Evidentiary Value of Digital Evidence

By,

SADAF WARSI

(Author)

B.A.LL.B (Hons.) 5th year

Aligarh Muslim University, Aligarh

Introduction

In today's rapidly evolving digital age, the concept of evidence has undergone a profound transformation. As the world becomes more interconnected and reliant on technology, the evidentiary landscape has expanded to encompass a new type of crucial information: digital evidence. Digital evidence, derived from electronic devices and online platforms, has become a cornerstone in modern investigations and legal proceedings, presenting an unprecedented level of insight into the activities, intentions, and interactions of individuals. This article delves into the evidentiary value of digital evidence, exploring its significance, challenges, and the transformative effect it has had on the realm of law and justice.

Definition of Evidence

Evidence is defined as either oral or documented in Section 3 of the Indian Evidence Act, 1872. Oral evidence refers to the statements that witnesses provide to the Honorable Court, whereas documentary evidence, which includes electronic recordings, is evidence that is presented to the

Court for review. If we look at it more closely, we can learn more about the kinds of evidence that are used in courts.

The evidence could be split as follows:

- Oral, or Documentary;
- Primary, or Secondary.

Primary and secondary evidence

Primary evidence: primary source of evidence is the document itself must be produced in order to produce the original electronic record.

Secondary evidence: Production of the computer output containing the electronic record; Certified copies or counterparts of documents that the party cannot provide in court, as well as the testimony of an expert or someone who has personally seen the document, constitute secondary evidence.

Legal precedent recognizes that Primary Evidence must take precedence over Secondary Evidence where it is available. The top court has allowed secondary evidence because it is frequently nearly impossible to present primary evidence in court due to its storage on hard drives, cloud servers, large servers, and other electronic data storages. The secondary evidence can be printed out, copied, or stored on any magnetic or optical material created by an electric instrument before the court. However, secondary evidence can only be admitted if it meets the requirements listed in section 65B of the Indian Evidence Act[1].

The Significance of Digital Evidence

Digital evidence, often referred to as electronic evidence, encompasses a wide range of data extracted from digital devices such as computers, smartphones, tablets, servers, and even Internet

[1] Indian Evidence Act,1872

of Things (IoT) devices. This can include emails, text messages, social media interactions, location data, financial transactions, browsing history, and more. What sets digital evidence apart is its inherent ability to create a detailed chronological record of an individual's actions and communications.

The evidentiary value of digital evidence lies in its ability to provide a clear and often irrefutable account of events, actions, and intentions. Unlike traditional forms of evidence, digital evidence is often difficult to manipulate or falsify, as it leaves a digital trail that is challenging to erase entirely. This digital trail, created as a consequence of routine digital interactions, forms the basis for investigations, court proceedings, and ultimately, the pursuit of justice.

Electronic documents as proof

The acceptability of secondary evidence in specific cases is specified under Section 65 of the Indian Evidence Act. The process for demonstrating the contents of electronic records that have been established under Section 65B is outlined in Section 65B. The Indian Evidence Act's Section 65B on the admissibility of electronic records states that any information pertaining to electronic records that is printed on paper or that has a copy made on an optical or magnetic medium is also considered secondary evidence if it meets the requirements outlined in that section. The original source of the information, which is an electronic device, is also admissible in any legal proceeding without the need for additional proof.

The following are the essential components of electronic evidence under the Indian Evidence Act:

1) The person who is legally permitted to have control over that electronic device should produce such produced information of electronic records.
2) This information must be stored while the person is acting normally over the course of their daily activities.
3) That person's daily routine has resulted in the electronic device storing that stored information about their activities.

4) To prevent any potential harm to its operation or to alter the veracity and correctness of its material contents, the aforementioned electronic equipment must be operational when storing or replicating such material information.
5) Any type of storage, copying, or creation of a counterpart of the information needed to be produced in court as electronic evidence must be free from any type of manual editing, manipulation, or distortion; only reliable and authentic material may be admitted as evidence in a court of law.

Various kinds of digital records

The Information Technology Act of 2008 provides a definition for electronic records, encompassing a broad spectrum of data forms. A few of them are CDs, DVDs, pen drives, hard drives, email, photographs, video, sound, and telephone recordings. The aforementioned electronic record formats address various constraints concerning their admission in a court of law and evidential value.

The value evidence is contingent upon the mode and manner of the electronic records' submission to the court. That is to say, if the electronic records are submitted in their original form, they are unquestionably more valuable; however, if you wish to submit a copy of the record on a different or comparable device, you must obtain a certificate for the court's admission and comply with the precedent set forth in Section 65b of the Indian Evidence Act.

