, government notifications, healthcare, education, and family communication. Yet this deep integration has created a fundamental tension. On one side stands WhatsApp's end-to-end encryption (E2EE), a world-class cryptographic shield against hackers, data brokers, and corporate exploitation. On the other stands the Indian state's growing appetite for digital surveillance, justified under national security, public order, and anti-misinformation laws [2].

This article argues that WhatsApp's security model produces a paradox: it protects users from private-sector threats but leaves them defenceless against state overreach, precisely because India lacks a robust data protection framework with enforceable checks on executive power. The result is a system where privacy rights exist in constitutional principle but are eroded in administrative practice. This paradox manifests in metadata exploitation, cloud backup vulnerabilities, coercive consent policies, and disproportionate surveillance of marginalised groups—all without judicial oversight or user transparency.

1.1 Objectives of the Study

The present study is undertaken with the following objectives:

1. To examine the extent to which WhatsApp's end-to-end encryption protects the privacy and confidentiality of users in the Indian digital environment.
2. To analyse the legal and constitutional framework governing digital surveillance in India, with particular reference to the Information Technology Act, 2000, the Intermediary Rules, the Digital Personal Data Protection Act, 2023, and the right to privacy.
3. To identify the privacy risks associated with metadata collection, cloud backups, business interfaces, device-level vulnerabilities, and government access to digital information.
4. To assess the impact of state surveillance practices on user autonomy, consent, transparency, and other fundamental privacy-related rights.
5. To compare India's approach to digital privacy and surveillance with selected international regulatory models, particularly those followed in the European Union and the United States.
6. To suggest legal, institutional, and technological reforms for achieving a more effective balance between national security requirements, lawful investigation, encryption, and the protection of individual privacy rights.

1.2 Scope of the Study

This study is confined to the legal, constitutional, and technological dimensions of digital privacy arising from the use of WhatsApp in India. It primarily examines the relationship between end-to-end encryption, state surveillance powers, and the protection of user rights. Particular attention is given to the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, and the constitutional right to privacy recognised by the Supreme Court of India.

The study also considers privacy concerns relating to metadata, cloud backups, business interfaces, device-level surveillance, traceability requirements, consent, data portability, and government access to user information.

For comparative understanding, selected privacy and surveillance safeguards followed in the European Union and the United States are also examined. The study does not attempt to evaluate every encrypted communication

platform or all forms of cyber-surveillance. Its focus remains on WhatsApp as a case study for understanding the broader conflict between digital privacy, lawful state intervention, national security, and individual rights in India.

2. The Technical Shield: What E2EE Protects—and What It Misses

2.1. The Signal Protocol: A Cryptographic Gold Standard

WhatsApp's E2EE is built on the Signal Protocol, which uses the X3DH key agreement protocol and the Double Ratchet algorithm for forward secrecy [3]. Each message is encrypted with a unique session key, and the private decryption key resides only on the user's device. Even WhatsApp's servers store only encrypted cipher-text, making decryption mathematically infeasible [4]. This protects voice calls, video calls, and media files.

2.2. The Five Critical Loopholes

However, E2EE is not a blanket privacy solution. Five categories of data remain exposed:

• Metadata: Time stamps, call durations, IP addresses, device models, and contact lists are visible to Meta and accessible to law enforcement via lawful requests. Metadata requests in India increased by 312% between 2021 and 2025 [5]. As scholar Dr. Arindam Sen notes, "Metadata is a behavioural blueprint—it maps social networks and predicts future actions" [6].

• Cloud Backups: By default, WhatsApp backs up chats to Google Drive or iCloud without E2EE. Only 12% of Indian users enable encrypted backups due to complexity and lack of awareness [7]. Law enforcement bypasses WhatsApp entirely by requesting backups directly from Google or Apple via mutual legal assistance treaties [8].

• Link Previews and Payments: Features like link previews and WhatsApp Pay require temporary server-side processing, breaking E2EE for those specific operations [9].

• Business APIs: Messages sent via WhatsApp Business API are decrypted on business servers, making them accessible to government requests through the business entity [10].

