VOLUME 6 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

WHATSAPP CHATS AS EVIDENCE: DIGITAL SURVEILLANCE OR VIOLATION OF THE RIGHT AGAINST SELF-INCRIMINATION?

- Ananya Anwesha & Aditi Suhasinee[1]

Abstract

WhatsApp messages have become crucial evidence in Indian courts, raising significant legal, ethical, and constitutional issues. This article examines the balance between utilizing WhatsApp evidence for justice and safeguarding key rights, such as privacy (Article 21) and protection against self-incrimination (Article 20(3)). Indian law enforcement agencies have robust safeguards against forced disclosure, supported by WhatsApp's end-to-end encryption, which restricts access even to the company itself. While encryption protects against unauthorized surveillance, it complicates lawful investigations, sparking debates on access, backdoors, and metadata use.Voluntary disclosure of chats may ease evidence admissibility, but does not fully waive privacy rights; courts carefully weigh privacy against relevance. Metadata, though less intrusive, still requires strict legal procedures to protect privacy.AI-driven digital forensics aid in authenticating WhatsApp evidence by detecting manipulations like deepfakes; however, courts continue to require traditional certification and chain of custody to ensure reliability. Legal ethics demand that lawyers balance confidentiality, authenticity, and privacy concerns while representing clients. Special care is needed in cases involving minors, where privacy and child protection laws impose heightened safeguards. Blockchain technology offers promise for tamper-proof verification of WhatsApp evidence, though legal systems must adapt accordingly. Cross-border evidence access faces challenges from jurisdictional and privacy conflicts, requiring adherence to international treaties and respect for sovereignty. WhatsApp evidence strengthens the legal process only when used with constitutional safeguards, technological protections, judicial oversight, and ethical responsibility, preserving fundamental rights in India's evolving digital era.

[1] Students at KIIT School of Law

Keywords: WhatsApp Evidence, End-to-End Encryption, Right to Privacy, Digital Forensics, Cross-Border Data Access.

Introduction

In the digital era, a private WhatsApp message can cast the transformation of a casual note into evidence in court. As one observer puts it, a smartphone is not just a thing around which life unfolds; it is life in itself, with the imprint of social, economic, personal, and even intimate experiences upon it. The very omnipresence of these messaging platforms is the wrench in the UPA works: for government agencies, WhatsApp chats represent treasure chests of clues, but compelling disclosure puts surveillance mode in outright conflict with India's constitutional shield against self-incrimination. To many citizens, even the simplest emoji or message could suddenly take legal significance if authorities request access to their private chats.[2]

Indian laws do indeed provide for strong safeguards on privacy and silence. Article 20(3) of the Constitution states that "no person accused of any offence shall be compelled to be a witness against himself". The Supreme Court in Kathi Kalu Oghad and Selviwent so far as to find this precludes any sort of testimonial compulsion—unlocking a phone, handing over a passwordthat would divulge the accused's inner thoughts.[3] Similarly, Section 161(2) of CrPC prohibits forcing a witness to answer questions that would incriminate them.[4] The right to privacy, now part of Article 21, provides another facet to the debate: unauthorized access to personal WhatsApp chats without following the due process of law might breach the Constitutional guarantees of liberty and privacy.

Conversely, the scenario here is not simple to unravel. WhatsApp chats usually contain either admissions or "links in the chain of evidence". For example, police in Hyderabad stopped people to search their WhatsApp for drugs, and this has provoked contrary opinions that such practices violate Article 21 and Article 20(3).[5] Furthering the conundrum is the fact that

[2] https://www.barandbench.com/columns/whatsapp-chats-criminal-investigation-legal-analysis#:~:text=Today%2C%20smartphones%20are%20not%20merely,Adamou
[3] https://www.newsclick.in/legality-whatsApp-surveillance-india#:~:text=In%C2%A0Selvi%2C%20it%20was%20held%20that,3
[4] https://www.ijllr.com/post/section-180-bnss-echoes-of-section-161-crpc-with-a-constitutional-core#:~:text=identical%20language,accused%20or%20suspect%2C%20rather%20than
[5] https://www.thenewsminute.com/telangana/hyderabad-cops-are-illegally-checking-phones-whatsapp-citizens-part-drug-crackdown-

WhatsApp has end-to-end encryption, whereby even the company cannot extract users' messages. Forcing platforms to break this encryption would, some warn, stir "major constitutional issues" on etc. lines of the well-publicized Apple-versus-FBI row in the U.S.