Mobile phones are incredibly practical and resourceful technology devices. It assists the legal and investigative systems in obtaining crucial evidence by helping to track down locations, record calls, take photos and videos, and access numerous other technological resources. Electronic records from mobile phones are accepted if they are submitted in their original form, meaning the phone itself, which is the main source of calls and media. For their duplicated version recordings on another comparable or dissimilar device to be admitted in court, they must get a certificate and meet the prerequisites outlined in Section 65B of the Indian Evidence Act.

Email is acknowledged as a reliable and genuine source of information. Emails are typically submitted using printouts that are certified under Section 65B of the Indian Evidence Act.

Challenges and Authentication

While digital evidence holds immense potential, its integration into legal proceedings is not without challenges. One of the primary challenges is ensuring the authenticity and integrity of the evidence. As digital content can be easily copied, altered, or fabricated, questions often arise about the accuracy and credibility of the information presented in court. To address this, stringent authentication processes are required to verify that the digital evidence presented is indeed genuine and untampered.

Digital forensics, a specialized field that involves the collection, preservation, and analysis of digital evidence, plays a pivotal role in addressing these challenges. Through advanced techniques and tools, digital forensics experts can examine the metadata, timestamps, and digital footprints associated with the evidence to establish its authenticity and chain of custody. Encryption, hashing, and secure data storage are also employed to ensure the evidence remains unaltered.

Transforming Legal Practices

The advent of digital evidence has significantly impacted legal practices across the globe. It has revolutionized the way investigations are conducted, enabling law enforcement agencies to gather comprehensive insights into criminal activities and patterns. For instance, in cases of cybercrime, digital evidence can help identify hackers, trace financial transactions, and reconstruct the sequence of events leading to a breach.

Similarly, in civil litigation, digital evidence has become indispensable. Electronic communication records can provide crucial evidence in contractual disputes, intellectual property cases, and employment claims. Social media interactions and online postings have also emerged as key elements in cases involving defamation, harassment, and character assassination.

Prominent case law related to evidentiary value of electronic evidence-

1. ***State of Maharashtra v. Dr. Praful B. Desai*** [2]

This case highlighted the need for electronic evidence to be proven through expert opinion and proper documentation to establish its authenticity and reliability.

2. ***State (NCT of Delhi) vs Navjot Sandhu alias Afsan Guru*** [3]

In this case, the Supreme Court discussed the importance of maintaining the integrity of electronic evidence and ensuring proper chain of cstody to establish its authenticity.

3. ***Anvar P.V. vs P.K. Basheer & Ors.***[4]

This case discussed the admissibility of electronic records under the Indian Evidence Act, 1872. It emphasized that electronic evidence, including emails and electronic documents, should be proved in accordance with the provisions of the Evidence Act.

[2] (2003) 4 SCC 601

[3] (2005) 11 SCC 600

[4] (2014) 10 SCC 473

According to the Supreme Court, secondary data on CDs, DVDs, and pen drives can only be admitted with a certificate under Section 65B(4) of the Indian Evidence Act. Oral testimony is insufficient to support electronic evidence; a certificate under Section 65B is required. Furthermore, the expert's opinion under Section 45A of the Indian Evidence Act does not serve as a means of avoiding the Section 65b procedure.

4. ***State of Punjab vs Baldev Singh***[5]

The Supreme Court reiterated the importance of adherence to the rules of the Indian Evidence Act while dealing with electronic evidence, and the need to establish the authenticity of such evidence.

5. ***State of Kerala vs Rasheed***[6]

The Supreme Court clarified the requirement of a certificate under Section 65B for electronic evidence and the consequences of not adhering to this requirement.

Privacy and Ethical Considerations

The rise of digital evidence also brings to the forefront complex ethical and privacy considerations. As digital evidence often involves personal information and private communications, the process of collecting, analyzing, and presenting such evidence must adhere to strict legal and ethical standards. Balancing the pursuit of justice with the protection of individuals' rights to privacy is a delicate task that legal professionals, lawmakers, and technologists must collaboratively address.

[5] (2015) 6 SCC 477
[6] (2019) 5 SCC 384

Conclusion

In an era where digital interactions permeate nearly every aspect of our lives, the evidentiary value of digital evidence is undeniable. Its ability to provide a detailed and often irrefutable account of events has transformed the way legal proceedings are conducted, allowing for more accurate and informed decisions. However, as with any powerful tool, digital evidence comes with its challenges, including authenticity, privacy, and ethical concerns. To harness its potential fully, legal systems must continue to evolve, incorporating technological advancements and innovative strategies while safeguarding the principles of justice and individual rights.