Challenges of electronic evidence and its admissibility in court

Geethapriya S, Tvisha G

Law students

School of law

Sastra deemed to be University, Thanjavur, India

tvishakrishna@gmail.com , geethapriya2003s@gmail.com

Abstract-In the present-day technology permeates every thread of human activity. From the ways we communicate and conduct business to banking, education and even the corridors of the justice system, digital devices and online platforms have become woven into the fabric of each sector. This sweeping shift, toward tech has given rise to a category of courtroom proof what's now called digital evidence. All the bits and bytes that sit on a screen or travel through a network emails, SMS chatter, CCTV reels, call logs, social-media footprints, computer documents and the endless stream of data tucked into gadgets make up what we call evidence. From tribunals to courts the pendulum is swinging ever more toward this digital trove to pin down facts and dispense justice with sharper precision.

The rapid spread of technologies has compelled courts to keep pace with a shifting landscape. Conventional ways of gathering and authenticating evidence now feel insufficient as an ever-growing portion of records is produced and stored electronically than, on paper. Still even though electronic evidence can boost the speed and precision of the justice system it also brings a host of complications. This raises questions about the data's authenticity, its reliability and the procedural steps needed to grant it authority, in court. Unlike documents whose authenticity can often be corroborated by the presence of a signature or the idiosyncrasies of handwriting digital records can be subtly altered, completely erased or even fabricated from nothing all while leaving little to no trace. This situation raises a concern: can the evidence submitted be trusted to portray the actual facts of the case?

In India the principal legal reference, for evidence is the Indian Evidence Act of 1872 later updated by the Information Technology Act of 2000 to bring records within its scope. The pivotal provision here is Section 65B which sets out the criteria, for a record to be deemed admissible in court. Specifically, Section 65B (4) requires a certificate that vouches for the record's reliability identifies the device that produced it and describes the process by which it was generated. When the certificate's missing people generally deem the evidence inadmissible.

The architecture of the law today bears the imprint of a pair of rulings. When the Supreme Court tackled Anvar P.V. v. P.K. Basheer in 2014 it drew a line: no electronic evidence gets a hearing without a Section 65B certificate.

That judgment locked in a exacting benchmark, for admitting records. Subsequently in the 2020 judgment of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal the Supreme Court reiterated that a certificate remains a cornerstone while simultaneously carving out a few defined exceptions chief, among them situations where the party seeking to introduce the evidence simply cannot access the device in question. Those pronouncements have equipped courts with a framework, for wrestling with electronic evidence yet they have also laid bare the persistent gaps and hazy ambiguities that still surface in practical application.

Key issues surrounding evidence include the risk that digital data can be altered or fabricated inadvertent slip-ups, during data collection, a dearth of proficiency among legal practitioners and non-compliance, with certification standards. A substantial proportion of investigating officers, lawyers and even judges often lack the training needed to understand the mechanics of systems. As a result, evidence may be. Discarded because of flaws. On top of that the surge, in cyber-crimes hacking, fraud makes it tougher to verify that digital evidence presented in court is genuine.

Indian courts have over time edged toward a realistic way of dealing with electronic evidence. Judges are becoming increasingly attuned, to the nuts and bolts and, alongside the legal lenses they're now factoring in the technological quirks of digital records. Still the road ahead looks steep. Drawn out. At the time there's a growing clamor for reform to tidy up the rules on evidence so they mirror today's reality. Moreover judges, lawyers and police officer's ought to receive training to deepen their grasp of forensics and to handle evidence properly. At the time the government must equip the courts, with facilities and specialist support ensuring that electronic evidence is evaluated and presented with precision.

