ADMISSIBILITY OF WHATSAPP CHATS AS ELECTRONIC EVIDENCE: BALANCING PRIVACY AND JUDICIAL AUTHENTICITY IN INDIA

Pragati Solanki*

ABSTRACT

This study examines the admissibility of WhatsApp chats as electronic evidence in Indian courts, focusing on the tension between privacy rights and legal accountability. With the right to privacy recognised as a fundamental right in K.S. Puttaswamy v. Union of India (2017), the use of WhatsApp chats as evidence raises concerns about infringing privacy and the right against self-incrimination. The research analyses the application of the Indian Evidence Act, 1872, particularly Section 65B, which mandates a certificate of authenticity for electronic evidence. It explores conflicting judicial interpretations, such as State v. Navjot Sandhu (2005) and Anvar P.V. v. P.K. Basheer (2014), which clarified that electronic evidence requires stricter authentication due to its susceptibility to tampering. The study also reviews High Court rulings and foreign jurisdictions, notably Canada, where encryption-based integrity tests enhance the reliability of electronic evidence. The findings highlight the need for a balanced framework in India to ensure the authenticity of WhatsApp chats while safeguarding privacy. Recommendations include adopting encryption systems akin to Canadian protocols to streamline Section 65B compliance, reducing procedural burdens while maintaining evidential integrity.

Keywords: Electronic Evidence, WhatsApp Chats, Section 65B, Evidence Act, Right to Privacy.

INTRODUCTION

The advent of social media platforms, particularly WhatsApp, has revolutionised communication, making it an integral part of personal, professional, and, at times, criminal interactions. With over two billion users globally, WhatsApp's end-to-end encryption and ease

*ASSISTANT PROFESSOR (LAW).

of use have made it a preferred medium for sharing sensitive information. However, this widespread use has also positioned WhatsApp chats as potential evidence in legal proceedings, ranging from criminal cases involving conspiracies to civil disputes concerning commercial transactions. The admissibility of these chats in Indian courts, governed by the Indian Evidence Act, 1872, raises complex legal and ethical questions, particularly in light of the Supreme Court's recognition of the right to privacy as a fundamental right in K.S. Puttaswamy v. Union of India (2017). This landmark judgment underscores the tension between using private communications as evidence and protecting individuals from unwarranted intrusions into their personal lives, including the right against self-incrimination.

Under the Indian Evidence Act, Section 65B mandates a certificate of authenticity for electronic evidence, acknowledging the susceptibility of digital records to tampering. However, judicial interpretations have varied, with cases like State v. Navjot Sandhu (2005) initially allowing secondary electronic evidence without strict certification, only to be overruled by Anvar P.V. v. P.K. Basheer (2014), which emphasised mandatory compliance with Section 65B. These inconsistencies reflect the broader challenge of balancing evidential reliability with procedural fairness. Moreover, the use of WhatsApp chats as legal notices or proof in bail applications, as seen in various High Court rulings, highlights evolving judicial perspectives on digital communication. This study aims to explore whether WhatsApp chats can serve as conclusive proof of guilt, the necessity of Section 65B certification, and the implications for privacy rights. By examining Indian jurisprudence alongside foreign frameworks, such as Canada's encryption-based integrity tests, it seeks to propose a robust mechanism for authenticating WhatsApp chats while safeguarding fundamental rights and ensuring judicial efficiency.

STATEMENT OF PROBLEM

The proliferation of social media platforms, particularly WhatsApp, has positioned them as critical tools for communication, but also as potential instruments for criminal activities, ranging from orchestrating riots to facilitating commercial offences like tax evasion. The admissibility of WhatsApp chats as electronic evidence in Indian courts presents a significant legal challenge, as it often conflicts with the fundamental right to privacy, affirmed in *K.S. Puttaswamy v. Union of India* (2017). This study critically analyses the judicial dilemma surrounding the use of WhatsApp chats as proof, given their susceptibility to manipulation in the digital age. Courts across India have grappled with whether such chats can reliably establish

an accused's guilt and whether their authenticity can be upheld without adhering to the mandatory certification requirement under Section 65B of the Indian Evidence Act, 1872 (not 1857, as erroneously stated). The analysis focuses on whether courts can bypass Section 65B's certification mandate when primary evidence of chats is available, and how judicial interpretations balance evidential value against privacy concerns and technological vulnerabilities.

