

---

# **PRIVACY ON INSTAGRAM VERSUS GOVERNMENT TRACKING: THE INDIAN LEGAL CONUNDRUM (A CRITICAL ANALYSIS OF END-TO-END ENCRYPTION ROLLBACK AND THE FIRST ORIGINATOR TRACEABILITY MANDATE)**

---

Moazzam Daksh Hada, Seedling School of Law and Governance, Jaipur National University<sup>1</sup>

## **ABSTRACT**

The convergence of Meta's discontinuation of end-to-end encryption for Instagram Direct Messages in May 2026 and India's escalating demand for "first originator" traceability under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2026, has precipitated a constitutional crisis at the intersection of digital privacy and state surveillance. This paper critically examines the legal conflict arising from the technical incompatibility between encryption and governmental traceability mandates, situating the debate within India's constitutional framework, particularly Article 21's guarantee of the right to privacy as elucidated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* and the Digital Personal Data Protection Act, 2023. The study analyses Meta's strategic withdrawal of Instagram encryption officially attributed to low adoption but occurring against intensifying regulatory pressure and evaluates its implications for India's 400 million Instagram users. Through a doctrinal analysis of the traceability provision under Rule 4(2) of the Intermediary Guidelines, the pending WhatsApp litigation before the Delhi High Court, and the Supreme Court's recent interventions regarding Meta's data practices, this paper argues that the current regulatory architecture fails the proportionality test prescribed in *Puttaswamy*. The research demonstrates that the first originator requirement, while ostensibly directed at combating deepfakes and child sexual abuse material, operates as a de facto mass surveillance mechanism undermining encrypted communication. The paper proposes a rights-preserving framework that reconciles legitimate law-enforcement imperatives with constitutional privacy guarantees through judicial oversight, narrow tailoring, and sunset clauses for traceability orders.

---

<sup>1</sup> Student at Seedling School of Law and Governance, Jaipur National University

## INTRODUCTION: THE ENCRYPTION FAULT LINE

The year 2026 has marked a watershed in the tension between digital privacy and state surveillance in India. In May 2026, Meta Platforms, Inc. discontinued end-to-end encryption (E2EE) for Instagram Direct Messages, rendering message content technically accessible to the company and, by extension, to governmental authorities pursuant to lawful orders.<sup>2</sup> This development coincides with the Indian government's sustained enforcement of the "first originator" traceability mandate under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in February 2026, requiring significant social media intermediaries to identify the original sender of viral messages upon judicial or executive order.<sup>3</sup>

The convergence exposes a fundamental fault line in India's digital governance. On one side stands the constitutional guarantee of privacy, elevated to the status of a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, encompassing secure communication and protection against arbitrary surveillance.<sup>4</sup> On the other hand stands the state's asserted imperative to combat deepfakes, child sexual abuse material (CSAM), and threats to public order objectives the government contends necessitate piercing encryption to identify originators of harmful content.<sup>5</sup>

This paper critically examines this conflict, evaluating the constitutional validity of the traceability mandate, the implications of Meta's encryption rollback for Indian users, and the broader ramifications for democratic discourse and the rule of law.

## TECHNICAL ARCHITECTURE AND META'S STRATEGIC PIVOT

End-to-end encryption is a communication protocol in which message content is encrypted on the sender's device and decrypted only on the recipient's device, with the service provider having no technical capability to access plaintext. The Signal Protocol, employed by WhatsApp since 2016, utilises the Double Ratchet Algorithm to generate ephemeral encryption keys for

---

<sup>2</sup> Meta Platforms, Inc., *End-to-End Encrypted Messaging on Instagram* (Mar. 2026). *Meta's Instagram Stopping Support for End-to-End Encrypted Messaging*, **The Hindu** (8<sup>th</sup> May, 2026).

<sup>3</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2), as amended by G.S.R. 120(E), dated 10.02.2026.

<sup>4</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, paras 121-122 (Chandrachud, J.).