To sum up electronic evidence has become a cornerstone of the legal system trimming the length of trials and sharpening the precision of judgments. Nonetheless its use must be tightly corralled by safeguards to ward off abuse. The authenticity and reliability of data should be formally. Subjected to thorough technical scrutiny. All parties involved judges, attorneys,

investigators and the general public need a working knowledge to ensure electronic evidence is handled responsibly. By tightening up the framework leveraging technology and rolling out dedicated training programs India can stitch together a more effective and trustworthy system, for handling electronic evidence. While digital evidence signals a step toward modernization its responsible use hinges on striking a balance, between legal insight and technological know-how

---

Objectives

1. To understand the legal requirements for admitting electronic evidence in Indian courts, especially under Sections 65A and 65B of the Evidence Act.

2. To identify the practical problems faced by police, lawyers, and judges while collecting, preserving, and presenting electronic records.

3. To analyse how courts have interpreted and clarified the rules on electronic evidence through major judgments like Anvar P.V., Arjun Panditrao, and others.

4. To assess the reliability and authenticity issues related to electronic data and understand why digital records are more vulnerable to tampering.

5. To suggest improvements in procedure, infrastructure, and training for better handling of electronic evidence in India

---

Tables of contents

I. Introduction

The infiltration of technology, into every corner of human life—how we converse, conduct business and run governments—has been profound. As a result, courts now find themselves handling a growing number of cases in which electronic records serve as the centrepiece of evidence. Such evidence can appear as emails CCTV footage, voice recordings of phone calls, computer files, social-media posts or digital photographs. Today these digital artifacts are commonplace, in both criminal proceedings, either bolstering or challenging the claims put forward by the parties involved.

Nonetheless as reliance, on evidence deepens a range of complications has surfaced. A primary worry concerns the way the legal system treats this kind of proof and the criteria it employs to assess its reliability. Unlike paper documents digital evidence can be altered, edited or erased without leaving traces. Consequently, it becomes especially thorny to determine whether a specific electronic record is the original or has been tampered with. Hence it becomes imperative to devise protocols that can both validate the authenticity and assess the credibility of electronic data before it is allowed to stand as evidence, in a courtroom.

In India the legal system has finally begun to acknowledge how pressing these issues are prompting a series of revisions. The Information Technology Act of 2000 for instance overhauled the Indian Evidence Act of 1872 by inserting provisions that deal specifically with evidence. Those amendments paved the way, for sections 65A and 65B which spell out the standards for presenting records as evidence, in court. In particular Section 65B outlines the conditions digital evidence must satisfy to be considered valid including the need, for a certificate that spells out the method and location of the record's production.

The paper navigates the realm of evidence laying bare the myriad hurdles judges confront when they must weigh such material. It also canvasses a suite of judgments that have steered courts in their treatment of digital records. Cases such, as Anvar P.V. v. P.K. Basheer

and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal stand out for their influence, on the interpretation and application of Section 65B. These rulings highlight the nature of certification while exposing the challenges that investigators and courts wrestle with as they strive to abide by established procedures.

The central questions this study ai[1]ms to explore are listed below:

1. According to statutes how is electronic evidence characterized and which conditions dictate its admissibility?

2. What, on-the-ground difficulties do investigators, attorneys and judges grapple with when trying to employ that kind of evidence?

3. What steps have Indian courts undertaken to assure that digital records are accurately authenticated and duly certified?

The paper is organized as follows: Chapter II details the research methodology presents the findings and offers interpretations; Chapter III provides a summary of the study; Chapter IV supplies suggestions and recommendations. Chapter V lists the references and sources consulted.

At its core the study aims to spotlight the expanding influence of evidence, within India's framework and to press for continual reforms that guarantee digital material is managed fairly securely and dependably.

II. The Main Body[2]

2.1 How the Study Was Conducted

Employing a qualitative lens the investigation leans largely on sources. It entails a dissection of the Indian Evidence Act of 1872 and the Information Technology Act of 2000 tracing the contours of their language. The analysis also canvasses the trail left by the Supreme Court and the High Courts drawing directly from their judgments and accompanying opinions. In addition, it weaves in material harvested from journals, a range of repositories and the reflections of eminent scholars.

The central aim of this paper is to chart the recurring legal-compliance challenges that surface with evidence— the nuances of Section 65B of the Evidence Act the thorny issue of technical reliability and the intricacies of the chain of custody. Framed, as an inquiry the work outlines these problems. Puts forward practical solutions to address them.