OBJECTIVE AND SCOPE OF RESEARCH

This study aims to:

- Critically evaluate the rules and procedures established by the Supreme Court and High Courts regarding the admissibility of WhatsApp messages as electronic evidence.
- Analyse the admissibility of electronic evidence through the lens of foreign case law, particularly from jurisdictions like Canada.
- The scope encompasses a comprehensive examination of Indian legal frameworks and judicial precedents, with a comparative analysis of international practices to contextualise the evidential treatment of WhatsApp chats.

RESEARCH QUESTIONS

- Can WhatsApp chats serve as conclusive proof to establish an accused's guilt in Indian courts?
- Can courts waive the mandatory certificate requirement under Section 65B(4) of the Indian Evidence Act, 1872, for WhatsApp chats when primary evidence is presented?

RESEARCH METHODOLOGY

This study employs a qualitative approach, relying on secondary sources as commentaries on the Indian Evidence Act, 1872, and relevant Supreme Court and High Court judgments. Data is sourced from legal texts, case law databases, and reputable websites, accessed through library resources and online platforms, ensuring a robust analysis of judicial trends and statutory interpretations.

SCOPE AND LIMITATION OF THE STUDY

The study is confined to Indian laws and judicial decisions from the Supreme Court and various High Courts, focusing on the principles of evidence law governing electronic records. It provides an in-depth analysis of these principles but is limited to the Indian legal context, with selective references to foreign jurisdictions for comparative insights.

LITERATURE REVIEW

Desmond Israel, "Proving Facts in the Digital Age: The Law of Electronic Evidence in Ghana" (SSRN, 2024):[1] This paper broadly addresses the legal framework for electronic evidence in Ghana under the Evidence Act, 1975 and the Electronic Transactions Act, 2008. WhatsApp chats are discussed as an illustration of the authentication challenges that electronic evidence poses. The author situates WhatsApp messages within a larger category of electronic records whose admissibility depends on relevance, authenticity, and reliability. The article notes that courts must determine whether such chats have been altered, whether authorship can be attributed, and whether integrity of storage is preserved. WhatsApp chats are thus treated not as a novel form of evidence requiring new legal rules, but as data that falls within existing evidentiary categories, albeit raising heightened concerns of manipulation. The analysis highlights how Ghanaian courts draw upon comparative jurisprudence (UK, US, Canada, Nigeria) when considering issues of digital evidence like WhatsApp. The paper's approach is more structural than case-driven; WhatsApp chats serve as an example of the broader evidentiary dilemma, rather than a central focus. This reflects the paper's intention to discuss evidentiary law generally while underscoring the specific challenges that messaging platforms bring to authentication and chain of custody.

Benedicta Ingrid Deviriana et al., "Analysis of WhatsApp Chat Usage as Court Evidence" (Devotion Journal, 2025):[2] This article is explicitly centred on WhatsApp as evidence in Indonesian courts. It systematically examines how chats are categorised (personal chats, group chats, screenshots, backups, deleted messages) and situates them under the ITE Law (Law No. 11 of 2008) and PERMA No. 1 of 2024. The authors highlight three persistent challenges: (1) absence of technical standards for submission, (2) inconsistent judicial precedents, and (3)

[1] Desmond Israel, Proving Facts in the Digital Age: The Law of Electronic Evidence in Ghana (14 August 2025) SSRN https://ssrn.com/abstract=5392634

[2] Benedicta Ingrid Deviriana and others, 'Analysis of Whatsapp Chat Usage as Court Evidence' (2025) 6(6) Devotion Journal of Community Service 574 https://doi.org/10.59188/devotion.v6i6.25492

manipulation risks. WhatsApp chats, according to the study, can serve as "letter evidence," "clue evidence," or stand as independent proof if complete with metadata and obtained legally. The analysis of the South Jakarta Religious Court divorce case illustrates judicial willingness to recognise WhatsApp chats as valid evidence under the ITE Law, provided authenticity and relevance are proven. Unlike the Ghana-focused paper, this study delves into the evidentiary weight of WhatsApp chats themselves, pointing to judges' difficulty in assessing screenshots due to the ease of alteration. It also insists on stricter verification procedures, forensic tools, and standardisation of practice. The analytical stance is both legal and technical, acknowledging the evidentiary potential of WhatsApp but stressing the urgent need for reform to ensure evidentiary integrity.