<sup>5</sup> Ministry of Electronics and Information Technology, Government of India, Statement on Traceability Rules (26<sup>th</sup> May, 2021).

each message, ensuring forward secrecy.<sup>6</sup> Under this architecture, the service provider functions merely as a conduit for encrypted data packets, lacking cryptographic keys necessary for decryption.

The Indian government's first originator traceability mandate creates a technical paradox striking at E2EE's heart. Traceability requires associating each message with a persistent identifier linking it to the original sender. Under true E2EE, the platform cannot access message metadata enabling such association without fundamentally compromising the encryption protocol.<sup>7</sup>

On 8<sup>th</sup> May, 2026, Meta formally discontinued E2EE support for Instagram DMs, a feature available as an opt-in since December 2023 but never enabled by default. Meta attributed the decision to "very low adoption rates," concentrating encryption resources on WhatsApp, which maintains E2EE as a default feature.<sup>8</sup> The operational impact is substantial: post-8<sup>th</sup> May, 2026, Instagram DMs are stored on Meta's servers in decryptable form, rendering content accessible for content moderation, legal compliance, and potential commercial utilisation. Indian users, one of Instagram's largest global markets, are particularly affected, as the Digital Personal Data Protection Act, 2023 (DPDP Act) empowers the Central Government to direct data fiduciaries to disclose personal data for specified purposes.<sup>9</sup>

While Meta framed the rollback as product optimisation, the timing suggests strategic calculus against intensifying regulatory pressure across jurisdictions, including India's traceability mandate and the European Union's Digital Services Act obligations.<sup>10</sup>

## THE REGULATORY LANDSCAPE: FIRST ORIGINATOR TRACEABILITY

The *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, impose comprehensive obligations on social media intermediaries. Rule 4(2) mandates that significant social media intermediaries providing messaging services "shall enable the identification of the first originator of the information on its computer resource as

---

<sup>6</sup> M. Marlinspike & T. Perrin, "The Double Ratchet Algorithm," Signal Protocol Specification (20<sup>th</sup> November, 2016).

<sup>7</sup> *WhatsApp LLC v. Union of India*, W.P.(C) No. 2021/2021 (Delhi High Court), para 34 of the petition.

<sup>8</sup> Meta Official Statement, cited in Test book, "Instagram Stop End-to-End Encryption, Privacy vs Security" (21<sup>st</sup> July, 2026).

<sup>9</sup> Digital Personal Data Protection Act, 2023, Section 12(2).

<sup>10</sup> *TechCrunch*, "India's Supreme Court to WhatsApp: 'You cannot play with the right to privacy' (3<sup>rd</sup> February, 2026).

may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority.”

The February 2026 amendments introduced additional safeguards. The amended Rule 4(2) includes a proviso that the intermediary shall not be required to disclose message contents or other user information. However, the fundamental requirement that platforms must possess technical capability to identify originators remains intact and is fundamentally incompatible with true E2EE.

The Rule specifies that traceability orders may be issued for offences relating to sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, or incitement to offences, or in relation to rape, sexually explicit material, or CSAM punishable with imprisonment for not less than five years. A further proviso mandates that no order shall be passed where “other less intrusive means are effective in identifying the originator.”<sup>11</sup>

The DPDP Act, 2023, India’s first comprehensive data protection legislation, establishes principles of data minimisation and purpose limitation. However, Section 12(2) creates a significant carve-out, permitting the Central Government to exempt any agency from the Act’s provisions for reasons of sovereignty, integrity, security of the State, and public order. This exemption, combined with the absence of E2EE on Instagram, creates a surveillance-ready environment previously structurally precluded.

## CONSTITUTIONAL FOUNDATIONS: THE RIGHT TO PRIVACY

The Supreme Court’s landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, unanimously held that the right to privacy is a fundamental right under Article 21. The Court articulated a three-part test for evaluating state actions infringing privacy:

- (i) legality, requiring valid law;
- (ii) legitimate aim, requiring permissible state objective; and
- (iii) proportionality, requiring proportionate means and exhaustion of less restrictive

---

<sup>11</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2), proviso.

alternatives.