2.2 Findings

A. The core concept, alongside the framework that underpins it

Definition:

Electronic evidence refers to any data stored or transmitted in a format that can be used as proof, in a courtroom. Following amendments Section 3 of the Indian Evidence Act defines " records" as a form of documentary evidence.

Legal provisions relevant, to this matter:

• Sections 65A and 65B: These provisions outline how electronic records are to be created and authenticated.

• Section 22A: it holds that verbal concessions concerning the substance of a dossier are inadmissible except when the dossier's authenticities called into question.

• Section 45A: Deals, with a specialist's view of a person who has sifted through evidence.

• The Information Technology Act of 2000 bestows legitimacy, on signatures underpins e-governance schemes defines cyber-crimes and affirms that electronic records are as valid, as their paper counterparts.

[1] Indian *Evidence Act, 1872*, 3 — defines "documents" to include electronic records after the 2000 amendment.
Indian Evidence Act, 1872, 65A–65B — provide special rules for admissibility and authentication of electronic records.

[2] Indian *Evidence Act, 1872*, 45A — expert opinion of an examiner of electronic evidence (digital/forensic expert) is admissible.
Information Technology Act, 2000, 3, 4, 5, 65–78 — give legal recognition to electronic records, digital signatures, electronic governance, and define various cyber-offences.

B. Judicial Interpretation – how courts read statutes

Key Cases Unveiling the Impact of Electronic Evidence, on Judicial Outcomes

1. **Anvar P.V. v. P.K. Basheer (2014) – 10 SCC 473**

Standing as a judgment, on the treatment of proof in India this case compelled the Supreme Court to grapple with a crucial question: could digital artefacts—such, as CDs and audio recordings—be admitted as evidence without a proper certificate attesting to their authenticity? In the past some courts had allowed material to slip in on the basis of a witness's testimony. In this landmark ruling however the Court drew a line insisting that any electronic record must satisfy the stipulations of Section 65B of the Indian Evidence Act before it can be admitted.

The Court affirmed that, in tandem with the record a certificate pursuant, to Section 65B(4) of the Act must be attached. This certificate should delineate the methodology employed to generate the record and certify that the device used was functioning as intended. It stands as the singular evidentiary foundation upon which the record's reliability and admissibility rest. That decision has rendered the procedure, for procuring records more stringent thereby ensuring that only authenticated and verified digital evidence may be admitted in court.

2. Arjun Panditrao Khotkar, vs. Kailash Kushanrao Gorantyal (2020)

During the hearing the Supreme Court took another look, at the Anvar P.V. Ruling effectively reaffirming it. The bench made it clear that as a matter of course a Section 65B certificate should accompany any evidence that is presented. In this setting the Court highlighted a principle: when a party cannot access the hardware that produced a record—perhaps because the data is held by a third party or a service provider—the tribunal may still admit the evidence if the record's provenance can be convincingly shown. The decision tackles a real-world obstacle that many litigants confront the difficulty of obtaining the device or system that generated the evidence essential, to their case.

3. Tomaso Bruno, versus the State of U.P. (2015)

At issue, in this case was how much weight CCTV footage ought to carry in a trial. The Supreme Court pointed out that electronic evidence— surveillance video—can be pivotal in bringing matters to light. It chided the prosecution for neglecting to put forward any footage that could have been used as proof remarking that the void of material weakens the state's case. The ruling serves as a reminder of the ever-growing importance of evidence, in cracking crimes and steering courtroom proceedings.

C. Common Challenges We've Identified[3]

1. Technical Tampering: Electronic data can be fiddled with by a range of individuals through a plethora of methods, which inevitably fuels scepticism, about whether the documenters genuine.

2. Issues, with a Section 65B Certificate: In practice many law-enforcement investigators skip obtaining the certificate, which often results in the evidence being ruled inadmissible.