The article deals with these tensions and more. We traverse across evidentiary rules (Section 65B of the Evidence Act) and more trend-based curriculum: voluntary disclosure of chats, metadata analysis, AI-assisted authentication, cross-border enforcement obstacles, and even some latest proposals like blockchain timestamping. In asking the question of whether WhatsApp evidence helps justice or works against the constitutional right to silence and right to privacy, we delve deeper into the layers of this unfolding conflict. Finally, the question emerges: Can law balance these contradictory aims, or will the latter be susceptible to violation?

Role of End-to-End Encryption in Protecting WhatsApp Chats from Unauthorized Surveillance

Imagine countless WhatsApp chats locked behind an unbreakable vault. End-to-end encryption assures just that: only the sender and receiver can hold the keys to decrypting a message.[67] Not even WhatsApp servers can peer into private conversations, let alone hackers and inept authorities. These agencies refer to it as "going dark" because even at legal intercepts, all they obtain are ciphertexts. Meaningful investigation, therefore, has to resort to other means such as seizing the device or exploiting vulnerabilities, or perhaps forging cooperation with the app developer. To sum it briefly, encryption places a cryptographic barrier that impedes the surveillance of communications.

This technical shield raises acute legal and policy questions. On one side, privacy is entrenched in Indian law: the Supreme Court, in the *K.S. Puttaswamy v. Union of India*, held privacy to be a fundamental right under Article 21 of the Constitution.[8] Encryption technologies give effect to that right by ensuring confidentiality in the absence of lawful authorization. On the other hand, the State cites the criminal law and security considerations:

156997#:~:text=Activists%20have%20slammed%20the%20move%2C,Part%20III%20of%20the%20Constitution

[6]https://carnegieendowment.org/research/2023/11/considering-indias-encryption-policy-dilemma?lang=en

[7]https://policyreview.info/articles/news/how-message-tracing-regulations-subvert-encryption/1642#:~:text=end%20encryption,available%20to%20law%20enforcement%20agencies

[8]https://www.jurist.org/commentary/2021/06/parashar-shekar-whatsapp-encryption-privacy/#:~:text=In%20Justice%20K,proportionality%20all%20weighed%20against%20it

Statutes such as the Telegraph Act, IT Act (for example, section 69 permitting interception orders), and the CrPC do require strict adherence to due process (judicial warrants) before any kind of snooping. Attempts to circumvent encryption outside legal channels would not be considered mere due-process violations of Article 21, but could amount to a civil wrong under tort-like causes of action for invasion of privacy (India is fast-tracking data-protection laws and civil remedies for unauthorized data breaches). Indeed, the Puttaswamy test holds that such intrusions must be lawful, necessary, and proportionate-the very standards that wide-ranging powers to decrypt are unlikely to satisfy.

The conflict is global and local. For example, law enforcement agencies across the globe might seek any measures, including "backdoors" or metadata mandates, to weaken encryption. The US FBI ironically requested Apple in 2016 to unlock a suspect's iPhone, in a standoff over encryption.[9] India, under the new IT Rules (2021), also requires traceability of message originators. WhatsApp contends that even tagging metadata is the insertion of a theoretical backdoor, thereby destroying privacy guarantees under E2E encryption.[10] This has led experts to warn that any kind of "exceptional access" can either weaken or outright compromise security. Backdoors inevitably introduce vulnerabilities that can be exploited by malicious actors or authoritarian regimes. The analysis says history has shown that once governments have been unable to resist building a capability to surveil their populations, that capability is guaranteed to be misused by the very governments or end up within hostile entities.[11] Even nations that have lobbied for exceptional access through a tech company have generally reversed their stance when it came to actually undermining encryption, with major companies refusing these requests, citing security and civil liberties.