Justice Chandrachud emphasised that privacy encompasses informational self-determination, control over personal information dissemination, and secure communication without unwarranted interception. The judgment explicitly recognised that in the digital age, privacy assumes critical importance as individuals conduct personal, professional, and political lives through digital platforms.

The constitutional right to privacy encompasses secure and confidential communication foundational to democratic citizenship. Encrypted communication enables whistleblowers to expose corruption, journalists to protect sources, activists to organise dissent, and ordinary citizens to discuss sensitive matters without fear of surveillance.<sup>12</sup> The Supreme Court's subsequent jurisprudence reinforced this understanding. In *Shreya Singhal v. Union of India*, the Court invalidated Section 66A of the IT Act on grounds of vagueness and chilling effect, recognising surveillance's profound impact on freedom of expression.<sup>13</sup>

## THE PROPORTIONALITY ANALYSIS: APPLYING THE *PUTTASWAMY* TEST

### ➤ The Legality Prong

The traceability mandate derives legal basis from Rule 4(2) of the Intermediary Guidelines, 2021, notified under Section 87 of the IT Act, 2000. WhatsApp and Facebook have challenged the mandate on the ground that the parent legislation does not authorise the government to require intermediaries to break encryption or build traceability mechanisms. Section 69 empowers the Central Government to issue directions for interception, monitoring, or decryption of information. However, as argued in pending litigation, Section 69 does not authorise mandating platforms to fundamentally alter technical architecture to enable traceability.

### ➤ The Legitimate Aim Prong

The government's stated objectives of combating deepfakes, CSAM, terrorism, and threats to public order constitute legitimate aims.<sup>14</sup> The proliferation of synthetic media and encrypted

---

<sup>12</sup> *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632, para 26.

<sup>13</sup> *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

<sup>14</sup> Ministry of Electronics and Information Technology, Government of India, Statement on Traceability Rules (26<sup>th</sup> May, 2021).

platforms' use for criminal coordination present genuine security challenges. However, the legitimacy of the aim does not automatically validate the means employed.

### ➤ The Proportionality Prong

**Suitability:** Traceability is technically suitable for identifying originators of specific messages. However, its suitability is undermined by significant limitations. As WhatsApp argued, originator identification does not equate to authorship identification; a user forwarding content created by another becomes the “first originator” within India even if they did not create the content. Moreover, sophisticated actors can circumvent traceability through virtual private networks, disposable accounts, and cross-platform forwarding.

**Necessity:** The necessity requirement demands no less restrictive means be available. Alternative approaches including targeted infiltration of criminal networks, forensic device analysis, and international law enforcement cooperation may achieve similar objectives without mandating mass surveillance infrastructure.<sup>15</sup>

**Fair Balance:** The traceability mandate tilts the balance decisively toward state surveillance. The requirement applies to all users, not merely those suspected of criminal activity, and operates without temporal or geographic limitations. The absence of sunset clauses, broad offence categories triggering orders, and limited judicial oversight contribute to a structural imbalance unsustainable under proportionality principles.

## JUDICIAL SCRUTINY: THE WHATSAPP LITIGATION AND SUPREME COURT INTERVENTION

In May 2021, WhatsApp and Meta filed petitions before the Delhi High Court challenging Rule 4(2)'s constitutional validity. The petitions argue the traceability requirement violates fundamental rights to privacy and free speech, is *ultra vires* the IT Act, and fails the *Puttaswamy* proportionality test. The core argument is that traceability and E2EE are technically incompatible; to identify any message's first originator, WhatsApp would be compelled to maintain a permanent database associating each message with its sender, effectively breaking encryption architecture.

---

<sup>15</sup> Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (July 2018), p. 112.

The government's defence rests on proportionality grounds, arguing the requirement serves public interest in detecting and punishing originators of content leading to serious crimes. The 2026 amendments, including the proviso that no order shall pass where less intrusive means are effective, are presented as evidence of regulatory proportionality.

