

---

# ADMISSIBILITY CONCERNS OF METADATA AND E2EE TECHNOLOGY: EVIDENTIARY NECESSITY V. ENCRYPTION

---

Sree Satya Vaishnavi Musunuri, BAJ-LLB (Hons.),  
ICFAI Law School, Hyderabad, Telangana.

## ABSTRACT

As humankind has rapidly evolved from computers to artificial intelligence, the judiciary has shifted from accepting physical documents as evidence to accepting metadata, WhatsApp messages, and other electronic evidence. Among these, end-to-end encryption is taking the front line.

Although electronic evidence has been recognised in previous legislation, such as the Indian Evidence Act, the new BSA establishes a stronger commitment to recognising the importance of digital evidence, including social media evidence.

And in the era of deepfakes, digital hate crimes, and cyber-related issues, new regulations are forming in accordance with new technologies; one such prominent case is the conflict of interest between the state and individuals in the admissibility of metadata, which, in most cases, has to break the technology of End-to-end encryption, also known as the E2EE feature, often observed in apps like WhatsApp,

This paper discusses E2EE and metadata, along with their relevance in modern evidence laws and the judiciary, and how they affect individuals' right to privacy, along with case laws and recommendations.

**Keywords:** Metadata, Encryption, Evidence, BSA, WhatsApp, Privacy.

**Introduction:**

<sup>1</sup>The new BSA includes electronic evidence, leading to multiple loopholes and complexities, such as metadata or social media evidence presented in court.

Electronic evidence, which is broader in scope than traditional evidence, is defined as follows:

“Data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.”

Under the BSA, electronic evidence and its admissibility are provided under sections 62 and 63 of the Act. It refers to any information stored electronically, resulting in metadata as a form of evidence in technical contexts.

It is now evident that metadata and end-to-end encryption fall under the ambit of electronic evidence.

<sup>2</sup>Under the Indian Evidence Act, 1872, now the BSA 2023, there are important sections that lay down the foundation for what constitutes evidence.

1. Section 2(d) BSA: Refers to what constitutes a document and includes any matter described or recorded upon any substance in the form of letters, numbers, etc., both in the form of a physical document and electronically; this new provision provides inclusivity to all kinds of evidence and makes producing evidence easier.

2. Section 61 BSA: This proviso plays a key role as it aims to protect digital evidence and ensure that evidence is not rejected because it is electronic.

3. Sections 62 and 63 BSA: Admissibility of electronic evidence, even as secondary evidence, as long as the original contents match the copies.

However, for electronic evidence to be admissible, the courts have decided in the case of Arjun

---

<sup>1</sup> Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 62–63 (India).

<sup>2</sup> Indian Evidence Act, No. 1 of 1872 (India), repealed by Bharatiya Sakshya Adhiniyam, No. 47 of 2023

Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)<sup>3</sup>. That certification is mandatory to be accepted as evidence, but if the original is produced, there is no need for the former. While emphasising the need for strict regulations even under the IT Act, the rules should also address issues of metadata, chain of custody, etc.

### **What is metadata and end-to-end encryption?**

In a simple analogy, metadata is like an index to a textbook; it helps guide the user to access the information. These are data that describe the data. It provides more information. The use of metadata depends on the type, that is, descriptive or structural. The main purposes of metadata are data governance, compliance, data tracking, and much more.

Metadata, if used correctly, can be used as circumstantial evidence and is commonly referred to as a digital footprint. For example, if a person 'A' claims that he was present in an area at a certain time, but his GPS was last seen in another area, this can be considered circumstantial evidence. In another example, where a person claims that he did not edit a document after submission, metadata such as last opened or last edited can serve as strong evidence of whether he edited the document.

There are three important forms of metadata:

**1. Descriptive metadata:** One of the most common forms of metadata, and easy to navigate, is descriptive metadata. As the name suggests, it is a descriptive or detailed form of data. For example, if you want to search for a book by its name in an online library, the name of the book, author, publishing house, etc., consists of descriptive metadata.

It is often formatted as an HTML link.

**2. Administrative metadata:** This form of metadata is more about technicalities of the subject, such as which format the user saved the document in (for example, whether a document is saved in Word format, PDF format, etc.) and the time taken. They are formatted as EXIF or system attributes.

**3. Structured metadata:** This can be called the map form of metadata; it provides links and

---

<sup>3</sup> Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1

connections between different subjects in the system. For example, if you download an online copy of a textbook and it shows which page leads to what text, that is structured data; it keeps the data in the system organised. It is formatted as XML or JSON.

Although metadata may seem complex to understand and track, it can be invaluable in cases where evidence has been erased or deleted. Metadata works like a secret spy that keeps track of everything the user does, like how a person who is injured and is absconding leaves a trail of blood stains along the way. Metadata works similarly; even if a person deletes their data on social media, metadata helps to track if they posted anything by tracking the last time they were seen active, the nature of the activity, and even which device they used, along with IP addresses.

For example, in a case where there is a hit and run case in an area without CCTV footage coverage, but there are two suspects, A and B, who claim to be somewhere else, to prove a person's guilt, circumstantial evidence plays the role of a smoking gun; here, if A's Instagram account was active during the time of the accident and the place where it was last active was the same location as the crime scene, it becomes easier to establish the guilt of A. Metadata serves a great use in forming a chain of circumstances.

