BRIDGING THE DIGITAL DIVIDE: CHALLENGES AND REFORMS IN ELECTRONIC EVIDENCE LAW

Kaustubh Singh, Xavier's Law School, St Xavier's University, Kolkata

ABSTRACT

In today's digital age, electronic evidence plays a pivotal role in both criminal and civil litigation. The Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000, recognizes electronic records as documentary evidence. Section 65B of the Evidence Act provides a special procedure for the admissibility of electronic records, particularly when presented as secondary evidence. This paper examines the principles of electronic evidence, the mandatory nature of Section 65B certification, judicial interpretations across landmark cases, and practical issues surrounding fair trial and authenticity. It further analyzes the balance between procedural compliance, privacy concerns, and the necessity of relying on electronic evidence in modern courts.

Introduction

Electronic evidence has become indispensable in modern legal proceedings, ranging from CCTV footage to emails, online chats, and digital signatures. With the rise of cybercrime and technology-driven transactions, courts increasingly rely on digital records to establish facts. Despite this, misconceptions persist regarding the special status of electronic evidence. Many believe that electronic evidence requires completely new laws; however, the Indian Evidence Act, 1872, already governs most evidence, and the IT Act, 2000, merely clarified that electronic records are "documents." Section 65B of the Evidence Act governs the admissibility of computer-generated evidence, providing a framework to present secondary evidence without producing the original electronic device. This paper discusses key principles of electronic evidence, Section 65B compliance, and landmark judicial decisions that have shaped current practice.

Electronic Evidence: Nature and Recognition

Electronic records encompass a wide range of materials, including data stored on CDs, pen drives, hard disks, memory cards, CCTV footage, emails, blogs, websites, and more. The Information Technology Act, 2000, defines electronic records as information generated, sent, received, or stored electronically. Under Section 4 of the IT Act, electronic records are legally recognized as documents, making them admissible in courts. Depending on the context, electronic evidence may serve as documentary evidence, object, or oral communication. For instance, emails and online chats are considered documentary evidence, while the functioning of software may be treated as an act of the machine itself. This multi-dimensional nature of electronic evidence has been aptly described as "digital chameleons," reflecting their adaptability and complex evidentiary value.[1]

The legal framework differentiates between **primary evidence**, which is the original electronic record itself, and **secondary evidence**, which includes printouts, copies, or reproductions of the record. Section 65B allows secondary evidence to be admissible if specific conditions are satisfied, including regular use of the computer, proper functioning, accurate data entry, and certification by a responsible officer under Section 65B(4). Courts have emphasized that non-compliance with Section 65B can affect the admissibility of electronic evidence, but procedural flexibility exists in ongoing trials to balance the fair trial of the accused and the public interest in establishing the truth.[2]

Judicial Interpretations and Case Studies

Several landmark cases have clarified the scope and limitations of Section 65B and the use of electronic evidence in criminal and civil proceedings. In *Chandrabhan Sudam Sanap v. State of Maharashtra (2025)*, the Supreme Court highlighted the mandatory nature of Section 65B(4) certification. The appellant, convicted of rape and murder, challenged the admissibility of CCTV footage. The Court held that mere recovery of footage was insufficient; a proper certificate under Section 65B was necessary, ultimately leading to the appellant's acquittal.[3] Similarly, in *Umer Ali v. State of Kerala (2025)*, the Kerala High Court emphasized that expert reports or FSL documentation cannot substitute for Section 65B certification, as non-production of the original electronic record could lead to an unfair trial.[4]

However, courts have also adopted a pragmatic approach where procedural flexibility is warranted. In *Shri Santosh Shet v. State of Karnataka (2023)*, the Karnataka High Court ruled that the non-filing of a Section 65B certificate does not vitiate proceedings if the trial allows marking, examination, and cross-examination under Section 311 of the Criminal Procedure Code.[5] Similarly, in *State of Karnataka v. T. Naseer (2023)*, the Supreme Court allowed the prosecution to produce a certificate mid-trial, reinforcing that fair trial principles aim to uncover the truth rather than penalize minor procedural delays.[6]

Other cases have addressed the delicate balance between fair trial and privacy. In *Anish Loharuka v. State of West Bengal*, the Supreme Court upheld directions allowing the accused to inspect electronic evidence while safeguarding the privacy of minor victims.[7] This demonstrates that courts are willing to issue ancillary directions to ensure both procedural fairness and the protection of sensitive information.

Furthermore, judicial interpretations have clarified the distinction between electronic records and ordinary documents. In *Meena Kumari Sinha v. M/s Maruti Suzuki India Ltd.*, the Jharkhand High Court held that Section 65B applies only to electronic records and not to photocopies of bank drafts, which can be admitted as secondary evidence under Section 65.[8] This distinction is crucial for practitioners to avoid misapplying procedural requirements.

Principles of Admissibility and Proof

The Supreme Court in *Anvar P.V. v. P.K. Basheer (2014)* emphasized that electronic records

cannot be admitted as secondary evidence without Section 65B certification, and Sections 63 and 65 relating to ordinary secondary evidence do not apply.[9] Courts have recognized the "silent witness" theory, allowing reliable electronic records such as photographs or CCTV footage to substantively "speak for themselves" if the process producing them is trustworthy. Authorship must be established, which can be done through direct testimony, circumstantial evidence, or expert verification under Section 45A of the Evidence Act.[10]

Electronic and digital signatures are also recognized under the IT Act, with Sections 73A and related provisions outlining procedures for proving authenticity. Emails, online chats, and websites are admissible depending on the court's satisfaction, with presumptions under Sections 85A, 85B, 85C, and 88A aiding proof of authenticity. Courts may consider chain of correspondence, user logs, and corroborating digital evidence to establish authorship and credibility.