In February 2026, the Supreme Court delivered sharp rebukes to Meta during hearings on appeals against a ₹213.14 crore penalty imposed by the Competition Commission of India for abusive data-sharing practices. Chief Justice Surya Kant warned that the Court would not permit Meta to “play with the right to privacy” of millions of Indian users. The Court questioned how “a poor woman selling fruits on the street” could meaningfully consent to complex data-sharing terms in a market where WhatsApp operates as a practical monopoly.

This intervention is significant for the broader privacy-encryption debate. By characterising data-sharing as a “decent way of committing theft” and insisting that the Court would not allow Meta to share “a single piece of information” during the appeal, the Supreme Court signalled robust judicial commitment to privacy protection that may influence the traceability litigation's outcome.<sup>16</sup>

## COMPARATIVE PERSPECTIVES AND THE DEEPFAKE IMPERATIVE

The European Union's Digital Services Act 2022/2065 emphasises transparency and fundamental rights protection without mandating encryption breaking.<sup>17</sup> The European Court of Human Rights, in *Big Brother Watch v. United Kingdom*, found bulk interception regimes violated Article 8 due to insufficient safeguards against arbitrariness.<sup>18</sup> The United States maintains robust encryption protections through the First Amendment and CALEA, which explicitly excludes information services from mandatory surveillance capabilities.<sup>19</sup>

The government's emphasis on combating deepfakes responds to a genuine threat. Deepfakes have been weaponised for political disinformation, financial fraud, and non-consensual pornography. The 2026 amendments require platforms to label AI-generated content and verify user declarations regarding synthetic media. However, the deepfake imperative does not justify

---

<sup>16</sup> *Meta Platforms, Inc. v. Competition Commission of India*, Supreme Court of India, oral observations (3<sup>rd</sup> February, 2026).

<sup>17</sup> Digital Services Act (EU) 2022/2065, Articles 14, 27, and 34.

<sup>18</sup> *Big Brother Watch v. United Kingdom*, (2018) ECHR 345, paras 317-322.

<sup>19</sup> Communications Assistance for Law Enforcement Act, 1994, 47 U.S.C. § 1002(b)(2).

the traceability mandate's breadth. Categories triggering orders extend far beyond deepfakes to encompass "public order" and "friendly relations with foreign States" categories susceptible to expansive interpretation and political manipulation.

The "**chilling effect**" on lawful speech is pronounced. Journalists relying on confidential sources, activists organising dissent, and ordinary citizens discussing sensitive matters face heightened risks if communications are subject to traceability.<sup>20</sup>

## CRITICAL ANALYSIS AND RECOMMENDATIONS

The current framework exhibits structural defects. The technical impossibility argument that traceability and E2EE are fundamentally incompatible remains unaddressed by the government's insistence that platforms should "technologically innovate."<sup>21</sup> Meta's differential treatment of Instagram and WhatsApp illustrates jurisdictional arbitrage, leaving Instagram users without protections available to WhatsApp users.<sup>22</sup> The mandate disproportionately impacts vulnerable users, marginalised communities, dissidents, and journalists who rely most heavily on secure communication.<sup>23</sup> A proportionate framework requires:

**First**, prior judicial authorisation by designated High Court judges for traceability orders, with ex parte applications permitted only for imminent threats.<sup>24</sup>

**Second**, narrow offence categories excluding broad concepts like "public order," focusing on specific serious crimes.<sup>25</sup>

**Third**, strict temporal limitations with mandatory deletion upon investigation conclusion and maximum six-month retention for unused data, coupled with parliamentary reauthorisation sunset clauses.<sup>26</sup>

**Fourth**, transparency reports detailing traceability orders received, complied with, and

---

<sup>20</sup> *Romesh Thappar v. State of Madras*, AIR 1950 SC 211, para 9.

<sup>21</sup> *WhatsApp LLC v. Union of India*, W.P.(C) No. 2021/2021 (Delhi High Court), para 48.

<sup>22</sup> Meta Platforms, Inc., Help Centre Update (March 2026).