## **E2EE:**

The concept of metadata negates the idea of E2EE (End-to-end encryption). Most commonly found in WhatsApp, E2EE is a technology that protects the privacy of users using the feature. Commonly discussed, E2EE encrypts the information between two users during the information flow. Once a user sends their information, it is encoded and decoded only when received by the receiver. This feature restricts third parties from accessing messages between the users. This has set a high bar for privacy standards. When metadata and end-to-end encryption are studied together, they are contradictory.

In simple terms, this is contradictory because while E2EE seeks to protect the content, metadata blows up the cover by revealing when and where the context occurred.

For example, if the prosecution wants to prove that a conversation took place between two individuals, but their phones look clean and all conversations are deleted, they can bring up metadata such as the time when their applications were active and from where they were active. If both individuals' phones were active at the same time, say 2:00 a.m., and there was an equal

number of texts on their devices. This at least establishes the possibility that they had a conversation of a similar nature.

In Navjot Sandhu's case, call-record metadata could be accepted as secondary evidence without a Section 65B certificate. The Supreme Court of India subsequently overruled Navjot Sandhu's stand in the case of Anvar P.V. v. P.K. Basheer by using the maxim 'generalia specialibus non derogant', which means that Section 65B is a special provision and prevails over the secondary evidence provisions. In such cases, where it is necessary for the evidence, mere acknowledgement of the happening of the event can be proven worthwhile.

The E2EE feature saves individuals' interests, but metadata serves public and justice interests.

While end-to-end encryption (E2EE) provides a safe space for users, metadata blows the cover. This raises serious questions.

This paper studies the individual's concern and right to privacy and the state's evidentiary necessity, and can be admissible while compromising the ideal behind end-to-end encryption.

### **Evidentiary Necessity V. Encryption of Privacy**

The primary conflict in admissibility is <sup>4</sup>Rule 4(2) of the IT Rules Act. This remains controversial.

It specifically targets social media intermediaries like WhatsApp and Instagram, which are used by more than <sup>5</sup>50 lakh people in the country.

“A significant social media intermediary providing services primarily like messaging shall enable the identification of the first originator of the information on its computer resource as 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 as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules,

---

<sup>4</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2), Gazette of India, Extra., pt. II, § 3(i) (Feb. 25, 2021)

<sup>5</sup> Social Media Intermediaries with More Than 50 Lakh Registered Users in India to Be 'Significant Social Media Intermediary' Under IT Rules 2021, Bar & Bench (Feb. 26, 2021), <https://www.barandbench.com/news/law-policy/platforms-with-more-than-50-lakh-users-to-be-significant-social-media-intermediaries-it-rules>.

2009, which shall be supported with a copy of such information in electronic form”

This rule requires social media platforms to be able to identify the originator of the information in question; however, they are required to do so only if asked to do so by a competent authority.

Although the government has provided certain conditions, tech companies like WhatsApp argue that they have to trace back every single message to reach the source, which violates the entire point of having the feature of end-to-end encryption.

In digital crime cases where the origin of the message must be tracked, it is impossible to do so without it. This chain is protected by end-to-end encryption.

Second, such provisions requiring the breaking of E2EE will encourage self-censorship, once again going against fundamental rights. WhatsApp, while arguing its case, has specifically provided data and mentioned that multiple vulnerable sections- journalists, civil societies, and sensitive groups require confidentiality, and they use the E2EE feature.

To trace one message, the rest must be disclosed.

Section 63 of BSA requires “(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:— (a) the computer output containing the information was produced by the computer or communication device during the period over which the computer or communication device was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication device; (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or communication device in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer or communication device in the ordinary course of the said activities”

This provision is subtly contradictory to E2EE.

This provision requires admissibility on the basis that the data must be regularly fed into the computer or device in the ordinary course of activities.

E2EE platforms use a technology that does not regularly feed the source or store identity-linked data. This provision forces companies to change their entire technology, compromise users' privacy, and operate against their privacy-centric design.

The requirement for tracing the origin of a text using the E2EE feature is not only complex, but it also means that the privacy of millions of users is being compromised, violating Article 21<sup>6</sup> of the Constitution.

## CASE LAWS

Despite the technology of E2EE being very recent, there have been several cases where the admissibility and eligibility of E2EE and metadata have been discussed directly and indirectly

### 1. Puttaswamy v. Union of India (II)<sup>7</sup>

The case dealing with metadata and state surveillance has dealt with sensitive issues such as individual privacy conflicting with the state's interests.

Consequently, the Court invalidated sections that enabled the indefinite retention of such data, reducing the retention period for authentication logs from five years to six months to ensure data minimisation.

