

DIGITAL EVIDENCE IN COURT: ADMISSIBILITY, RELIABILITY AND CHALLENGES IN INDIA

¹ Eliza Maisnam, ²Dr. Abhimanyu Sethy

¹Research Scholar, Department of Law, Arunodaya University, Itanagar, Arunachal Pradesh, India

²Supervisor, Department of Law, Arunodaya University, Itanagar, Arunachal Pradesh, India
elimairembam18@gmail.com

Abstract

The swift progression of technology has revolutionized the global scenario. The changes brought by the digital revolution have transformed the legal arena, particularly regarding the utilization of digital evidence in court proceedings. This paper investigates the legal framework governing the admissibility, reliability, and challenges of digital evidence in courts functioning in India.

It delves into the statutory provisions outlined in the Information Technology Act, 2000, and related amendments that form the foundation of digital evidence admissibility, including the Indian Evidence Act, 1872. The paper also explores practical issues faced by legal practitioners in acquiring, preserving, and presenting digital evidence, which includes challenges faced due to data tampering and the evolving nature of cybercrimes.

Furthermore, the paper discusses the need for more legal reforms to match the implications of emerging technologies.

In conclusion, the specific objective of the paper is to highlight the importance of strategies and foresight for the effective utilization of digital evidence in Indian courts to ensure that the principles of justice and fairness are intact in the digital age.

Keywords: Digital, technology, legal, evidence, court, justice

Introduction:

The 1950s brought about computers, and since then, the data format storage has been binary. Now, if we look at the vast amount of data available, the 1s and 0s have mostly overtaken the paperwork. Computers did make a late entry in India compared to other developed countries, but the data in India has crossed chiefly over to the digital format. Everything is becoming enclosed in the digital arena, from education, health, finance, departments, institutions, the legal spheres, etc. Hence, traces of evidence left or generated are also highly impacted and influenced by digitisation.

The digitisation process has brought about a sea change in the documentation process, with the proliferation of technology transforming how evidence is generated, stored, and presented in legal proceedings.

According to Section 79 A of the IT Act, 2000, “Electronic form evidence” means any information of probative value that is either stored or transmitted electronically. It includes computer evidence, digital audio, digital video, cell phones, and digital fax machines. Digital evidence—from emails, social media posts, and text messages to more complex data like computer logs, CCTV footage, and encrypted files—plays an increasingly important role in civil and criminal cases.

However, digital evidence presents unique challenges in the courtrooms. The inherent nature of digital data—being easily modifiable, duplicable, and often challenging to authenticate—raises serious concerns about its integrity. The issues of data tampering, unauthorised access, and the complexities of ensuring chain of custody further complicate the judicial process. Moreover, the reliance on technology demands a certain level of technical expertise from legal professionals and judges, which can be a significant hurdle in a legal system traditionally rooted in physical evidence and manual documentation.

The global standards of evidence management and data protection also influence the judiciary's approach to digital evidence in India. It is necessary to balance local legal principles with international best practices. The admissibility of digital evidence hinges on strict compliance with legal procedures, and any lapses can lead to crucial evidence being excluded, thereby impacting the outcome of cases. Additionally, the reliability of digital evidence is under scrutiny in light of emerging technologies like blockchain, artificial intelligence, and digital forensics, which offer new ways to validate or challenge digital records.

Admissibility of evidence is the eligibility of a particular item as evidence in a case. In simple terms, it means the acceptance of a particular character or allowing it to be introduced, used or produced during legal proceedings. It is the information age, and most information now leaves behind digital footprints. The paper will examine the admissibility, reliability, and challenges the judiciary and legal practitioners face in handling this evolving evidence.

Analysing essential case laws, statutory provisions, and technological advancements will provide a comprehensive understanding of the complexities of digital evidence in India. Furthermore, it discusses the need for continuous legal reforms and capacity building within the judiciary to effectively address digital evidence's dynamic nature. The ultimate goal is to ensure the legal system remains robust and capable of delivering justice in an increasingly digital world.

Theoretical framework:

Digital evidence is increasingly becoming a crucial aspect of the legal landscape, especially in courts of law. In the Indian context, digital evidence's admissibility, reliability, and challenges come under the purview of statutes, judicial interpretations, and evolving technological considerations.

This paper considers three theories to examine the admission, reliability and issues of Digital Evidence in Courts.

According to the realist theory, law is filled with ambiguities, vagueness, and contradictions, and there is no correct answer regarding decisions by the judges. Legal realism emphasises the law's adaptability to social and technological changes. This theory supports the idea that laws should evolve to address the unique challenges digital evidence poses. Technological neutrality, a related concept, holds that the law should not favour one type of technology over another but should apply consistently across all evidence, including digital.

The reliability theory emphasises the accuracy and trustworthiness of electronic evidence presented in court. It scrutinises the methods used to collect, preserve, and present

the evidence to ensure it accurately reflects the original data. This theory focuses on reducing the risk of data manipulation and corruption by focusing on the importance of forensic processes and technologies.