<sup>23</sup> Singh, Pranesh. "The First Originator Rule and Its Impact on Encrypted Messaging in India," *Stanford Journal of International Law*, Vol. 58 (2022), p. 98.

<sup>24</sup> *Big Brother Watch v. United Kingdom*, (2018) ECHR 345, paras 317-322.

<sup>25</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, para 181.

<sup>26</sup> *Ibid.*

challenged, with user notification upon investigation conclusion.<sup>27</sup>

**Fifth**, investment in alternative technologies: client-side scanning, AI-generated content watermarking, and international mutual legal assistance treaties that preserve encryption integrity while addressing security concerns.<sup>28</sup>

## CONCLUSION:

### PRESERVING PRIVACY IN AN AGE OF DIGITAL SURVEILLANCE

The conflict between Instagram's encryption rollback and India's traceability mandate crystallises a defining challenge: reconciling individual privacy with state security. The current regulatory framework fails this reconciliation. By mandating technical capabilities compromising encryption, the government has prioritised surveillance over constitutional safeguards, creating a regime the *Puttaswamy* proportionality test cannot sustain.

Meta's strategic withdrawal of Instagram encryption exacerbates this imbalance by removing privacy protections users previously possessed. The convergence of platform decisions and regulatory mandates creates a surveillance ecosystem wherein Indian users' private communications are rendered accessible to corporate data mining and state interception.<sup>29</sup>

The Supreme Court's robust intervention in the Meta-CCI litigation offers judicial resistance to this trajectory. By insisting privacy is non-negotiable, the Court signalled that constitutional principles retain force in the digital sphere. The pending WhatsApp litigation will test whether this commitment extends to striking down the traceability mandate itself.

The path forward requires not encryption's abandonment but its reinforcement, coupled with targeted, proportionate, and judicially supervised mechanisms addressing genuine security threats. A framework mandating encryption-breaking for all users to catch a criminal minority is neither proportionate nor constitutional. The right to privacy, as the Supreme Court held in *Puttaswamy*, is not a conditional privilege but a fundamental right the state may infringe only through lawful, necessary, and proportionate means. The traceability mandate, on rigorous analysis, fails to meet these exacting standards. In an age of escalating digital surveillance,

---

<sup>27</sup> Digital Services Act (EU) 2022/2065, Article 15.

<sup>28</sup> Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy* (July 2018), p. 115.

<sup>29</sup> Digital Personal Data Protection Act, 2023, Section 12(2).

preserving encrypted communication is not merely a technical preference but a constitutional imperative.

## BIBLIOGRAPHY

### A. CONSTITUTIONAL AND STATUTORY INSTRUMENTS

| No. | Citation                                                                                                                               |
|-----|----------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Constitution of India, 1950.                                                                                                           |
| 2.  | Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).                                                                       |
| 3.  | Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated 25.02.2021.           |
| 4.  | Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), dated 10.02.2026. |
| 5.  | Information Technology Act, 2000.                                                                                                      |

### B. CASE LAW

#### ➤ Supreme Court of India

| No. | Citation                                                                                            |
|-----|-----------------------------------------------------------------------------------------------------|
| 1.  | <i>Justice K.S. Puttaswamy (Retd.) v. Union of India</i> , (2017) 10 SCC 1.                         |
| 2.  | <i>Justice K.S. Puttaswamy (Retd.) v. Union of India</i> , (2019) 1 SCC 1 [ <i>Puttaswamy II</i> ]. |
| 3.  | <i>R. Rajagopal v. State of Tamil Nadu</i> , (1994) 6 SCC 632.                                      |
| 4.  | <i>Romesh Thappar v. State of Madras</i> , AIR 1950 SC 211.                                         |
| 5.  | <i>Shreya Singhal v. Union of India</i> , (2015) 5 SCC 1.                                           |