Challenges and Legislative Gaps

While the legal framework governing electronic evidence in India is well-established through the Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000, and codified procedures under Section 65B, several practical challenges and legislative gaps persist. These challenges hinder the effective use of electronic evidence and complicate the judicial process.

1. Strict Compliance and Procedural Burden

Section 65B mandates certification for secondary electronic evidence, which, while intended to ensure authenticity, has created procedural hurdles. Courts have repeatedly observed that non-compliance can lead to exclusion of critical evidence, even when the authenticity is unquestionable. This strict compliance requirement poses difficulties in cases where original devices are inaccessible, damaged, or seized during investigations. For instance, mobile phones, cloud-stored data, or online records may not be physically available for certification, creating a disconnect between legal mandates and technological realities.

2. Ambiguity in Secondary Evidence and Certificates

The current statutory provisions lack clarity on who qualifies as the "responsible officer" under Section 65B(4) and the specific contents of the certificate. Different courts have interpreted

this requirement variably, leading to inconsistent judgments and legal uncertainty. The lack of a standardized format for certification often results in contested admissibility, even when evidence is genuine and critical for the case.

3. Technological Evolution vs. Static Legal Provisions

The law struggles to keep pace with the rapid evolution of technology. New forms of electronic evidence such as blockchain transactions, encrypted cloud storage, AI-generated documents, social media metadata, and ephemeral messaging apps are not explicitly addressed under existing provisions. While courts have relied on general principles to admit such evidence, this creates a risk of inconsistent application and challenges in verifying authenticity.

4. Privacy and Data Protection Concerns

The collection and presentation of electronic evidence often involve sensitive personal information, including communications, financial data, or medical records. The current legislative framework does not adequately address privacy concerns in the context of evidence collection, storage, and disclosure. Courts have had to balance Section 65B compliance with fundamental rights such as privacy, often issuing ad hoc directions. A lack of comprehensive statutory guidelines on privacy safeguards creates uncertainty and may compromise both fairness and the protection of victims or third parties.

5. Limited Judicial and Investigative Expertise

Handling electronic evidence requires technical expertise for proper authentication, extraction, and analysis. However, many courts and investigative agencies lack personnel with adequate digital forensics skills, resulting in procedural delays, errors in certification, or challenges to evidence admissibility. This gap is particularly pronounced in rural or lower judiciary courts, where reliance on technological experts is limited.

6. Enforcement and Practical Difficulties

Even when Section 65B is complied with, practical enforcement challenges remain. For example, in cybercrime or corporate fraud cases, evidence may be stored across multiple jurisdictions or foreign servers. Coordinating retrieval, certification, and authentication in such scenarios often exceeds current procedural mechanisms, highlighting the need for legislative

updates that address cross-border electronic evidence.

7. Need for Legislative Reform

Scholars and judges have suggested that a dedicated legal framework for electronic evidence, potentially as a separate chapter within the Evidence Act, could resolve these gaps. Such reform could standardize certification procedures, define responsible officers, establish guidelines for emerging digital evidence, and integrate privacy safeguards. The Madras High Court, in *Yuvaraj v. State*, emphasized the need for legislative clarity to streamline admissibility and reduce inconsistent judicial interpretation.

8. Balancing Authenticity, Fair Trial, and Practicality

Courts are often forced to navigate a tension between strict procedural compliance and the broader principles of a fair trial. Overly rigid enforcement of Section 65B can result in the exclusion of probative evidence, adversely affecting justice, while overly lax interpretation risks admitting unauthenticated or tampered data. A legislative framework that explicitly accounts for such flexibility while setting minimum standards could reduce judicial discretion and promote consistency.

Conclusion

Electronic evidence has transformed the legal landscape, offering courts powerful tools to establish facts and protect rights. Section 65B provides a mechanism for admitting secondary evidence, but courts have balanced strict procedural compliance with fair trial principles. Landmark cases such as *Chandrabhan Sudam Sanap*, *Umer Ali*, and *Anvar P.V.* have reinforced the importance of Section 65B certification while also recognizing practical realities and the need for flexibility. Moving forward, awareness of statutory provisions, judicial guidance, and technological expertise will be crucial for the effective use of electronic evidence in India. Ensuring authenticity, protecting privacy, and facilitating fair trials must remain the guiding principles as electronic evidence becomes increasingly central to the pursuit of justice.

Endnotes:

1. Information Technology Act, 2000, §§ 2(r), 2(t).
2. Indian Evidence Act, 1872, § 65B(4).
3. Chandrabhan Sudam Sanap v. State of Maharashtra, 2025 INSC 116.
4. Umer Ali v. State of Kerala, 2025 KER 24851.
5. Shri Santosh Shet v. State of Karnataka, 2023.
6. State of Karnataka v. T. Naseer, 2023 INSC 988.
7. Anish Loharuka v. State of West Bengal, Supreme Court.
8. Meena Kumari Sinha v. M/s Maruti Suzuki India Ltd., Jharkhand HC.
9. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
10. Indian Evidence Act, 1872, § 45A.
11. Yuvaraj v. State, Madras HC.