International Journal of Early Childhood Special Education (INT-JECSE)
DOI: 10.48047/INTJECSE/V14I1.531 ISSN: 1308-5581 Vol 14, Issue 01 2022 PP: 4282-4288

Admissibility of Digital Evidence

Mansi Singh, Research Scholar,
Faculty of Law & Governance Jayoti Vidyapeeth Women's University, Jaipur
mansisingh14@yahoo.com
8826687141

Abstract
The proliferation of computers and digitalization has brought about significant and transformative changes in society. However, like other aspects of human life, cyberspace is not immune to risks and criminal activities. The abundance of content and information, coupled with easy and widespread accessibility, has led to an increase in misuse of the cyber environment. This misuse has raised concerns about the authenticity and reliability of electronic texts, as they are susceptible to distortion.

When it comes to electronic evidence, law enforcement organisations have unique hurdles since its legitimacy is routinely called into question. Electronic evidence, unlike traditional types of evidence, demands specialised training and competence in the domain of cyberspace. As a result, the procedures used for researching and analysing electronically stored or obtained material are critical for presenting such evidence in court.

In this paper, we aim to examine and assess the validity of electronic evidence within the context of judicial pronouncements and legal requirements. We will analyze the factors that impact the acceptance and the admissibility of the electronic evidences in the court of law, considering the unique challenges it presents.

Keywords: Indian Evidence Act, Evidence, Digital/Electronic Evidence, Admissibility, IT Act

Research Methodology

This research paper on the admissibility of electronic evidence involves a systematic approach to investigate the topic. Firstly, a comprehensive literature review will be conducted to explore existing knowledge and legal frameworks surrounding the admissibility of electronic evidence. Relevant academic papers, legal articles, books, and case studies will be reviewed to gain insights into the current state of the field. This step will help identify key concepts, legal principles, and precedents that shape the admissibility of electronic evidence in different jurisdictions.

Following the literature review, a doctrinal research approach will be employed, focusing on legal provisions, legislation, and case law. Primary sources, such as legal statutes, court decisions, and legal guidelines, will be analyzed to understand the legal requirements and standards for admitting electronic evidence in court. This analysis will involve interpreting legal provisions, examining the application of legal principles in relevant cases, and identifying any gaps or inconsistencies in the existing legal framework. The research methodology will provide a structured and rigorous approach to examine the admissibility of an electronic evidence, contributing to knowledge in this field.

Introduction

Historically, evidence stored electronically has been treated as hearsay in the legal system, as there were no reliable methods to verify the accuracy of data stored in electronic or digital formats. In the present digital age, where technology permeates every aspect of our lives, the admissibility of digital evidence has become critical subject regarding concern within the legal realm. As society increasingly relies on digital interactions and transactions, legal disputes often involve the presentation and analysis of digital evidence, ranging from emails and social media posts to surveillance footage and computer-generated records. However, the unique characteristics of digital evidence present complex challenges in determining its admissibility in court proceedings.

The aim of this research paper is to explore the multifaceted landscape of digital evidence admissibility, shedding light on the key factors, considerations, and evolving legal frameworks that govern its acceptance within the judicial system. By examining the legal principles, precedents, and emerging trends, this study seeks to provide a comprehensive understanding of the hurdles and opportunities surrounding the admissibility of digital evidence.

Digital evidence, unlike traditional forms of evidence, possesses distinctive attributes that necessitate a specialized approach. The inherent characteristics of digital data, such as its ease of alteration, complexity, and vulnerability to tampering, raise questions about its reliability, authenticity, and integrity. Moreover, the dynamic nature of technology, which continually evolves and introduces new forms of communication and data storage, further complicates the assessment of any digital evidence in legal proceedings.

The admissibility of a digital evidence is influenced by a variety of factors, including statutory provisions, legal doctrines, and judicial guidelines. Rules of evidence that have traditionally governed paper-based documentation may require adaptation to accommodate the unique challenges posed by digital evidence. Additionally, legal systems across jurisdictions may differ in their approaches, creating a need for harmonization and uniformity in dealing with digital evidence on a global scale.