Overall, E2E encryption is a robust defence against illegal monitoring. While law enforcement pressures the state to chip away at exceptions, constitutional safeguards, and tort law,it cautions against compromising the cryptographic shield of WhatsApp. Any backdoor or mandated weakening of encryption would undermine digital security, but also test core rights (Article 21's right to privacy and Article 19's free speech implications) without a thoroughly justified lawful basis. The debate continues to rage: do the security interests of the state

[9]https://carnegieendowment.org/research/2021/09/understanding-the-encryption-debate-in-india?lang=en
[10]https://www.indiatoday.in/technology/features/story/whatsapp-vs-indian-govt-on-it-rules-can-encryption-be-broken-who-is-right-who-is-wrong-1807649-2021-05-27
[11]https://policyreview.info/articles/news/how-message-tracing-regulations-subvert-encryption/1642#:~:text=Proponents%20of%20encryption%20point%20out,linked%20to%20the%20Chinese%20government

render encryption vulnerable to being compromised, or must the law maintain this bastion of privacy from all but the most meticulous judicially-monitored surveillance?

Voluntary Disclosure and Privacy: Consent Isn't a Free Pass.

Suppose a litigant mistakenly shares a WhatsApp exchange with the other party or the court. Has she forfeited all right to privacy? Not quite. The Supreme Court has always presumed that privacy is "implicit in the right to life and liberty" under Article 21 of the Constitution, the right to be let alone. Crucially, India does not embrace the US-style "third-party doctrine." In *District Registrar v. Canara Bank (2004)*[12]The Court ruled that even if a depositor "voluntarily" gave over bank papers to a third party, the privacy interest of the depositor continued. Analogously, a WhatsApp message shared by one party remains under the protection of Article 21; the circumstance that it so happens to be in someone else's hands does not invalidate confidentiality instantaneously.

That apart, privacy is not absolute.[13] Where a chat is directly material, courts balance its probative value. Evidence law is concerned with relevance, not with collection. As recently put by one high court, a chat is "admissible so long as it is relevant, irrespective of the fact how it is collected". Thus, in divorce cases, Section 122 of the Evidence Act specifically waives spousal privilege a husband can lead his wife's private messages in a suit between the two of them. Pioneer cases such as *R.M. Malkani v. Maharashtra (1973)* and *Puttaswamy v. Union (2017)* remind us that illegally or improperly obtained but material evidence can still be led, subject to balancing against privacy. Accordingly, where a party voluntarily leads chats, Article 20(3)'s protection against self-incrimination simply doesn't arise – the confession can be relied on in criminal and civil proceedings equally.[14]

Incriminating WhatsApp conversations have a significant influence on the outcome of criminal and civil proceedings. Plaintiffs can strong-arm defendants into settlement using screenshots, and defendants can reveal conversations to bar claims. India does not have a "privacy tort," but disclosure of sensitive information can result in breach of confidence or defamation actions. In criminal proceedings, voluntary disclosure is preferable. The Bharatiya

[12] Distt. Registrar & Collector, ... vs Canara Bank Etc, AIR 2005 SC 186

[13] https://www.legalbites.in/topics/articles/can-whatsapp-chats-be-used-as-evidence-in-matrimonial-disputes-1158839#:~:text=compelled%20to%20undergo%20medical%20examination,In%20cases%20of%20conflict%20between

[14] https://www.legalbites.in/topics/articles/can-whatsapp-chats-be-used-as-evidence-in-matrimonial-disputes-1158839#:~:text=The%20court%20drew%20heavily%20from,right%20to%20a%20fair%20trial

Nagarik SurakshyaSanhita, Section 33[15], requires reporting of serious offenses, with a penalty for default, and provides pardons for complete and truthful disclosure, preferring the sharing of evidence in return for leniency. Plea-bargaining legislation available (CrPC Sec. 265A) provides for a reduction of charges for cooperation. Defendants can therefore employ incriminating conversations to receive lighter punishment, and prosecutors can employ disclosure of messages to secure plea bargains.