This judicial ruling is currently the main defence for platforms that employ End-to-End Encryption (E2EE), such as WhatsApp/Meta. According to the ruling's "Three-Fold Test," any government intervention in privacy rights must be supported by a specific law, have a legitimate purpose, and, most crucially, be proportionate to the threat. Meta asserts that the government's "Traceability" requirement, which aims to trace the "first originator" of a message, fails this test because it would force the decryption of the encryption protocols that safeguard all users simply to locate one individual. With respect to the disclosure of metadata by courts, the ruling held that the executive branch cannot call for private information without judicial oversight (a warrant or order from a judge) and that a high threshold of necessity must

---

<sup>6</sup> INDIA CONST. art. 21.

<sup>7</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1

be met to ensure that even in the pursuit of justice, the constitutional right to privacy is not circumvented by sweeping data requests.

## **2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)<sup>8</sup>**

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) decision provides a procedural framework that underlies the admissibility of digital evidence, such as metadata, in Indian courts. Although the Puttaswamy decision laid down the right to privacy, the Khotkar decision clarified that any electronic record (such as call records or message timestamps) must be accompanied by an obligatory Section 65B(4) certificate to qualify as the primary evidence. This has a direct correlation with End-to-End Encryption (E2EE): since E2EE messages cannot be read, courts and investigation agencies ultimately turn to metadata to establish a connection or timeline. However, the Khotkar decision ensures that the "chain of custody" for such metadata is secure and tamper-proof. When courts demand the production of metadata, they must reconcile the Khotkar procedural requirements with the Puttaswamy "Proportionality Test" to ensure that the requirement for "traceability" or "originator information" does not become a means for mass surveillance or an unconstitutional infringement of a user's basic right to digital anonymity.

## **3. WhatsApp LLC v. Union of India<sup>9</sup>**

In the ongoing litigation of WhatsApp LLC v. Union of India, the introduction of the Bharatiya Sakshya Adhiniyam (BSA), 2023, has added another layer of complexity to the dispute regarding metadata and end-to-end encryption (E2EE) by establishing that the BSA will replace the Indian Evidence Act on July 1, 2024.

WhatsApp argues that the requirement for "traceability" in the IT Rules, 2021 (which WhatsApp claims is unconstitutional under the Puttaswamy privacy standard), runs counter to the protections afforded to individuals through E2EE. However, the BSA provides a tool for the government to establish a basis for utilising metadata to identify the origins of messages sent by WhatsApp users, as it has formally elevated the status of electronic records and metadata (including server logs and timestamps) to that of primary evidence. Section 63 of the BSA (which replaces Section 65B of the Indian Evidence Act) allows for the introduction of a

---

<sup>8</sup> Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1

<sup>9</sup> WhatsApp LLC v. Union of India, W.P.(C) 4648/2021 (Delhi High Court) (pending)

"certificate of authenticity" to identify digital data.

The result is that a "chain of custody" for electronic evidence must now have the same verifiable requirement as that established by the Arjun Panditrao Khotkar (2020) decision. At the heart of the dispute, the government is now able to use the BSA's new FMF to justify its demands for metadata to identify the source of messages sent by WhatsApp users. In contrast, WhatsApp is of the opinion that to provide "traceability" through the government's request for metadata, WhatsApp would have to create a permanent "backdoor" to E2EE. As such, WhatsApp asserts that the backdoor does not satisfy the Puttaswamy proportionality test, and therefore, by creating it, millions of people's privacy would be lost to solve crimes efficiently through metadata collection.

## **CONCLUSION:**

With the change in legislation over the years, it is important to not just adapt to the change in technologies but also to the public's concern over their privacy. Despite the hurdles in serving both, there should be a balance between the privacy of the public and the protection of the public.

The BSA should serve as a tool for authentic justice, not mass surveillance. A few recommendations can be implemented in the evidence law, such as restricting the need for metadata only to cases that involve the security of the state or are heinous in nature, and seeking permission from higher and appropriate authorities, such as the High Court, for approval to access entire data or a major chunk of the user's data. Although a cumbersome process, it is necessary to avoid self-censorship and ensure that it passes proportionality tests. Instead of relying on decryption, hashing technology can be implemented, which does not require decoding everything, but only the ones with the specific hash attached. In this way, only the trail to the text is discovered, but not the entire conversation is discovered.

## **BIBLIOGRAPHY:**

### **I. STATUTES**

1. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
2. Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).
3. The Constitution of India (1950).
4. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

### **II. JUDICIAL DECISIONS (CASE LAW)**

1. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1
3. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
4. WhatsApp LLC v. Union of India, W.P.(C) 4648/2021 (Delhi High Court) (pending).

### **III. ARTICLES:**

1. <https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-union-of-india-ii/>
2. <https://www.scconline.com/DocumentLink.aspx?q=ng4M2RO4>
3. <https://sflc.in/legal-challenges-traceability-provision-what-happening-india/#:~:text=Undermines%20right%20to%20free%20speech,will%20lead%20to%20self%2Dcensorship.>
4. <https://www.okta.com/identity-101/hashing-vs-encryption/>
5. Social Media Intermediaries with More Than 50 Lakh Registered Users in India to Be 'Significant Social Media Intermediary' Under IT Rules 2021, Bar & Bench (Feb. 26, 2021), <https://www.barandbench.com/news/law-policy/platforms-with-more-than-50-lakh-users-to-be-significant-social-media-intermediaries-it-rules>.