This research paper will delve into various aspects associated with the admissibility of digital evidence. It will explore topics such as the authentication and verification of digital evidence, chain of custody concerns, the role of expert witnesses, and the admissibility challenges posed by emerging technologies like blockchain, artificial intelligence, and deepfakes. Furthermore, it will examine landmark legal cases and the precedents they set, as well as the evolving legal frameworks and standards that courts and legislatures are developing to address these challenges.

By comprehensively analyzing the complexities and evolving nature of digital evidence admissibility, this research paper aims to contribute to the ongoing discourse surrounding the legal treatment of digital information. It endeavors to provide legal professionals, scholars, and policymakers with a deeper understanding of the issues at hand, fostering the development of effective strategies and guidelines to ensure the fair and just treatment of digital evidence in our increasingly digitized society.

Law on Digital Evidence

The fast growth of computer technology and the widespread use of information technology have prompted considerable modifications in legal frameworks across the world to accommodate the admission of digital evidence. In India, the introduction of digital evidence as a critical component of judicial procedures led the passage of The Information Technology Act, 2000. This Act amended numerous existing Indian legislation, including The Indian Evidence Act of 1872, The Indian Penal Code of 1860, and The Banker's Book Evidence Act of 1891, to handle the admissibility of digital evidence.

Types of Digital Evidence

Digital evidence encompasses a wide range of electronic data that holds significance in legal proceeding[1]s. These types of evidence play a crucial role in establishing facts, communication records, intentions, and other relevant information in a case. Here are some elaborations on the various types of digital evidence:

1. Emails: Emails are electronic messages exchanged through email platforms. They can serve as critical evidence in legal proceedings due to their ability to provide a clear record of communication between parties. Email evidence can establish the timing and content of conversations, as well as the intentions or agreements made by individuals involved in a case[2]. It is important to analyze email

[1] https://ujala.uk.gov.in/files/15.pdf

[2] M/s. Xact Studio International v M/s. Liwona SP. Z.O.O 2018 SCC OnLine Del 9469

DOI: 10.48047/INTJECSE/V14I1.531 ISSN: 1308-5581 Vol 14, Issue 01 2022 PP: 4282-4288

headers, attachments, and any digital signatures or encryption present to ensure the authenticity and integrity of the evidence.

2. Digital Documents: Digital documents, including word processing files, spreadsheets, PDFs, and presentations, have become the norm in today's digital age. These documents can be highly relevant as evidence, as they can contain crucial information, contracts, agreements, financial records, or any other documentation related to a case. Metadata associated with these documents, such as creation dates, authorship details, and revision history, can provide valuable insights into the document's authenticity and chain of custody.

3. Social Media Content: With the widespread use of social media platforms, user-generated content has become an important source of digital evidence. Social media posts, messages, comments, photos, and videos can offer significant insights into a person's activities, state of mind, relationships, or actions relevant to a case. Social media evidence requires careful consideration of privacy settings, authentication methods, and any possible alterations or manipulation of the content.

4. Computer Files and Metadata: Digital files, such as documents, images, videos, and audio recordings, hold immense evidentiary value. Metadata associated with these files, including file properties, timestamps, and geolocation data, can provide contextual information critical to understanding the origin, authenticity, and handling of the evidence. Metadata analysis, forensic examination of file attributes, and file hashing techniques can help establish the integrity and reliability of digital files.

5. Surveillance Footage: Surveillance footage captured by cameras, including CCTV systems, dashcams, or body-worn cameras, can provide visual evidence of events, activities, or individuals involved in a case. Such footage can be crucial in criminal investigations, accident reconstructions, or establishing the credibility of witness testimonies. The quality, timestamp accuracy, and chain of custody of surveillance footage are essential considerations for its admissibility in court.

6. Internet Browser History and Search Logs: Internet browser history and search logs can offer valuable insights into a person's online activities. They can reveal websites visited, searches conducted, online purchases made, or information sought. Internet browser history can be relevant in cases involving cybercrimes, online harassment, intellectual property disputes, or establishing a person's digital footprint. Authentication and preservation of browser history are crucial to ensure its admissibility and integrity.