#### ➤ High Courts of India

| No. | Citation                                                                                                               |
|-----|------------------------------------------------------------------------------------------------------------------------|
| 1.  | <i>Facebook India Online Services Pvt. Ltd. v. Union of India</i> , W.P.(C) No. 2022/2021 (Delhi High Court, pending). |
| 2.  | <i>WhatsApp LLC v. Union of India</i> , W.P.(C) No. 2021/2021 (Delhi High Court, pending).                             |

#### ➤ Supreme Court of India (Pending / Ongoing)

| No. | Citation                                                                                                                 |
|-----|--------------------------------------------------------------------------------------------------------------------------|
| 1.  | <i>Meta Platforms, Inc. v. Competition Commission of India</i> , S.L.P.(C) No. [pending] (Supreme Court of India, 2026). |

#### ➤ International Tribunals

| No. | Citation |
|-----|----------|
|-----|----------|

|    |                                                                                                                                                                                                          |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | <i>Big Brother Watch and Others v. the United Kingdom</i> (often cited as <i>Big Brother Watch v. United Kingdom</i> ), Applications Nos. 58170/13, 62322/14 and 24960/15, ECtHR Grand Chamber judgment. |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### C. BOOKS AND MONOGRAPHS

| No. | Citation                                                                                                                |
|-----|-------------------------------------------------------------------------------------------------------------------------|
| 1.  | Solove, Daniel J. <i>Nothing to Hide: The False Tradeoff Between Privacy and Security</i> (Yale University Press 2011). |
| 2.  | Zuboff, Shoshana. <i>The Age of Surveillance Capitalism</i> (PublicAffairs 2019).                                       |

### D. JOURNAL ARTICLES AND SCHOLARLY PAPERS

| No. | Citation                                                                                                                                                                                                                          |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Bhandari, Vidushi & Sengupta, Anirban. "India's Intermediary Rules 2021: Impact on Encryption and Free Speech," <i>Journal of Intellectual Property, Information Technology and E-Commerce Law</i> , Vol. 12 (2021), pp. 456-478. |
| 2.  | Maheshwari, Namrata. "Traceability and End-to-End Encryption: A Technical and Legal Analysis," <i>Internet Policy Review</i> , Vol. 10, No. 3 (2021).                                                                             |
| 3.  | Singh, Pranesh. "The First Originator Rule and Its Impact on Encrypted Messaging in India," <i>Stanford Journal of International Law</i> , Vol. 58 (2022), pp. 89-112.                                                            |

### E. OFFICIAL REPORTS, COMMITTEE REPORTS AND POLICY DOCUMENTS

| No. | Citation                                                                                                                                                                                                                    |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Justice B.N. Srikrishna Committee, <i>A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians</i> (July 2018).                                                                                              |
| 2.  | Ministry of Electronics and Information Technology, Government of India, <i>The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026</i> (10 <sup>th</sup> February, 2026). |

### F. ONLINE RESOURCES, NEWS ARTICLES AND PERIODICALS

| No. | Citation                                                                                                                                                                                                                 |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | <i>Forbes India</i> , "Facebook, WhatsApp Sue Indian Government Over Traceability Requirement" (26 <sup>th</sup> May, 2021).                                                                                             |
| 2.  | Software Freedom Law Centre (SFLC.in), "What is the 'Originator or Traceability' Provision in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021?" (12 <sup>th</sup> April, 2021). |

|    |                                                                                                                                                      |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. | <i>TechCrunch</i> , “India’s Supreme Court to WhatsApp: ‘You cannot play with the right to privacy’” (3 <sup>rd</sup> February, 2026).               |
| 4. | Test book, “Instagram Stop End-to-End Encryption, Privacy vs Security” (21 <sup>st</sup> July, 2026).                                                |
| 5. | <i>The Hindu</i> , “Meta’s Instagram Stopping Support for End-to-End Encrypted Messaging” (8 <sup>th</sup> May, 2026).                               |
| 6. | <i>The Indian Express</i> , “Is WhatsApp Really Private? US Lawsuit Alleges Meta Has Access to Encrypted Messages” (31 <sup>st</sup> January, 2026). |