Short answer: consent for release of a conversation certainly makes it more probable to be admitted as evidence, but it does not necessarily preclude underlying privacy rights created by statute.Courts will still look at the context, materiality, and probative weight of the tendered evidence. For one judge, production of a WhatsApp log is merely "mere inclusion in record"the burden remains for the fact-finder to determine its genuineness. Finally, while voluntary disclosure obviates some procedural concerns, concerned parties should not cavalierly ignore the constitutional protection of privacy.

Use of Metadata from WhatsApp Conversations as a Less Invasive Form of Digital Evidence

Imagine investigating crime not through the interception of private messages, but through monitoring a subject's online behaviour from WhatsApp call logs and connection history. For law enforcers, WhatsApp metadata, essentially records of who called whom and when, is powerful evidence. Since metadata is not encrypted and is legally accessible, agencies tap this online trail.[16] As a cybersecurity expert put it, "without metadata, no investigation would take place."[17] since call duration and time records reveal contact patterns and timelines, even when chat content is protected by end-to-end encryption.

In Indian law, WhatsApp call logs and corresponding connection information are electronic records. Call Detail Records (CDRs) are retained by phone companies that record call times, duration of calls, and cell tower location.CDRs can be obtained U/S 91 of the CrPC or telecom legislation and can be used as evidence if they are accompanied by the necessary

[15] https://iclg.com/practice-areas/business-crime-laws-and-regulations/india#:~:text=Yes%2C%20under%20Section%2033%20of,a%20Magistrate%20or%20police%20officer

[16] https://economictimes.indiatimes.com/wealth/tax/is-the-government-already-reading-your-whatsapp-chats-despite-the-governments-denial-heres-what-experts-are-saying/articleshow/119656223.cms?from=mdr

[17] https://www.medianama.com/2023/11/223-india-police-metadata-use-tracking-2/#:~:text=,facto%2C%20so%20they

Section 65B certificate.[18] In *Anvar P.V. v. P.K. Basheer*, the Supreme Court held that a Section 65B (4) certificate must be submitted to establish that computer-generated records are authentic.Practically, a certified WhatsApp log (with information linking a number to a person) can link a suspect to an event. For example, legal specialists note that a certified CDR with subscriber details unambiguously links phone numbers to call times and tower locations, indicating an individual is somewhere. Furthermore, digital forensics manuals note that metadata and timestamps "enableexpertsto investigate more precisely" by providing a "complete picture" of events.

Metadata is not entirely anonymous. India's Constitution guarantees privacy as an aspect of personal freedom (Art. 21)[19], so even call-detail data has to be gathered cautiously. Records of whom we call and when disclose individual routine and social acquaintances, and bulk collection is a significant privacy hazard. Indian law considers informational privacy as both a constitutional right and an issue of the judiciary, thus meaning that improper surveillance can have legal consequences.[20] Consequently, the gathering of WhatsApp metadata still requires a court or a strict legal process, adhering to the necessity and fairness standards. Ultimately, metadata is an effective investigatory tool but it has to adhere to Article 21's standards of being lawful and fair. WhatsApp call durations and timestamps, although disclosing less than chat messages are still material evidence, accepted under strict proof corroboration rules and constitutional privacy safeguards.

Implications of AI and Digital Forensics in Authenticating WhatsApp Evidence

Picture a courtroom where a WhatsApp screenshot determines the outcome of a case but what if that screenshot were a high-definition deepfake? In the cyber-age of today, litigants are increasingly seeking the services of AI-driven forensic software to determine if a chat has been deep faked or doctored. Digital sleuths rifle metadata and device artefacts for the telltale signs of manipulation mismatched timestamps, garbled EXIF data, or machine-learning

[18] https://www.lawweb.in/2024/06/how-to-prove-call-details-recordcdr-in.html#:~:text=,service%20provider%20to%20ensure%20authenticity

[19] https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-union-of-india-ii/#:~:text=Under%20the%20Constitution%20of%20India%2C,chapter%20II%20deals%20with%20enrollment