Werner Uys & Kobus Joubert, "Forensic Inquiries: Evidencing the Reliability and Admissibility of Digital Communication" (SSRN/OIDA Journal, 2022):[3] This paper, situated in the South African legal context, evaluates how digital communications—including WhatsApp are treated under the Electronic Communications and Transactions Act, 2002 and the Cybercrimes Act, 2020. WhatsApp is mentioned alongside SMS and emails as part of data messages admissible as evidence. The discussion emphasises forensic challenges, such as authorship verification, chain of custody, and metadata extraction. WhatsApp chats are analysed under the same framework as SMS messages: the issue is proving that the sender is indeed the owner of the device, especially when multiple people may access a phone. Techniques like stylometry (linguistic analysis), N-Gram, and probabilistic evaluation are suggested for authorship determination. While WhatsApp is not the exclusive focus, it is presented as a paradigmatic example of social messaging evidence where authentication is complex. The paper is less concerned with judicial precedents than with forensic methodology—how investigators and analysts should collect, preserve, and present WhatsApp chats to meet admissibility standards. It highlights the danger of assuming that digital evidence is inherently reliable, urging courts and practitioners to rigorously test the integrity of WhatsApp records before giving them probative weight.

Across the three papers, WhatsApp chats are consistently framed as a challenge of authenticity and reliability rather than dismissed as inadmissible. The Ghanaian study uses WhatsApp as an example of the broader doctrinal issues with electronic evidence; the Indonesian study

[3] Werner Uys and Kobus Joubert, 'Forensic Inquiries: Evidencing the Reliability and Admissibility of Digital Communication' (2015) OIDA International Journal of Sustainable Development (Ontario International Development Agency, Canada) http://www.ssrn.com/link/OIDA-Intl-Journal-Sustainable-Dev.html

places WhatsApp chats at the core of its inquiry, mapping legal gaps and advocating reforms; and the South African study positions WhatsApp within forensic methodologies, highlighting techniques for establishing authorship and chain of custody. Collectively, the literature shows convergence on one point: WhatsApp chats are admissible in principle but fragile in practice, requiring robust standards of verification, judicial consistency, and forensic expertise to ensure their evidentiary value.

ELECTRONIC EVIDENCE AS SECONDARY EVIDENCE UNDER THE INDIAN EVIDENCE ACT

Under Sections 61–90A of the Indian Evidence Act, 1872,[4] documents in criminal and civil proceedings are admitted as primary or secondary evidence. Section 65[5] delineates conditions for secondary evidence admissibility, imposing stricter criteria compared to primary evidence, as it requires demonstrating the unavailability of primary evidence. Section 3[6] of the Act broadly defines evidence to include electronic records, while Section 2(1)(t) of the Information Technology Act, 2000,[7] classifies electronic evidence as data stored or transmitted in electronic form. Given the heightened risk of tampering with electronic records, Sections 65A and 65B prescribe specific authentication requirements, including a mandatory certificate under Section 65B(4). In State v. Navjot Sandhu (2005),[8] the Supreme Court controversially permitted secondary electronic evidence without certification, conflating it with physical documents under Sections 63 and 65.

This ruling overlooked the technological vulnerabilities of digital evidence. However, in Anvar P.V. v. P.K. Basheer (2014),[9] a three-judge bench, led by Chief Justice Lodha, overruled Navjot Sandhu, emphasising that electronic evidence constitutes a special category requiring compliance with Section 65B's four conditions to ensure authenticity. This decision invoked the principle of *generalia specialibus non derogant*, highlighting the distinct treatment of electronic records due to their susceptibility to manipulation.

[4] Indian Evidence Act 1872, ss 61–90A
[5] Indian Evidence Act 1872, s 65
[6] Indian Evidence Act 1872, s 3
[7] Information Technology Act 2000, s 2(1)(t)
[8] State v Navjot Sandhu (2005) 11 SCC 600
[9] Anvar P.V. v P.K. Basheer AIR 2015 SC 180

However, In Rakesh Kumar Singla v. Union of India (2020),[10] the Punjab and Haryana High Court relied on WhatsApp messages presented by the Narcotic Control Bureau to establish the accused's involvement in contraband transactions. However, the absence of a Section 65B certificate undermined their admissibility.[11] Citing Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020),[12] the court affirmed that WhatsApp messages require certification to be admissible, reflecting a cautious judicial approach to their evidential weight in bail proceedings.