The third theory, the chain of custody, lays the framework for the authentication of digital evidence, ensuring that the evidence produced in court remains untampered and unaltered, so there is the requirement for meticulous documentation and preservation. It involves the journey from the collection of data to the presentation of evidence in the court. If there are any breaks in this flow, doubts on the integrity of the evidence can arise.

In conclusion, digital evidence in Indian courts necessitates a robust theoretical framework that addresses the complexities of its admissibility, reliability, and authenticity. By integrating the perspectives of legal realism, technological neutrality, and the principles of reliability and chain of custody, this paper underscores the need for adaptive legal standards that can effectively manage the challenges posed by digital evidence. These theories collectively provide a foundation for ensuring digital evidence is accurately collected, preserved, and presented, maintaining its integrity and trustworthiness in judicial proceedings.

Admission of electronic evidence in India:

According to Section 61 of the Indian Evidence Act, the task of proving any form of document is through the examination of either primary or secondary evidence. Section 62 defines *primary evidence* as the original document, and regarding electronic documents, Section 65A stipulates that their contents must be proven by Section 65B. The general rule established by the Indian Evidence Act is that every document should be proven using primary evidence. Hence, secondary evidence is subject to the conditions outlined in Section 65.

The electronic document, whether primary or secondary, can be interpreted only by a computer as it is in binary code. Therefore, a court can only independently review such a document with a person who can provide written testimony regarding its contents, making the distinction between “primary” and “secondary” electronic documents practically irrelevant. Section 65B of the Indian Evidence Act outlines the procedure for producing a certificate to make an electronic document admissible in court. The focus is on ensuring that proper certification accompanies the evidence.

Therefore, an electronic document must always be certified to ensure it accurately reflects what it represents when read on a computer using the appropriate software. The person providing this certification acts as an expert who assists the court, a role formalised under Section 65A, with the certification process detailed in Section 65B.

A pivotal case is *Shafi Mohammad v. The State of Himachal Pradesh*, where the Supreme Court provided crucial insights into the admission of electronic evidence under Section 65B, emphasising the need for strict procedural compliance and also throwing light on the requirement of a certificate in the case of admission of digital evidence. In the *Anvar P.V. v. PK Basheer & Ors* case, the apex court delves deeply into the authentication of electronic evidence. The court’s interpretation of Section 65B and its focus on the necessity of a certificate for secondary electronic evidence reinforced the importance of procedural precision in handling electronic evidence. The court held electronic records and digital

signatures as admissible evidence in the Bodala Murali Krishna v. Smt. Bodala Prathima case.

In the Dharambir v. Central Bureau of Investigation case, the court held that Section 65B encompasses the computer output and the hard disk containing stored information as evidence. It differentiated electronic records: one being the hard disk itself, and the other being the active information (text, sound, video files) that can be copied to other devices like CDs or pen drives.

The Supreme Court assessed the digital evidence used by the Haryana Assembly Speaker, including interview transcripts from various television channels, to disqualify a member for defection in the Jagjit Singh v. State of Haryana case. The above-mentioned cases stand testimony to the fact that there is a growing trend in Indian courts towards recognising and valuing digital evidence in legal proceedings.

Reliability of Digital Evidence:

Courts have progressively started to accept digital evidence. For instance, in the Amitabh Bagchi v. Ena Bagchi case, the court ruled that digital mediums such as video conferencing can be used and physical appearance is not mandatory. The court underlined in the case of Tomaso Bruno and Anr. v. State of Uttar Pradesh that technological advancements and scientific methods must be integrated into investigations, recognising electronic evidence as crucial for establishing facts. They noted that scientific and electronic evidence can significantly aid investigative agencies.

The court dealt with the admission of mobile phone records for admission as evidence in State (NCT of Delhi) v. Navjot Sandhu, concerning the December 2001 Parliament attack. Despite the defence's claim that the prosecution's failure to produce a certificate invalidated the records, the apex court found that the cross-examination of a witness knowledgeable about the computer's operation and the printout process was sufficient to establish the call records' validity.

Challenges:

The swift evolution of technology has brought both new challenges and opportunities in the realm of electronic evidence. Recent high-profile cases involving leaked WhatsApp chats and social media posts obtained during investigations have underscored the need for a robust and adaptive legal framework to address the admissibility of digital evidence. Specifically, Section 65B has faced scrutiny as it adapts to emerging technological trends and evolving legal standards.

The court provided significant insights into the interpretation and application of Section 65B in the case of Arjun Panditrao Khotkar v. Kailash Kishanrao Goratyal. The court delineated the distinctions between primary and secondary evidence and reinforced the requirement for certificates to validate secondary copies of electronic records. Additionally, it emphasised the critical role of procedural adherence and technological proficiency in handling electronic evidence.

Significant challenges persist despite advancements in defining the legal framework for electronic evidence. The rapid expansion of digital technologies, the enormous volume of electronic data, and the continually shifting landscape of cyber threats present ongoing

obstacles for legal professionals and courts. Issues such as data privacy, cybersecurity, and the verification of electronic records remain complex and pressing, so lawmakers, legal practitioners, and technology experts need to collaborate effectively to address these challenges and adapt legal frameworks to the digital age. Efforts to streamline electronic evidence procedures, enhance technological infrastructure, and increase digital literacy among legal professionals are crucial for ensuring the effective administration of justice in the digital era.