[20] https://clsnluo.com/2024/11/08/horizontal-application-of-privacy-rights-a-constiutional-tort-framework/#:~:text=Indian%20law%20recognises%20the%20right,leading%20to%20its%20dual%20recognition

markers to establish authenticity.[21] At FTI Consulting, experts cite cases "where individuals have used digital tools to manipulate screenshots of messages to advance their cases," observing that the "ability to authenticate or invalidate the authenticity" of the photographs is now "critical" to ascertaining facts. Likewise, AI-driven algorithms are being trained to identify unlikely patterns in a WhatsApp photograph lacking the customary iPhone camera signature or displaying an impossible timeline as probable "machine-generated." Such new forensic tools wed old-school analysis with deep learning: where a detective's hunch might have been enough in the past, only an algorithm can now determine whether a message stream is genuine or fabricated.[22]

Legal frameworks are racing to keep pace. The Constitution's assurances loom large. Article 21's assurance of a fair trial and informational privacy (according to *K.S. Puttaswamy v. Union of India*[23]) restricts excessive data trawling, while Article 19 safeguards speech (with defamation, public order, etc., as exceptions)[24]. Parliament's new code of evidence, the Bharatiya Sakshya Adhiniyam, paradoxically considers electronic records to be primary evidence but continues to require strict certification for their admissibility.[25] Under the Bharatiya Nyaya Sanhita, creating a false "electronic record" is already a criminal offense (forgery)[26], and producing it as evidence has severe penalties[27]. Courts have also raised flags: in *Arjun Panditrao v. Kailash*, the Supreme Court reaffirmed that in the absence of the required Section 65B certificate, digital records have "no evidentiary value"[28]. So, while AI tools vow to authenticate WhatsApp chats, the judiciary continues to require ancient proof chain of custody, expert testimony, and statutory formalities to accept them.

[21] https://www.fticonsulting.com/insights/articles/deepfakes-evidence-tampering-digital-forensics#:~:text=Similar%20approaches%20can%20be%20used,experts%20are%20monitoring%20this%20space

[22] https://www.webasha.com/blog/ai-in-digital-forensics-a-revolutionary-breakthrough-or-a-risky-gamble#:~:text=Artificial%20Intelligence%20,legal%20considerations%20and%20best%20practices

[23] https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges#:~:text=Court%2C%20defamation%20and%20incitement%20to,The%20Court%20observed

[24] https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges#:~:text=Article%2019,is%20an%20important%20facet%20of

[25] https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023#:~:text=includes%20electronic%20records%20in%20the,definition%20of%20documents

[26] https://www.advocatekhoj.com/library/bareacts/bharatiyanyayasanhita/336.php?Title=Bharatiya%20Nyaya%20Sanhita,%202023&STitle=Forgery#:~:text=,may%20be%20committed%2C%20commits%20forgery

[27] https://devgan.in/bns/chapter_14.php#:~:text=Whoever%20causes%20any%20circumstance%20to,is%20said%20%E2%80%9Cto%20fabricate%20false

[28] https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2/#:~:text=Three%20Justices%20of%20the%20Supreme,be%20produced%20before%20the%20Court

This tension raises the issue: machine-created evidence can be convincing, but it's not always perfect, and AI detection tools themselves are susceptible to bias and error, and their "black box" nature creates legal challenges. Legal acceptance of an algorithmic conclusion: Will a judge accept an algorithmic conclusion without knowing how it was trained? Courts struggle worldwide with the admissibility of AI-driven forensics: a survey last year comments on how AI facilitates "rapid evidence analysis," but with accompanying threats of "deepfake forgery" and "legal admissibility challenges." In India, until case law and statute evolve, litigants will have to detail the forensic process how an AI flagged a message as a forgery, what data trails it followed as expert evidence. Meanwhile, tort law awaits the blame: a deepfake WhatsApp conversation that defames someone might lead to a defamation liability (civil or criminal).