WHATSAPP MESSAGES AS EVIDENCE AND MODE OF SERVICE: JUDICIAL TRENDS AND CHALLENGES

The Gujarat High Court, in a bail application, admitted WhatsApp messages circulated by the accused, rejecting tampering claims and imposing conditions to prevent further dissemination. Conversely, in National Lawyers Campaign for Judicial Transparency and Reforms v. Union of India (2017),[13] the Delhi High Court ruled that unverified WhatsApp posts lack authenticity to justify an FIR, emphasising the need for credible evidence. The Bombay High Court, in SBI Cards & Payment Services Pvt Ltd. v. Rohidas Yadav (2015),[14] erroneously held WhatsApp messages admissible under Section 65 of the Indian Evidence Act, 1872, contradicting the Supreme Court's mandate in Anvar P.V. v. P.K. Basheer (2014) for compliance with Sections 59 and 65A.

The Bombay High Court accepted the "blue tick" as proof of notice receipt but overlooked authenticity concerns. The Supreme Court Registrar's 2022 order clarified that WhatsApp is not a valid mode of service under Supreme Court Rules, despite High Courts' flexibility during the COVID-19 lockdown, as seen in In Re: Cognisance for Extension of Limitation (2020).[15] The Supreme Court's cautious approach in A2Z Infraservices Ltd. v. Quippo Infrastructure Ltd. (2021)[16] further underscores the unreliability of WhatsApp chats without Section 65B certification, citing their susceptibility to manipulation. This judicial inconsistency highlights

[10] Rakesh Kumar Singla v Union of India CRM-M No 23220 of 2020 (Punjab-Haryana HC, 14 January 2021)
[11] Aditya Mehta, Arjun Sreenivas & Swagata Ghosh, 'Section 65B of the Indian Evidence Act, 1872: Requirements for Admissibility of Electronic Evidence Revisited by the Supreme Court' (2020) https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/
[12] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal AIR 2020 SC 4908
[13] National Lawyers Campaign for Judicial Transparency and Reforms & Ors v Union of India & Ors W.P.(C) 4447/2017 (Delhi HC, 22 May 2017)
[14] SBI Cards & Payment Services Pvt Ltd. v. Rohidas Yadav 2018 SCC Online BOM 1262
[15] In Re Cognizance for Extension of Limitation (2021) ibclaw.in 266 SC
[16] Quippo Infrastructure Ltd vs A2Z Infraservices Ltd & Anr AIR 2021 CALCUTTA 180

a tension between adapting to digital evidence and ensuring its integrity, aligning with international practices like Canada's encryption-based integrity tests, which offer a model for enhancing reliability while addressing privacy and procedural concerns.

COMPREHENSIVE ANALYSIS OF AUTHENTICATION STANDARDS AND CONSTITUTIONAL RIGHTS

Contemporary Challenges in Admissibility: The landscape of digital evidence admissibility in India has become increasingly complex due to rapid technological evolution and divergent judicial interpretations. WhatsApp messages, in particular, exemplify the tension between modern communication practices and established evidentiary rules. While High Courts have occasionally adopted a more pragmatic approach, allowing consideration of digital records under specific conditions, the Supreme Court has consistently emphasised procedural rigour, expressing scepticism about the reliability of such evidence. The Court has noted that "anything can be created and deleted on social media these days," highlighting the inherent vulnerability of digital communications to manipulation.[17]

The jurisprudence from 2024-2025 further underscores this cautious approach. The Delhi High Court, in July 2024, reaffirmed that WhatsApp conversations are inadmissible without certification under Section 65B of the Indian Evidence Act.[18] This ruling reflects the judiciary's insistence that authenticity must be demonstrable through formal verification processes. The Supreme Court's decision in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)[19] has become a seminal authority, mandating strict certification and creating a uniform standard for electronic evidence admissibility. This trend demonstrates a clear prioritisation of procedural safeguards over expediency, signalling judicial awareness of the risks associated with unverified digital communications. However, these developments also reveal tensions. On one hand, courts recognise the utility of digital communications in modern litigation; on the other, the absence of standardised forensic protocols across jurisdictions creates inconsistency.