3. Lack of Technical Expertise: A clear gap remains in how lawyers, police officers and judges grasp evidence.

4. Chain of Custody: How a device is handled, logged and stored can tip the scales on its worth—any lapse or break in that custody trail can undercut its credibility.

5. Cybersecurity Risks: The chance that hackers or malware could tinker with—or completely erase—essential data triggers security concerns.

6. Jurisdictional obstacles: When information lives on servers actually reaching it and confirming its accuracy turns into a task.

7. Limited Legal Awareness: When the requirements are misunderstood, procedural mistakes and slowdowns, in paperwork become commonplace.

2.3 Discussion

In India electronic evidence only finds a place, in court when it satisfies the required criteria. Over rulings the judiciary has repeatedly underscored that authenticity and reliability are indispensable before any digital proof is admitted. Even as technology becomes more

[3] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 — 65B certificate mandatory for electronic evidence.
Arjun Panditrao Khotkar v. Kailash K. Gorantyal, (2020) 7 SCC 1 — Reaffirmed *Anvar*; 65B certificate needed unless device unavailable.
Tomaso Bruno v. State of U.P., (2015) 7 SCC 178 — Stressed importance of CCTV and electronic proof

sophisticated and swifter the corresponding legal provisions lag behind. A rigorous application of Section 65 B is often invoked as a shield against tampering. That very strictness can sometimes lead to the exclusion of evidence that, in reality 's trustworthy.

Consistency:

Judges demand proof that a digital record's the original and hasn't been altered. In practice establishing that authenticity usually requires testimony, verification of hash values and a forensic examination of metadata—resources that're n't always readily available.

Developments, in the judiciary:

With the Anvar P.V. Case finally settled the judiciary tightened its grip, on the certification requirement. Yet the 2018 judgment, in Shafhi Mohammad v. State of Himachal Pradesh opened a loophole permitting an exception where the requisite certificate could not be obtained. That lingering uncertainty was later resolved by the Arjun Panditrao Khotkar decision, which reaffirmed the nature of Section 65B.

Real-world stumbling blocks:

Many local police agencies and district courts still go without a digital-forensics lab or the trained staff to run one. As a result, crucial evidence—phone records, surveillance video and the like—often ends up inadmissible after slip-ups. Because the digital world never stays still—emails, social-media posts, cloud-based files—it keeps throwing hurdles into the road of evidence collection and preservation.

Negotiating the Tension Between Law and Technology:

The legal apparatus needs to reconcile the parties' craving for data, with the complexities of real-world circumstances. Banning evidence outright risks its brand of injustice while a blanket tolerance could erode the very notion of fairness. The sensible path lies somewhere in, between—emphasising measurement, careful documentation and proper certification than swinging to either extreme.

Chapter III –

In today's world picturing a courtroom without any electronic evidence feels like a flight of fancy. Technological progress has surged to a point where every piece of information and every service run through the internet or lives inside electronic devices. Whether the dispute involves cyber-crime, fraud, a smear campaign or a corporate clash the digital breadcrumbs—emails, CCTV footage, social-media posts, mobile call records and computer files—often become the thread that pulls the truth into view. In light of that electronic evidence now underpins proceedings throughout India.

Yet notwithstanding the courts' mounting dependence, on evidence a host of issues still linger when it comes to its admissibility and credibility. The chief snag lies in proving that digital data are both precise and trustworthy. In contrast, to the permanence of paper records electronic information can be tweaked, reconfigured or wiped clean without leaving any breadcrumb. Consequently, it falls upon the judiciary to institute iron-clad procedures that verify any submitted evidence is authentic and untampered.

India is gradually turning a corner on these problems. A watershed moment arrived with the 2000 Information Technology Act and the later tweaks, to the 1872 Indian Evidence Act, which birthed Sections 65A and 65B. Those clauses lay out a roadmap for courts to admit proof. Still the rules often fall short of reality. Many police officers' investigators and lawyers simply lack the technical know-how to gather and present data. In turn the failure to observe every nuance of the process has given rise to a problem of procedural non-compliance.