In general, AI and digital forensics are transforming WhatsApp evidence. They have the thrilling power to expose fakes, but they will be balanced by courts against due-process protections. Technology cannot replace judicial review, as academics have cautioned. For now, verifying a disputed chat will continue to be a hybrid process where the trustworthiness of algorithms will have to clear constitutional and evidentiary thresholds before they gain the judge's confidence.[29]

The Ethical Dilemma for Lawyers in Handling WhatsApp Evidence

The rise of WhatsApp as a dominant communication platform presents new ethical challenges for lawyers, who must balance their duties to verify authenticity and maintain confidentiality while safeguarding justice and privacy. Under the Bar Council of India Rules and similar international standards, lawyers must rigorously authenticate WhatsApp evidence. This includes ensuring compliance with Section 65B of the Indian Evidence Act, obtaining proper certification, verifying metadata, and maintaining an unbroken chain of custody. Failure to do so risks evidentiary exclusion and potential professional misconduct.[30] Landmark rulings like *Anvar P.V. v. P.K. Basheer* emphasize the court's insistence on strict compliance to uphold credibility.[31]

[29] https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2/#:~:text=Three%20Justices%20of%20the%20Supreme,be%20produced%20before%20the%20Court

[30] https://www.linkedin.com/pulse/want-produce-whatsapp-messages-evidence-court-read-know-hemant-kelkar-wssuf

[31] https://bhattandjoshiassociates.com/are-whatsapp-messages-admissible-in-court-of-law/

Confidentiality is paramount.Private WhatsApp messages are within an advocate's duty to preserve client confidentiality.[32] Mishandling of information can violate privacy rights under *Justice K.S. Puttaswamy (Retd.) v. Union of India*, and the advocate can be taken to task through disciplinary proceedings or tort action for invasion of privacy.[33][34]A difficulty arises when evidence involves third-party privacy or is not entirely consensual. Courts, including the Madhya Pradesh High Court, focus on fairness, necessitating scrutiny of such evidence to avoid privacy invasion. Counsel must disclose how digital evidence was obtained, sometimes through the use of in-camera hearings or redactions to avoid irrelevant private information.[35]

Typical common law cases like *R v. Coughlan and Carpenter v. United States* also indicate lawyers' roles in authenticating digital evidence without invasive searches. Data protection laws like GDPR and India's Digital Personal Data Protection Act, 2023, impose even more requirements on consent and lawful processing.[36]

The ethical balancing act in handlingWhatsApp evidence reflects broader digital-age tensions: advocating zealously for clients while safeguarding fundamental privacy rights. To uphold digital due process and constitutional tort protections, legal practice and policy must adapt, equipping lawyers to responsibly navigate this complex landscape.

Impact of WhatsApp Evidence on Juvenile Justice and Child Protection Cases

The use of WhatsApp evidence in juvenile justice and child protection matters raises critical legal and ethical concerns. Courts must carefully balance protecting minors' rights against the necessity to investigate potential wrongdoing, given the sensitive nature of children’s private communications.[37]

The Indian Constitution guarantees privacy under Article 21, especially for children since they are vulnerable. Article 39(e) mandates the state to protect children from exploitation. The Juvenile Justice (Care and Protection of Children) Act, 2015, ensures child-sensitive procedural procedures in the best interest of the child. Electronic evidence, like WhatsApp

[32] https://www.livelaw.in/articles/whatsapp-chats-reliable-source-of-evidence-indian-law-290734
[33] https://law.asia/indias-data-protection-law-children/
[34] https://www.varindia.com/news/data-protection-rules-to-safeguard-children-s-online-presence
[35] https://www.telegraph.co.uk/news/2017/12/28/parents-should-check-childrens-whatsapp-chats-spanish-court/
[36] https://www.scconline.com/blog/post/2020/05/23/legal-framework-for-privacy-of-minors/
[37] https://www.indiatoday.in/law/story/whatsapp-chats-section65-electronic-evidence-act-supreme-court-aryan-khan-case-1870234-2021-10-27

messages, is regulated under Section 65B of the Indian Evidence Act, requiring certified digital evidence. The BNSS further secures protection for evidentiary integrity.[38]The Digital Personal Data Protection Act, 2023, has stricter provisions for processing children's data, requiring parental consent and banning harmful uses of data.