[17] Aditya Mehta, Arjun Sreenivas & Swagata Ghosh, 'Section 65B of the Indian Evidence Act, 1872: Requirements for Admissibility of Electronic Evidence Revisited by the Supreme Court' (2020) https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/

[18] SCC Online, 'Delhi High Court Rules WhatsApp Chats Inadmissible Evidence Without Proper Certification; Rejects Dell International Services' Delay Condonation Appeal' (6 July 2024) https://www.scconline.com/blog/post/2024/07/06/delhi-high-court-whatsapp-chats-inadmissible-evidence-without-proper-certification-rejects-dell-international-services-delay-condonation/

[19] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal AIR 2020 SUPREME COURT 4908

The divergence in High Court rulings indicates a need for more comprehensive legislative guidance to harmonise evidentiary standards and avoid fragmented judicial interpretations.

Privacy Rights and Legislative Framework: The use of WhatsApp messages as evidence raises profound constitutional concerns, particularly regarding the right to privacy under Article 21. The Supreme Court, in K.S. Puttaswamy v. Union of India (2017),[20] recognized privacy as a fundamental right, thereby imposing limitations on the state's ability to access personal communications without consent or due process. Extraction of private conversations through secondary means, including printouts or third-party devices, may constitute an infringement of this right. The legal challenge arises from balancing investigative necessity against individual privacy, particularly in scenarios where evidence is sought from devices not directly controlled by law enforcement.

The Digital Personal Data Protection Act (DPDP), 2023,[21] provides a statutory framework to regulate personal data processing, including messages exchanged on platforms like WhatsApp. Section 17 permits government access to encrypted messages under narrowly defined circumstances, such as national security, law enforcement, and public order. Despite these provisions, the practical implementation of lawful access remains unsettled, creating ambiguity about the precise boundaries of permissible interception. The DPDP Rules 2025 further strengthen protection mechanisms by imposing breach notification obligations and defining enhanced fiduciary responsibilities, signalling a gradual institutionalisation of data governance principles. International comparative standards provide instructive benchmarks.

In the United States, Fourth Amendment protections demand judicial warrants for digital searches, while the Federal Rules of Evidence outline rigorous authentication protocols, ensuring due process and safeguarding privacy.[22] Similarly, Canadian jurisprudence integrates systematic integrity testing within its Electronic Transactions Act, requiring evidence of system integrity, operational reliability, and an unbroken chain of custody.[23] India's evolving framework could benefit from adopting similar procedural rigour and technical standards, which would mitigate the risks of both wrongful prosecution and unauthorised surveillance.

[20] K.S. Puttaswamy v Union of India (2017) 10 SCC 1
[21] Digital Personal Data Protection Act 2023, No. 22 of 2023, Gazette of India (11 August 2023) https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[22] F Sankare, The Use of Digital Evidence in the US Criminal Justice System and the Fourth Amendment: Identifying and Revealing the Perceptions of Privacy, Data, and Security in America (Doctoral dissertation, Marymount University, 2023)
[23] S Coughlan, 'Canada' in Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010)

The mutable nature of digital communications constitutes the central challenge for judicial reliance on such evidence. WhatsApp messages can be altered, deleted, or fabricated with relative ease, undermining evidentiary credibility. Consequently, courts increasingly demand robust authentication methods that extend beyond traditional documentary proof. The Bharatiya Sakshya Adhiniyam (2023) introduces dual certification under Section 63, requiring attestation by both the party producing the evidence and an expert, thereby exceeding the procedural stringency previously mandated under Section 65B of the Evidence Act.

Forensic verification now necessitates multi-layered procedures, encompassing: Metadata Authentication, scrutiny of timestamps, sender and receiver identifiers, and transmission logs to detect potential tampering. Meticulous documentation tracing evidence handling from extraction through court presentation, ensuring integrity. In addition, Encryption analysis could also be considered via a technical assessment of WhatsApp's end-to-end encryption to identify vulnerabilities or unauthorised access.[24]

Technological innovations offer potential solutions. Blockchain-based authentication systems can create immutable, cryptographically verifiable records of digital communications, while zero-knowledge proofs preserve privacy by validating authenticity without exposing content. Artificial intelligence (AI) can augment forensic analysis, detecting altered timestamps, fabricated metadata, and other subtle manipulations.[25] However, reliance on such technologies raises additional questions: the opacity of AI algorithms, the judiciary's technical capacity to assess complex digital evidence, and the potential risk of over-dependence on automated verification. These considerations highlight the necessity for courts to combine technological tools with rigorous procedural safeguards.