7. Cell Phone Data: Cell phone data, including call logs, text messages, GPS location information, and app usage records, can be highly valuable in legal proceedings. This data can establish communication patterns, location information, timelines, or associations relevant to a case[3]. Analyzing cell phone data often requires expertise in mobile device forensics and the ability to extract, interpret, and authenticate the data for its admissibility in court.

8. Forensic Data: Forensic data refers to digital evidence collected and analyzed using specialized forensic techniques and tools. This includes recovering deleted files, uncovering hidden data, examining encrypted information, or analyzing any kind of data from computer hard drives, mobile devices, or any other storage media. Forensic analysis can provide critical evidence by revealing digital footprints, identifying user activities, or verifying the authenticity and integrity of a digital evidence.

Understanding the complexities of different types of any digital evidence is crucial for legal professionals, as it involves not only collecting and preserving the evidence but also effectively presenting it in court. It requires expertise in digital forensics, data analysis, authentication methods,

[3] Syed Asifuddin v State of Andhra Pradesh 2005 SCC OnLine AP 1100

DOI: 10.48047/INTJECSE/V14I1.531 ISSN: 1308-5581 Vol 14, Issue 01 2022 PP: 4282-4288

and adherence to legal standards to ensure the admissibility and credibility of digital evidence in legal proceedings.

Amendments in the Evidence Act
The Evidence Act has been amended several times throughout the years to keep up with substantial changes in the legal landscape. These amendments include measures addressing the admission of electronic records alongside traditional paper-based documentation.

Evidence
The definition of "evidence" has been amended to constitute electronic records, expanding on the conventional categories of oral and documentary evidence established in Section 3(a) of the Evidence Act. Similarly, the concept of "documentary evidence" has been broadened to include all forms of papers, including electronic recordings brought in court for inspection. The word "electronic records" is defined under the IT Act to include various types of electronically stored, received, or transmitted data, records, pictures, sounds, and other similar formats.

Admissions
To embrace a broader variety of remarks, Section 17 of The Evidence Act,1872 has been modified to redefine "admission." It now covers remarks made not just orally or in writing, but also electronically, as long as they indicate facts important to the subject matter. In addition, a new provision, Section 22A, has been added to the Evidence Act. This section focuses on the significance of spoken testimony in relation to the contents of electronic records. Oral confessions about electronic records are regarded significant only where the legitimacy of the given electronic records is in doubt or under dispute, according to this rule.

Statements as Part of the Electronic Records
As stated in the Section 39 of the Evidence Act, when a statement is embedded within an electronic record, the court is required to carefully assess the electronic record's evidence to gain a comprehensive understanding of the nature, significance, and context in which the statement was made. This clause applies to statements that are part of a bigger document, a dialogue, a single document, or a document that is part of a series of letters or documents.

Admissibilty of the Digital Evidence Under Indian Evidence Act 1872
The admissibility of digital evidence is a critical part of Indian law, which is controlled by the Indian Evidence Act, 1872. The Act establishes standards for the admission and examination of various sorts of evidence in court.

Section 3 of the Indian Evidence Act recognises four forms of evidence: documented evidence, oral evidence, main evidence, and secondary evidence. Sections 65A and 65B of the Act apply to digital evidence, which is a subset of documentary evidence.

Section 65A covers electronic record admissibility, saying that information included in an electronic record printed on paper or saved, recorded, or replicated on optical or magnetic media can be regarded a document and offered as evidence in court. The integrity of the electronic record, however, must be kept and authenticated in line with Section 65B.

The admissibility of electronic records as evidence is expressly addressed in Section 65B of the Indian Evidence Act. When electronic records are requested to be acknowledged, they must be accompanied by a certificate issued by the person in charge of the computer or equipment that generated the record. This certificate should affirm the circumstances surrounding the creation of the electronic record, as well as describe the procedure of making, storing, and retrieving the record.

Furthermore, the individual issuing the certificate must have the appropriate skills and meet the standards outlined in Section 79A of the Information Technology Act of 2000. The certificate establishes the validity and integrity of the electronic record, which is essential for its acceptance in

DOI: 10.48047/INTJECSE/V14I1.531 ISSN: 1308-5581 Vol 14, Issue 01 2022 PP: 4282-4288

court. It is vital to remember that the judge determines the admissibility and weight of digital evidence depending on the case's unique facts.