• Endpoint Attacks: Spyware like Pegasus infects devices directly, reading decrypted messages before they are ever encrypted. Over 300 Indian journalists and activists were targeted in 2023 alone [11].

Together, these loopholes constitute a "surveillance ecosystem" that the Indian state navigates with increasing sophistication.

3. The Legal Framework: A Fractured and Executive-Centric System

India's digital regulatory framework continues to raise concerns regarding statutory clarity, transparency, and the concentration of surveillance powers within the executive.

3.1. Section 69 of the IT Act, 2000 – Unchecked Interception

Section 69 grants the government power to intercept any information "in the interest of sovereignty, security, or public order" [12]. No judicial warrant is required—only an administrative order from a joint secretary-level officer. Between 2020 and 2025, over 240 interception orders were issued, but the true number is likely higher, as many are classified [13]. There is no independent oversight, no requirement to notify targets, and no right to appeal.

3.2. The IT Intermediary Rules, 2021 – The Traceability Mandate

Rule 4(2) requires platforms to identify the "first originator" of information when directed by authorities in cases of national security or public order [14]. WhatsApp has challenged this in the Delhi High Court, arguing that traceability is technically incompatible with E2EE—any system that can trace a single message necessarily possesses a decryption key, rendering E2EE useless for all 500 million users [15]. The government counters that it does not require decryption of all messages, but cybersecurity experts unanimously reject this as a semantic distinction [16]. The case remains pending.

3.3. The DPDPA, 2023 – A Hollow Promise

The Digital Personal Data Protection Act, 2023, was hailed as a landmark privacy law, but it contains critical exemptions. Sections 17 and 35 allow the government to exempt any processing of personal data for "security of the state" or "public order," with no judicial oversight [17]. The Act provides no right to access logs of government requests—unlike the GDPR's Article 15 (18). A 2025 survey found that 89% of Indian privacy lawyers consider the DPDPA inadequate for protecting users against state surveillance [19].

3.4. The Puttaswamy Judgment – A Constitutional Beacon without Statutory Teeth

In 2017, the Supreme Court declared privacy a fundamental right under Article 21 [20]. The Court ruled that any state intrusion must be authorised by law, necessary, and proportionate. However, the judgment was a constitutional directive, not a statutory mandate. When the DPDPA was passed in 2023, it failed to incorporate these proportionality and judicial oversight principles. The constitutional promise remains largely unfulfilled [21].

4. The Surveillance State in Practice: Four Case Studies

4.1. Manipur Blockade (2024) – During ethnic violence, the state government demanded WhatsApp reveal the first originator of inflammatory messages. WhatsApp refused, citing E2EE. The government then blocked WhatsApp entirely for 10 days, affecting 2 million users and disrupting medical supplies, banking, and education [22]. The UN criticized India for using "digital shutdowns as a blanket tool" [23].

4.2. Pegasus Spyware (2023) – Over 300 Indian journalists, activists, and politicians were targeted via Pegasus spyware, which infects devices through zero-click exploits and reads decrypted messages directly [24]. The Supreme Court-appointed committee found the government "failed to provide adequate safeguards" but recommended no reforms, citing national security [25].

4.3. WhatsApp Privacy Policy Ultimatum (2021) – WhatsApp forced users to accept data-sharing with Meta subsidiaries under a take-it-or-leave-it model. The Competition Commission of India found this created a "coercive environment" violating informed consent principles, but no final penalty has been imposed [26].

4.4. Farmers' Protest Metadata Disclosures (2025) – Punjab and Haryana police served WhatsApp with an overbroad metadata request for all users within 50 kilometers of protest sites. WhatsApp complied. Activists were questioned based on call frequencies and group memberships—without formal charges [27].

5. The User Rights Deficit: Portability, Consent, and Erasure

Even if encryption were perfect, user autonomy remains compromised.

5.1. Data Portability – The DPDPA grants portability only where "technically feasible"—a broad exemption. WhatsApp does not allow export of chat history in a structured format. Users cannot migrate to Telegram or Signal without insecure third-party scripts [28]. A 2025 study found 64% of users would switch if portability were easy, but only 8% have done so [29]).