TOWARDS A BALANCED FRAMEWORK

A coherent legal framework must reconcile investigative needs with constitutional privacy rights. Legislative reforms should focus on:

- **Comprehensive Digital Evidence Legislation:** Codifying procedures for the collection, authentication, and admissibility of electronic records, providing clear guidance to courts and law enforcement.

[24] M.S.M Alatawi, On the Security of End-to-End Encrypted Messaging and Calling Applications (Doctoral dissertation, 2024)
[25] M Nayak, 'AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection' (2024) 20(1s) J Electrical Systems 211

- **Judicial Capacity Enhancement:** Establishing specialised digital evidence benches or technical advisory panels to evaluate complex electronic evidence with appropriate expertise.
- **Standardised Forensic Protocols:** Creating national-level protocols for evidence collection, storage, and verification to ensure consistency and reliability.

Privacy protection measures are equally critical. Access to private digital communications must be strictly regulated, generally requiring judicial warrants, with emergency exceptions narrowly defined. Data minimisation principles should limit evidence collection to information directly relevant to ongoing investigations. Law enforcement agencies should operate under transparency obligations, disclosing data access procedures and providing accountability reports to ensure procedural compliance.

International comparative models provide valuable guidance. The Canadian approach to systematic integrity testing, coupled with American constitutional protections, illustrates how technical standards and privacy safeguards can coexist without undermining investigative efficacy. India's regulatory framework could integrate similar measures and develop technical benchmarks, while retaining strong judicial oversight to prevent abuse.

CHALLENGES RELATING TO THE AUTHENTICITY OF WHATSAPP MESSAGES AS EVIDENCE

The authentication of WhatsApp messages as evidence presents one of the most complex challenges in contemporary digital jurisprudence. Unlike traditional paper records, WhatsApp messages are outputs of computerised systems that can be easily altered, deleted, or fabricated. Their inherent mutability undermines the fundamental requirement of authenticity, exposing judicial proceedings to the risk of manipulation.[26] Metadata, including timestamps, sender identifiers, and device information, can be modified without leaving discernible traces, while the message content itself can be falsified. This technological malleability raises serious concerns about the reliability of evidence, as litigants could exploit digital vulnerabilities to fabricate evidence or misattribute liability. The courts must therefore navigate a dual challenge:

[26] K.F Mefolere, 'WhatsApp and Information Sharing: Prospect and Challenges' (2016) 4(1) International Journal of Social Science and Humanities Research 615

validating the integrity of digital communications while safeguarding procedural fairness in litigation.[27]

Judicial caution in India reflects the gravity of these challenges. The Supreme Court has repeatedly emphasised the necessity of certification under Section 65B of the Indian Evidence Act. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020),[28] the Court overruled earlier precedents and held that electronic records, including WhatsApp messages, are inadmissible unless accompanied by a certificate confirming authenticity and integrity. This requirement creates a procedural safeguard but also introduces practical obstacles. Obtaining Section 65B certificates from service providers often proves cumbersome, particularly when messages are stored on international servers or require specialised technical validation. Delays in certification can impede litigation timelines, burden judicial resources, and create inequities where one party cannot access the necessary documentation.

Beyond procedural requirements, these challenges intersect with privacy rights. Extracting messages from devices without consent raises constitutional concerns under Article 21, particularly after the Supreme Court affirms privacy as a fundamental right in K.S. Puttaswamy v. Union of India (2017). Reliance on secondary sources, such as printouts or screenshots, further complicates the matter, as such evidence may not reflect the original message environment and could be susceptible to manipulation. Consequently, courts are compelled to balance the dual imperatives of investigative utility and protection of individual privacy, highlighting the tension between judicial prudence and the practical realities of modern digital communication.

TECHNOLOGICAL AND COMPARATIVE INSIGHTS ON AUTHENTICATION

To address these challenges, technological solutions and comparative legal frameworks provide critical guidance. Digital forensics now employs multi-layered approaches to authenticate electronic records. Metadata analysis helps detect inconsistencies in timestamps or device identifiers, while detailed chain-of-custody documentation ensures accountability in evidence handling from extraction through presentation in court.[29] Cryptographic verification,

[27] C Morris, R.E Scott and M Mars, 'WhatsApp in Clinical Practice - The Challenges of Record Keeping and Storage: A Scoping Review' (2021) 18(24) International Journal of Environmental Research and Public Health 13426

[28] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal AIR 2020 Supreme Court 4908