Moreover, uneven infrastructure throws up hurdles. Many courts, across India are still wrestling with tools, which hampers their capacity to gather organize and display evidence efficiently. For example, confirming signatures. Parsing metadata demand specialized hardware and expertise that aren't universally available. Likewise, the necessity of a Section 65B certificate—though has become an impediment. This certificate is meant to certify that the evidence is authentic and has been properly verified. Yet often the person presenting the evidence isn't familiar, with the device's technical details nor has access, to the original device required to issue the certificate. As a result, legitimate evidence can be dismissed because of procedural technicalities.[4]

Dealing with these problems calls for a policy that remains flexible while still guaranteeing the security of the evidence. Judges and legislators could come to an agreement that even though the integrity of records must be preserved the admission process can be made simpler. In addition, offering updates and training—through workshops and seminars, on the digital systems—would be advantageous for judges, lawyers and investigators alike. Such instruction would not only impart an understanding of how these systems operate. Also teach the proper methods, for handling that kind of evidence. Amplifying public awareness, via campaigns that stress the necessity of safeguarding and generating evidence could cultivate responsibility and deeper comprehension, among citizens.

[4] *information Technology Act, 2000* — introduced legal recognition for electronic records and enabled amendments to the *Indian Evidence Act, 1872* including Sections 65A–65B.
Indian Evidence Act, 1872, 65A–65B — provide the procedure for admitting electronic evidence and require a 65B certificate for authenticity

In short electronic evidence now sits at the heart of courtroom battles. Its full promise however can only be unlocked if the law is sturdy enough and the technology is, up, to snuff. India stands on the brink of a scenario where digital proof is processed with ease, fairness and crystal-clear transparency—provided judges receive rules facilities get a boost and practitioners obtain solid technical training. Striking that spot will lift the courts' competence and sharpen the fidelity of decisions that rely on tech-driven evidence.

Chapter IV: Recommendations and Prospects, for the Future

1. Legal reform efforts:

Streamlining the certification process laid out in Section 65B is essential and exploring authentication approaches—such, as hash verification—should be given serious consideration.

2. Training Programs, for Judges and Police:

Regular training that hones in, on digital-evidence handling should be offered to judges, prosecutors and law-enforcement officials.

3. Setting up units:

Communities ought to be equipped with accredited digital-forensic laboratories, a step that safeguards the integrity of any evidence collected.

4. The Standard Operating Procedures (SOPs):

A nationwide set of guidelines needs to be put in place to steer the gathering, safekeeping and showcasing of records.

5. Awareness, among the public:

Properly schooling both attorneys and the parties they represent on evidence is vital to stop it from being tossed out.

6. Nurturing cooperation, on the stage:

Giving a boost, to legal assistance treaties (MLATs) is key, to unblocking the flow of cross-border data and digital records.

7. Enlisting blockchain technology:

Exploring blockchain technology to timestamp and verify records is a step worth taking.

8. Possible Avenues, for Future Research:

Future research could zero in on evidence the growing menace of deepfakes and the privacy quandaries that complicate their admissibility in court.

Chapter Five: References

1. Indian Evidence Act of 1872 subsequently amended by the Information Technology Act of 2000.

2. The Information Technology Act, 2000.

3. Anvar P.V. v. P.K. Basheer (2014) — 10 SCC 473.

4. The case of Arjun Panditrao Khotkar, versus Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

5. Tomaso Bruno v. State of Uttar Pradesh (2015) – case reported at 7 SCC 178.

6. Shafhi Mohammad, v. State of Himachal Pradesh (2018) 2 SCC 801.

7. Sharma, R. (2021). "Admissibility of Electronic Evidence, in Indian Courts—Issues & Challenges." Indian Law Journal of Technology & Law.

8. A. Agarwal (2020) contributed "Digital Evidence and the Indian Judicial Approach", to Cyber Law Review volume 6.

9. The Ministry of Electronics and Information Technology, Government of India.

10. An assorted collection of commentaries and internet-borne legal resources.