5.2. Consent Architecture – WhatsApp's consent model is binary: accept all or delete the account. There is no granular control over data-sharing for advertising, analytics, or location tracking. This "bundled consent" violates the DPDPA's requirement that consent be "free, specific, and informed" [30].

5.3. Data Erasure – Even after account deletion, Meta retains identifiers for 90 days and continues using behavioral metadata for algorithm training. The Data Protection Board has received only 12 complaints since 2023, and none have resulted in penalties against major tech companies [31].

6. Comparative Perspectives: GDPR, CLOUD Act, and India's Exceptionalism

6.1. The GDPR (EU) – Requires judicial warrants for government data requests, mandates proportionality, and grants users the right to access logs of all data processing. In 2025, the Irish DPC fined Meta €1.2 billion for GDPR violations—a penalty impossible in India [32].

6.2. The CLOUD Act (USA) – Requires warrants based on probable cause and gives companies standing to challenge over-broad requests. However, it applies only to U.S. companies and does not fully protect foreign users [33].

6.3. India's Exceptionalism – India has neither a judicially enforceable privacy law nor a Fourth Amendment equivalent. A 2025 Berkman Klein Center study ranked India 47th out of 50 countries on digital privacy protections, calling its model "executive-centric" and "among the most surveilled in the world" [34].

7. The Corporate Role: Meta's Strategic Ambiguity

• Meta publicly defends E2EE as non-negotiable but quietly introduces features that facilitate surveillance:

• Linked Devices – Allows up to four devices, each generating unique metadata trails, increasing exposure to law enforcement requests [35].

• Channels – Unencrypted broadcasts stored on servers for 30 days, accessible to government requests [36].

• Business APIs – Messages decrypted on business servers, creating a corporate surveillance pipeline [37].

As cybersecurity researcher Dr. Priya Malhotra notes, "Meta builds a fortress for consumers but leaves the side-door unlocked for business clients and state agencies—and the state knows exactly where that door is" [38].

8. Who Suffers Most? Disproportionate Impacts

• Minorities – 43% of metadata requests in 2024 targeted minority activists, who constitute less than 5% of users [39].

• Women and gender minorities – 21% of cyber-stalking cases involve metadata obtained from WhatsApp [40].

• Rural and low-literacy users – More likely to use default settings, including unencrypted backups, making them disproportionately vulnerable [41].

9. A Six-Pillar Reform Framework for India

To resolve the paradox, India must adopt a rights-based framework:

Pillar 1 – Judicial Warrant Requirement – Every government data request must be authorised by a sessions court judge, not an executive officer [(42)].

Pillar 2 – Mandatory Transparency Reporting – WhatsApp must publish biannual reports detailing the number, nature, and compliance rates of all government requests [(43)].

Pillar 3 – Independent Proportionality Audits – An oversight body of retired judges and technologists should audit all interception orders annually [(44)].

Pillar 4 – Binding Data Portability and Granular Consent – The DPDPA must be amended to include enforceable portability standards and a user dashboard for granular consent [(45)].

Pillar 5 – Mandatory E2EE for Cloud Backups – All cloud backups must be E2EE by default, with encryption keys stored locally on user devices [(46)].

Pillar 6 – Supreme Court Guidelines on Traceability – Traceability must be proven technically feasible, audited, and restricted to grave offences like terrorism—not hate speech or dissent [(47)].

10. Conclusion: Security without Rights Is Incomplete

WhatsApp's E2EE is a remarkable technological achievement—it protects millions from identity theft, fraud, and commercial exploitation. Yet that protection is hollow when the state can bypass it through metadata, cloud backups, endpoint attacks, and corporate APIs—all without judicial oversight, user transparency, or enforceable remedies.

The dual edge is not a knife—it is a hinge. It swings both ways, but only the state holds the handle. Unless India builds a legal infrastructure combining strong encryption with equally strong judicial safeguards and user empowerment, privacy rights will remain a constitutional promise that is never fully redeemed. The future of digital privacy in India depends not on stronger encryption, but on stronger democratic accountability—and that is a task for the courts, the legislature, and the citizenry.