Conclusion:

Electronic evidence has emerged as a crucial component of modern legal practice, bringing substantial challenges and significant opportunities for legal professionals and the judiciary. The mandate for a certificate under Section 65B highlights the necessity for rigorous procedural adherence and advanced technological proficiency in managing electronic evidence.

As our society becomes increasingly digital, it is essential for all stakeholders—including lawmakers, legal practitioners, and technology experts—to remain vigilant, adaptable, and proactive in addressing the complexities associated with electronic evidence. The rapid evolution of technology, the vast volume of electronic data, and the sophisticated nature of cyber threats necessitate continuous adaptation of the legal framework to keep pace with these developments. Strengthening legal standards, improving technological infrastructure, and enhancing digital literacy among legal professionals are crucial steps in ensuring effective justice in the digital age.

It becomes relevant and necessary to foster a collaborative approach between the legal and technological communities to successfully navigate the complexities of electronic evidence. This includes promoting ongoing education and training for legal professionals on emerging technologies and best practices for handling electronic evidence. Additionally, efforts should be made to streamline the procedures for presenting electronic evidence in court, ensuring that these processes are efficient and secure.

Furthermore, a concerted effort must be made to address data privacy and cybersecurity issues, which are increasingly pertinent in the digital era. By developing robust legal frameworks and implementing advanced technological solutions, we can better protect sensitive information and ensure that electronic evidence remains reliable and secure. In an ever-evolving digital sphere, where new technologies and innovative minds continually reshape the landscape, there will inevitably be ambiguities in applying a consistent set of rules. What suffices in one scenario—perhaps a certificate—may require procedural precision in another, especially when dealing with electronic evidence. Whether it is digital signatures, hard disks, or interview transcripts, the challenges are endless as new technologies proliferate, bringing new forms of cybercrime.

Jurists are increasingly adapting to these technological and societal changes by accepting and relying on digital evidence to pronounce judgments. This shift suggests that virtual and legal realism will advance technologically. The authentication processes—such as the issuance of certificates, examination of digital signatures, and meticulous data collection—underscore the reliability theory's focus on the accuracy and trustworthiness of digital data.

Since data tampering remains a significant challenge, the chain of custody theory plays a crucial role, forming the backbone for documenting and preserving digital evidence.

In conclusion, as the digital world continues to expand and evolve, the legal system must remain agile and adaptive, ensuring that the integrity of justice is upheld in the face of new challenges and opportunities.

References:

1. Brian Leiter, 'Rethinking Legal Realism: Toward a Naturalised Jurisprudence' (1997) 76 Texas Law (Review 267, 301)
2. Dubey, V., "Admissibility of Electronic Evidence: An Indian Perspective," vol. 4, no. 2, 2017.
3. Harasta, J., "Trust by Discrimination: Technology Specific Regulation & Explainable AI," Proceedings of the EXplainable AI in Law Workshop (XAILA 2018) co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018), December 12th, 2018, Groningen, the Netherlands, pp. 2-8.
4. Pandey, K.A., VP Sarathi's Law of Evidence, Eastern Book Company, 2021.
5. Schafer, Burkhard & Mason, Stephen, The Characteristics of Electronic Evidence in Digital Format, in Electronic Evidence, LexisNexis, 2013.
6. Singh, Yatindra, Cyber laws, 2016.
7. Takwani, C.K., Indian Evidence Act, (1872), Whytes, 2021.
8. Whitcomb, C. M., "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," vol. 1, no. 1, 2002.
9. Section 3, The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).
10. Section 2(1)(t), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
11. <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbfgGhdfgFHYtyhRtMjk4NzY=>
12. <https://www.ijmh.org/wp-content/uploads/papers/v4i7/F0649024620.pdf>
13. https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf
14. <https://ijcrt.org/papers/IJCRT2205188.pdf>
15. <https://www.ijmh.org/wp-content/uploads/papers/v4i7/F0649024620.pdf>
16. https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf
17. <https://indiankanoon.org/doc/172105947/>

18. <https://www.aironline.in/legal-articles/Video%20Conferencing%20and%20the%20Law%20:%20An%20Analysis%20of%20a%20Landmark%20Judgement%20and%20its%20Consequences>
19. <https://updates.manupatra.com/roundup/contentssummary.aspx?iid=12894>
20. <https://indiankanoon.org/doc/187283766/>
21. <https://main.sci.gov.in/jonew/judis/27092.pdf>
22. <https://indiankanoon.org/doc/1611925/>
23. <https://www.casemine.com/judgement/in/5609af58e4b01497114161f4>
24. <https://indiankanoon.org/doc/22898/>
25. <https://indiankanoon.org/doc/193239104/>
26. MANU/SC/0057/2015
27. MANU/SC/0058/2018
28. MANU/SC/0521/2020
29. MANU/SC/0834/2014
30. MANU/SC/0176/1985: 1985 (Supp) SCC 611.