Finally, the Indian Evidence Act, namely Sections 65A and 65B, provide the legal basis for the admission of digital evidence in India, assuring its treatment on par with conventional forms of documented evidence, subject to certain circumstances and limitations.

This encompasses scenarios where the original document:

1. Is held by someone who is unfriendly or uncooperative.
2. Has been acknowledged or represented by the person who suffered harm or their authorized representative.
3. Has been misplaced or damaged.
4. If is difficult to transport, making it impractical to bring to the court physically.
5. If it a public document of the State.
6. Can it be established through authenticated copies when certain legal restrictions apply.
7. Consists of a compilation of multiple documents.

Authenticity Certificate

Section 65B(4) of the Evidence Act focuses on the non-technical requirements, notably the requirement of an authentication certificate. The primary goal of this certificate is to meet the requirements outlined in the previous sub-section (2) of Section 65B. It requires that the certificate be executed or signed by a person in a responsible position related to the equipment used to create the data. The certificate must precisely identify the electronic record holding the statement, describe how it was created, and provide relevant data about any equipment used in its development. These details help to prove that the record was created by a computer. Furthermore, the certificate must address any issues about the requirements for acceptance. The objective of this certificate is to confirm the data's integrity and validity, allowing the court to rely on it. This is critical because electronic data is vulnerable to manipulation and change.

Digital Evidence and Forensics

The usage of computers by both criminals and law enforcement organisations has changed the terrain of modern crime and investigation. As a result, the area of digital evidence forensics has emerged, which plays an important role in combatting computer-related crimes.

Digital evidence is information that has evidential value in judicial proceedings and is stored or communicated in binary format. It is present on a variety of devices, including computer hard drives and mobile phones. While digital evidence was first connected with electronic crimes such as child pornography or credit card fraud, it is today used to prosecute a wide range of criminal offences. Email communication or mobile phone data from suspects, for example, might reveal critical evidence about their intentions, locations during a crime, and relationships with other persons involved. A significant 2005 case included a floppy disc that led detectives to the BTK serial killer, who had eluded arrest since 1974 and was responsible for at least ten deaths.

To successfully combat electronic crime and acquire relevant digital evidence for all sorts of offences, law enforcement organisations are incorporating digital evidence collection and processing, often known as computer forensics, into their infrastructure. However, these agencies have difficulties in educating officers to handle digital evidence and keeping up with quickly expanding technologies, such as different computer operating systems.

As technology improves, the discipline of digital evidence forensics continues to expand, bringing both benefits and problems for law enforcement. As criminals' use of technology becomes more sophisticated, it is critical for investigators and forensic analysts to keep up to date on the newest innovations in digital evidence gathering and processing. They can successfully use digital evidence to bring offenders to justice and preserve the integrity of investigations in the digital era if they do so.

DOI: 10.48047/INTJECSE/V14I1.531 ISSN: 1308-5581 Vol 14, Issue 01 2022 PP: 4282-4288

Recent Judicial Precedents

In the case of **State of Punjab v Amritsar Beverages Ltd**[4], the Sales Tax Department conducted a search and seizure operation, confiscating computer hard disks and documents from the dealer's premises. The confiscation was authorised because of a clause in the Punjab General Sales Tax Act of 1948, especially Section 14. This part required the return of confiscated papers within a defined deadline, as well as the provision of a receipt to the dealer. The Sales Tax Authority, on the other hand, refused to return the hard disc, claiming that it did not meet the criteria of a document. The matter finally reached the Supreme Court, which took into consideration technological improvements since the Sales Tax Act's inception. The court found in a creative interpretation of the law that the Evidence Act should be viewed in the context of modern life, allowing for a flexible and imaginative approach. As a consequence, it was decided that officers should create copies of the hard disc or procure a hard copy, sign or seal it, and deliver a copy to the relevant party.

In the case of **Jagjit Singh v State of Haryana**[5], the Supreme Court examined digital evidence in the form of interview transcripts from various television channels. The court confirmed the admissibility of electronic evidence and supported the Speaker of the Legislative Assembly's reliance on recorded interviews in finding defection disqualification.