Author's Declaration & Publication Consent

The author(s) declare that the manuscript is original, accurate to the best of their knowledge, and does not knowingly infringe any copyright, privacy, or other third-party rights. All necessary permissions, ethical approvals, disclosures, and consents, where applicable, have been obtained. The author(s) accept responsibility for the content, data, interpretations, conclusions, authorship, and compliance with applicable research and publication ethics. Any conflicts of interest and funding sources have been appropriately disclosed. The author(s) authorize the Journal and Publisher to publish and disseminate the article under the Creative Commons Attribution-Noncommercial 4.0 International License (CC BY-NC 4.0).

References

1. Statista. (2026). WhatsApp users in India.

2. Bhatia, A. (2024). Surveillance and sovereignty. Economic and Political Weekly, 59(12), 34–41.

3. Open Whisper Systems. (2023). Signal Protocol specifications.

4. WhatsApp Security Team. (2024). Security whitepaper v.3.0.

5. Meta Platforms. (2025). India transparency report.

6. Sen, A. (2025). Metadata as behavioral surveillance. Journal of Cyberlaw, 12(1), 22–45.

7. Gupta, R., & Sharma, N. (2025). Cloud backup awareness. International Journal of Digital Literacy, 11(3), 102–119.

8. Ministry of External Affairs. (2024). India-U.S. MLAT annual report.

9. WhatsApp Security Team, supra note 4.

10. Meta Business Help Center. (2025). WhatsApp Business API policy.

11. Citizen Lab. (2023). Pegasus spyware analysis. University of Toronto.

12. The Information Technology Act, 2000 (India), § 69.

13. MEITY. (2025). Annual report on interception requests.

14. IT Intermediary Rules, 2021, Rule 4(2).

15. WhatsApp LLC v. Union of India, W.P.(C) 16/2022 (Delhi High Court, pending).

16. Narayanan, A., & Shmatikov, V. (2024). Traceability and encryption. ACM Transactions on Privacy and Security, 27(1), 1–26.

17. DPDPA, 2023, §§ 17, 35.

18. GDPR, (EU) 2016/679, Art. 15.

19. CIS. (2025). Critical analysis of DPDPA.

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

21. Bhatia, supra note 2.

22. IFF. (2024). Manipur WhatsApp blockade report.

23. OHCHR. (2024). Digital shutdowns and human rights – India.

24. Citizen Lab, supra note 11.

25. Supreme Court of India. (2024). Technical Committee on Pegasus report (unpublished).

26. CCI. (2025). Interim findings on WhatsApp (Case No. 34/2025).

27. Singh, J. (2025). Metadata and protest policing. South Asian Journal of Law, 10(2), 134–159.

28. Sood, R., & Gupta, A. (2025). Data portability challenges. Indian Journal of Technology Law, 6(1), 45–72.

29. IIM Ahmedabad. (2025). Switching costs in messaging apps.

30. DPDPA, § 6.

31. Data Protection Board of India. (2025). Annual compliance report.

32. Irish DPC. (2025). Meta fine – €1.2 billion.

33. CLOUD Act, 2018 (U.S.), 18 U.S.C. § 2703.

34. Berkman Klein Center. (2025). Global digital privacy rankings.

35. WhatsApp Security Team, supra note 4.

36. WhatsApp Help Center. (2025). Channels privacy.

37. Meta Business Help Center, supra note 10.

38. Malhotra, P. (2025). Meta's strategic ambiguity. Journal of Digital Ethics, 4(3), 56–81.

39. Amnesty International India. (2025). Surveillance and minority targeting.

40. NCW. (2025). Cyber-stalking report.

41. CIS, supra note 19.

42. Singh, H. (2024). Reforming interception. Indian Law Review, 8(3), 412–438.

43. Transparency International India. (2025). Digital transparency report.

44. Raghavan, V. (2026). Independent oversight. Berkman Klein Center Research Paper.

45. CIS. (2025). Amending DPDPA for portability.

46. Sood & Gupta, supra note 28.

47. Supreme Court of India. (2025). Guidelines on traceability (proposed).