Indian courts emphasize proportionality and protection in admitting WhatsApp evidence against children. Indian courts have applied WhatsApp-shared child pornography against the principles of authentication under Section 65B in cases such as *Just Rights for Children Alliance v. S. Harish*.[39] Indian courts demand robust evidence of relevance and restrict the gathering of evidence in the interest of privacy. Globally, measures such as the EU's General Data Protection Regulation align with India's protective measures. Court decisions, such as that of a Spanish court in permitting parental monitoring of a child's WhatsApp for welfare, are an international validation of proportionality between child protection and privacy.[40]

Children's privacy in online communication needs diligent investigative practices. Evidence gathering should be confined to that which is necessary for the child's well-being or legal purposes to meet data protection legislation and admissible electronic evidence requirements, while conducting in-camera hearings and censoring extraneous private information to minimize trauma.[41][42]The authorities should also eschew intrusive searches that unnecessarily violate children's privacy. This conforms to constitutional morality and legal guidelines, where WhatsApp evidence involving children should be considered only in compelling situations, with robust due process and privacy safeguards.

The Future of Digital Evidence: Blockchain and WhatsApp Verification Mechanisms

As digital communication increasingly forms the backbone of modern evidence, the need for robust mechanisms to verify the authenticity and integrity of electronic records, such as

[38]https://www.mondaq.com/india/data-protection/1276834/privacy-week-series-status-of-childrens-data-under-the-indian-privacy-regime
[39]https://www.medianama.com/2022/11/223-data-protection-bill-2022-protection-of-childrens-data/
[40]https://www.livelaw.in/high-court/delhi-high-court/whatsapp-conversations-cant-be-read-as-evidence-without-mandatory-certificate-under-evidence-act-delhi-high-court-262312
[41]https://jgu.edu.in/child-rights-clinic/bar-on-disclosing-minor-victims-identity-in-media-applies-to-whatsapp-groups-also-jharkhand-high-court/
[42]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/

WhatsApp messages, has become paramount.[43]Blockchain technology, with its unique features of decentralization, immutability, and transparency, presents a promising frontier for enhancing digital evidence verification, offering transformative potential for both Indian and international jurisprudence.

The power of blockchain lies in its distributed ledger, whereby every entry is securely linked and time-stamped, creating an immutable record of transactions.[44][45]Applied to WhatsApp evidence, it immutably and securely stores message data from the time it was generated. It creates a digital fingerprint that courts can use to authenticate chats, avoiding the conventional application of Section 65B of the Indian Evidence Act, which is neither immutable nor decentralized. BNSS and BSA have yet to implement blockchain authentication. The application of these technologies can reinforce custody chains and mitigate tampering or fabrication issues, making digital evidence more reliable.

Disputes regarding WhatsApp chat genuineness usually result from doctored screenshots and fake messages. Blockchain authentication is beneficial by offering tamper-evident proof of message presence. Beyond centralized digital certification, blockchain's decentralized platform minimizes forgery threats. Blockchain transparency also permits data integrity checks, which boost court confidence. Blockchain is, therefore, a viable remedy to authenticate WhatsApp proof, providing trustworthy digital communication in courts.[46]

Courts and legislatures are acknowledging blockchain's potential in evidentiary authentication. U.S. Federal Rules of Evidence and EU laws are being modified to encompass blockchain-backed digital proof, with an emphasis on technological neutrality and dependability. Indian courts are beginning to engage with these technological advancements, as seen in recent court rulings in support of technology assistance for evidence authentication. Problems persist, such as all-litigant accessibility, standard protocols for blockchain utilization, and privacy rights due to*Justice K.S. Puttaswamy (Retd.) v. Union of India*'s

[43]https://lawbhoomi.com/how-to-prove-whatsapp-messages-in-court/
[44]https://ssrana.in/articles/digital-footprints-and-little-steps-why-privacy-matters-for-children/
[45]https://www.scconline.com/blog/post/2025/06/19/illegally-procured-whatsapp-chat-in-matrimonial-dispute-is-admissible-as-evidence-under-section-14-of-family-courts-act-mp-high-court-scc-times/
[46]https://ccgnludelhi.wordpress.com/2023/11/21/navigating-the-indian-data-protection-law-childrens-privacy-and-the-digital-personal-data-protection-act-2023/

privacy jurisprudence.[47] Successful regulation and judicial training are essential for unlocking blockchain's potential while protecting constitutional safeguards.