In **State (NCT of Delhi) v Navjot Sandhu**[6], a case related to the attack on Parliament, the admissibility of mobile telephone call records was at issue.The accused claimed that the phone records could not be considered credible since the prosecution failed to provide the required certificate as required by Section 65B(4) of the Evidence Act. The Supreme Court, on the other hand, determined that the authenticity of the call records may be proven by cross-examination of a witness who was knowledgeable with the operation of the computer system and the method of collecting the call data.

In **State of Maharashtra v Dr Praful B Desai**[7], the question of examining a witness via video conference arose. The Supreme Court recognised video conferencing as a technical innovation that allows for efficient distant communication that is comparable to being physically there. The court authorised a video conferencing examination of a witness, emphasising its relevance as an integral component of electronic evidence.

Subsequent High Court rulings, such as **Amitabh Bagchi v Ena Bagchi**[8], have followed this Supreme Court decision. The High Court of Andhra Pradesh, in **Bodala Murali Krishna v Bodala Prathima**[9], emphasized the need for precautions to ensure witness identification and the accuracy of the equipment used during video conferencing. Parties wishing to use video conferencing facilities must bear the associated expenses.

Conclusion

The implementation of the IT Act and subsequent amendments to the Evidence Act have had a notable impact on the utilization of electronic records in legal proceedings. However, despite the importance placed on certification in several judicial rulings, the practice of certification has become more customary than mandatory. The recent ruling in the case of Shafhi Mohammed by the High Court has raised doubts regarding the necessity of a certificate under Section 65B of the Evidence Act, highlighting the need for additional clarification from the judiciary.

As the cyber space continues to evolve, it is essential for the courts to adapt and keep pace with these changes. This adaptability is crucial to instill confidence in the use of electronic records while considering the practical aspects of their utilization. It is important for the courts to ensure that the legal framework surrounding electronic evidence remains up to date and relevant to the current cyber landscape.

[4] (2006) 7 SCC 607
[5] (2006) 11 SCC 1
[6] (2005) 11 SCC 600, AIR 2005 SC 3820, 2005 Cri LJ 3950, 122 (2005) DLT 194(SC).
[7] (2003) 4 SCC 601
[8] (2003) 4 SCC 601
[9] 2007 (2) ALD 72

DOI: 10.48047/INTJECSE/V14I1.531 ISSN: 1308-5581 Vol 14, Issue 01 2022 PP: 4282-4288

In addition to the certification requirement, there are other functional aspects that the courts should consider when dealing with electronic records. These include issues such as authentication, integrity, and the admissibility of specific types of electronic evidence, such as emails and social media content. Privacy concerns and data protection also play a significant role in determining the admissibility and reliability of electronic records.

To promote confidence in the use of electronic records, it is crucial for the courts to adopt a proactive approach. This can be achieved by staying updated on technological advancements, collaborating with experts in the field of cybersecurity and digital forensics, and conducting regular training programs for judges, lawyers, and court staff. By doing so, the courts can ensure a fair and efficient administration of justice in the digital age.

In conclusion, while the IT Act and the Amendments to the Evidence Act have paved a way for the use of electronic records in judicial proceedings, there are still challenges and areas that require further clarification and development. It is imperative for the courts to adapt to the evolving cyber space and address the functional aspects surrounding electronic evidence. By doing so, they can foster confidence and promote the effective use of electronic records in the pursuit of justice.

References

1. https://www.jetir.org/papers/JETIR2112501.pdf
2. https://ijirl.com/wp-content/uploads/2022/05/A-COMPARATIVE-ANALYSIS-OF-ADMISSIBILITY-AND-RELEVANCE-OF-ELECTRONIC-AND-DIGITAL-EVIDENCE-IN-CRIMINAL-CASES.pdf
3. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html
4. https://nij.ojp.gov/digital-evidence-and-forensics
5. https://jhany.com/wp-content/uploads/2020/09/authenticatingdigitalevidence.pdf
6. https://www.lexology.com/commentary/litigation/india/amarchand-mangaldas-suresh-a-shroff-co/digital-evidence-an-indian-perspective