[29] S Barbosa and S Milan, 'Do Not Harm in Private Chat Apps: Ethical Issues for Research on and with WhatsApp' (2019) 14(1) Westminster Papers in Communication and Culture 49

including hashing functions, allows courts to detect even minor alterations in message content, creating an additional layer of reliability. Artificial intelligence is emerging as a transformative tool for detecting digital manipulation. Advanced machine-learning models can analyse linguistic patterns, metadata inconsistencies, and potential deepfake indicators in WhatsApp messages. Studies conducted in 2024 have demonstrated up to 92% accuracy in identifying synthetic alterations, suggesting that AI can complement traditional forensic analysis and streamline judicial evaluation of electronic evidence.[30]

Blockchain-based solutions provide another innovative mechanism for enhancing authenticity. By recording message hashes in an immutable distributed ledger at the time of dispatch, courts can verify the integrity of messages without accessing the content itself. Zero-knowledge proofs further strengthen privacy by enabling authenticity verification while preventing exposure of sensitive communications.[31]

Comparative international standards offer additional insight. Canada's General Standards protocol establishes a structured framework for authenticating electronic records, requiring proof of authenticity, system integrity, and creation in the ordinary course of business or under a recognised hearsay exception. Alberta and Ontario evidence statutes further recognise encryption systems as reliability safeguards, demonstrating a multi-tiered approach that balances evidentiary admissibility with privacy rights. The U.S. Fourth Amendment similarly emphasises due process protections, mandating judicial warrants for digital searches and providing clear procedural rules for electronic evidence. Such frameworks offer instructive benchmarks for India, highlighting the importance of harmonising technical verification with constitutional safeguards.

POLICY RECOMMENDATIONS AND PATH FORWARD

Addressing the authenticity challenges of WhatsApp messages requires a comprehensive, multi-pronged policy framework. First, certification processes under Section 65B should be streamlined. Statutory timelines for service providers must be established, ensuring the timely

[30] M N I Khan and I Ahmed, 'A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence' (2025) 5(2) International Journal of Scientific Interdisciplinary Research 01-29.
[31] Vedik Bairwa and Awaneesh Kumar, ' Clause 247: A Trojan Horse for Digital Surveillance?' (Cell for Law & Technology, National Law Institute University, Bhopal, 2025) https://clt.nliu.ac.in/?p=1187

issuance of certificates, while courts should be empowered to appoint neutral digital custodians where providers fail to comply.

Second, uniform forensic standards are essential. National guidelines should govern collection, preservation, chain-of-custody documentation, and metadata verification. Judicial officers, forensic experts, and law enforcement personnel should be trained in emerging AI verification techniques, cryptographic validation, and blockchain-based timestamping to ensure technical competence and consistency.

Third, privacy safeguards must remain integral. Access to end-to-end encrypted messages should require judicial authorisation, except in narrowly defined emergencies. Data minimisation principles must limit collection to information strictly relevant to investigations, while transparency obligations for law enforcement agencies—including audit trails and regular reporting would enhance accountability and maintain public trust.

Finally, integration of technological innovation with legislative clarity and judicial oversight is critical. AI-driven manipulation detection, cryptographic hashing, and blockchain-based timestamping should be embedded within procedural protocols to create a robust evidentiary framework. At the same time, courts must retain oversight authority to interpret and evaluate complex digital evidence, ensuring that technological solutions complement rather than replace judicial scrutiny. Comparative lessons from Canada and the United States illustrate that structured authentication standards, coupled with constitutional protections, can create a balanced approach that ensures both evidentiary reliability and protection of fundamental rights.

CONCLUSION

The authenticity of WhatsApp messages as evidence embodies the intersection of law, technology, and privacy. The inherent mutability of digital communications, coupled with procedural complexities in certification and verification, underscores the necessity of rigorous forensic and technological safeguards. Judicial insistence on Section 65B certification reflects appropriate caution, yet practical challenges necessitate complementary mechanisms, including AI-assisted verification and blockchain-based authentication. A balanced framework for India must harmonise investigative efficacy with privacy protection. Streamlined certification, uniform forensic protocols, AI and cryptography-driven verification, and robust judicial oversight together provide a pathway for courts to rely confidently on WhatsApp

evidence while respecting constitutional rights. The evolution of India's digital evidence jurisprudence will ultimately depend on integrating technological advancement, legislative clarity, and judicial innovation, ensuring that digital communications can serve as reliable, admissible evidence without compromising procedural integrity or fundamental freedoms.