Blockchain verification mechanisms hold transformative promise to secure the integrity, authenticity, and admissibility of WhatsApp evidence. By embedding immutable, timestamped records within digital ledgers, these technologies can preclude tampering disputes, strengthening the evidentiary value of digital communications in courts. The future legal landscape will likely witness a critical convergence of blockchain innovation with statutory frameworks like BNSS and BNS, heralding a new era of reliable, transparent digital justice.

Cross-Border Access and Challenges with WhatsApp Chats as Evidence in Global Investigations

Cross-border access to WhatsApp data as evidence in global investigations presents substantial jurisdictional and procedural challenges, largely due to WhatsApp's data storage practices and relevant international legal frameworks. WhatsApp primarily stores messages and user data on servers located in multiple countries, often outside the jurisdiction of the country seeking access. This geographical dispersion complicates the ability of national law enforcement authorities to directly obtain digital evidence without navigating complex international legal cooperation mechanisms.

Courts and data protection authorities have a hard time claiming jurisdiction over extraterritorial data. EU law makes WhatsApp a data controller for users' personal data on devices, irrespective of the server's location. Therefore, data processing continues to be in line with the user's country's law, even if servers are foreign, with foreign authorities' access being hampered. Similarly, the Dutch court order maintains that smartphones locally are "use of equipment," expanding jurisdiction but failing to address cross-border data retrieval challenges. These uncertainties result in delays and legal disputes.

To access WhatsApp evidence held abroad, law enforcement authorities normally resort to MLATs or letters rogatory for evidence.[48]MLAT procedures are, however, faulted as slow and bureaucratic, hindering access to important evidence. WhatsApp's policy insists on formal

[47]https://timesofindia.indiatimes.com/city/mumbai/e-documents-admissible-as-primary-evidence-in-court-safeguards-must/articleshow/111545508.cms
[48]https://www.linkedin.com/pulse/foreign-platform-already-subject-eu-data-protection-laws-seinen

legal procedures under national law and human rights before content release. Various national security or privacy legislation can limit international cooperation, and hence, evidentiary gaps. Privacy rights and effective law enforcement are at odds. Data protection legislation such as the EU's GDPR and India's Digital Personal Data Protection Act is stringent in transfer conditions of data across borders, focusing on lawful processing and consent. Courts globally increasingly insist on transparency and due process in such requests, balancing respect for digital sovereignty while inhibiting cross-border crime.Future arrangements such as cloud acts might attempt to expedite these processes while being respectful of basic rights.

In sum, effective cross-border access to WhatsApp chats for legal evidence critically depends on navigating overlapping jurisdictional claims, ensuring compliance with international treaties like MLATs, and respecting evolving global privacy standards, all while striving for prompt and fair investigations.[49]

Conclusion

The use of WhatsApp messages as courtroom evidence in India exposes important tensions between evolving technology, legal frameworks, and constitutional rights. WhatsApp chats, once seen as private, are increasingly scrutinized as potential legal evidence, raising questions about privacy, due process, and reliability. Laws such as the Indian Evidence Act, BSA, and emerging data protection regulations strive to balance justice needs with fundamental rights found in Articles 21 and 20(3) of the Constitution. Although end-to-end encryption safeguards user privacy, pressures from law enforcement for exceptions threaten both digital security and individual freedoms.[50]

Courts must navigate complex issues involving user consent, the evidentiary value of chat data, metadata privacy concerns, and AI-driven authentication requirements.[51] Child protection cases demand heightened confidentiality. Technologies like blockchain could enhance evidence integrity, but legal and judicial systems need to evolve alongside these advances. Cross-border data requests add another layer of complexity, requiring careful management of international agreements and digital sovereignty.

[49] https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited/
[50] https://academic.oup.com/idpl/article/13/3/225/7226249
[51] https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group

To ensure that digital evidence supports justice without infringing on rights such as privacy, silence, and fair trial, strong regulation and vigilant judicial oversight are essential. The real challenge is not simply adapting to new technology, but doing so while upholding core democratic and constitutional principles in the digital era.