# THE IMPORTANCE OF DIGITAL FORENSICS IN THE ADMISSIBILITY OF DIGITAL EVIDENCE

Dr. Pratyusha Das[1] & Pradeepta Sarkar[2]
*Dean & Assistant Professor of Law, Xavier Law School, St. Xavier's University Kolkata, Email: pratyushadas@sxuk.edu.in*
*&*
*Barrister-at-law, member of Lincoln's Inn, Email: pradeepta24sarkar@gmail.com*

**Abstract**

*There is a paradigm shift in the notion of evidence in the modern era as increasing disputes are technical in nature and there is a voluminous increase in cybercrime. To cope with this situation, courts seek for electronic records for settling any dispute or proving an offence. However, due to the certain unique traits of electronic records or digital evidence, they are susceptible to misuse and thus result in abuse of the process of law which might lead to miscarriage of justice. Hence, it has to pass through the rigorous processes of admissibility. There are also various scientific methods which experts formulate to identify, retrieve, preserve and present such evidence in court. This process is known as "Digital Forensics". Initially, to frame a standard for admissibility was a difficult situation as it was susceptible to different interpretations. Presently, the law is more or less settled. However, there are certain variations in different jurisdictions. This article in Part A features an understanding of Digital Forensics and Digital Evidence. It also focusses on how digital evidence may be used in law enforcement. The section details the step-by-step process followed by digital forensic analysts to present evidence in court. Part B, highlights the admissibility criteria of digital evidence in the UK and India. The article mainly focuses on the law in India, as found in the Indian Evidence Act and also explores key case law findings that have shaped the admissibility of digital evidence in India to date. The concluding remarks draws a brief comparison between the state of admissibility of digital evidence in India and UK as well as the opinions of several scholars and judges on this issue.*

**Keywords:** Digital Forensics, Digital Evidence, miscarriage of justice, Indian Evidence Act, electronic records

## Introduction

In the modern era, the metaphysical digital world is just as big a part of our lives as the real world itself. Various social, administrative and economic activities now take place in the digital

space. This means that it has also become a hotbed for criminal activity. With the growing number of digital offences increasing dramatically, modern criminal cases and investigations require the use of digital evidence. It provides an exclusive window to access the correspondences of companies or individuals from the data and statistics that can be generated using the huge amount of information which might not have been possible to record on pen and paper. [1]As Oliver Leroux stated in the International Review of Law, Computers, and Technology "The gathering, conservation, communication and presentation of the computer-derived evidence must fulfil legal requirements with regard to the admissibility of the evidence…It is therefore essential to ensure…that computer-related evidence was collected, preserved and transmitted in accordance with legal requirements…"[2] This is what Digital Forensics enables us to do and why it is an important field to integrate into any legal system as "the value of digital evidence has exploded globally".[3]

This article has been divided in to two sections. Section A deals with defining digital forensics and digital evidence in layman's terms and go over some of the key aspects of both concepts. Section B of the article deals with how the digital evidence produced by the forensic process is admissible for use by courts in India and for comparison, how the UK legal system has integrated the admission and use of digital evidence

**Section A: Understanding Digital Forensics and Digital Evidence.**

**Defining Digital Forensics**

The term digital forensics can be interchanged with the term computer forensics or cyber forensics[4] as it is the art and science of applying computer science to aid the scientific and legal process. It is a relatively new field that combines elements of computer science and law to collect and analyse data from computer systems, networks, wireless communications[5], which is admissible as evidence before a court of law[6]. Put simply, digital forensics is the process of recovering evidence from digital media. It is the examination of computers, cyberspace, and

[1] Professor U Sieber 'Legal aspects of computer-related crime in the information society—COMCRIME study'.
[2] Olivier Leroux (2004) Legal admissibility of electronic evidence, International Review of Law, Computers & Technology, 18:2, 193-220, DOI: 10.1080/1360086042000223508 [https://doi.org/10.1080/1360086042000223508] (Last accessed Jan. 10, 2022)
[3] Losavio MM, Pastukov P, Polyakova S, Zhang X, Chow KP, Koltay A, James J, Ortiz ME (2019) The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. Wiley Interdiscip Rev Forensic Sci 1(5):e1337
[4] An Investigation Into Computer Forensic Tools." In ISSA, 2004, pg. 1-11.
[5]Dahbur, Kamal, Bassil Mohammad, The Anti-Forensics Challenge, 2011, at 1-7
[6]Ries, David G, Clark Hill PLC. "Digital Forensics in the Courts." (2017).

other electronic devices for evidence, in a forensically sound manner with the aim of identifying, preserving, recovering, analysing, and presenting facts and opinions about that evidence.

It is a broad field which is constantly evolving. Nowadays tablets, smartphones and flash drives are common and depending on the type of device, media or artifacts, this field has branched into various forms of forensics encircling computer forensics such as System Forensics, Network Forensics, Web Forensics, Data Forensics, Proactive Forensics, E-mail Forensics, Enterprise Forensics, Cyber Forensics, Digital Forensics.

There are three main types of investigations, and they differ in terms of the legal restrictions and guidelines as well as the type of digital evidence that is dealt with and the ultimate report that is made after concluding the investigation.

1) Criminal Forensics - The first and the largest form of digital forensics is criminal forensics. This is usually undergone as part of a larger law enforcement investigation. The aim is to extract intact digital evidence for use in trials where an expert report and testimony is given that can be understood by the jury and provide relevant facts that can help them make their decision.

2) Intelligence Gathering -. Similar to the first, this is also in relation to criminal activity, but the aim is to provide information that can track, stop or identify criminal activity. Unlike the first type, forensic soundness is less of a requirement unless this evidence is to be later used in court.

3) Electronic Discovery/eDiscovery – This is like criminal forensic but is used in civil cases. There are usually more legal limitations and restrictions on the scope of these investigations due to various privacy and human rights laws that are applicable in the jurisdiction.

**Defining Digital Evidence**

Digital evidence has been defined by the council of Europe as “any evidence obtained from data contained in or created by any device, the operation of which depends on software or data stored or transmitted through a computer system or network”[7] This definition provides much

[7] Council of Europe (2019) Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings < https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c> (Last accessed Jan. 10, 2022)

clarity as it not only includes digitally born evidence but recognises data which during its life is transformed and then stored or exchanged in electronic form as digital evidence as well.

Digital Evidence provides unique challenges separate from traditional evidence due to the key characteristics unique to this type of evidence.

- The first issue is the intangible nature of the evidence. Unlike visible and corporeal objects of proof, the evidence is invisible and intangible which opens several practical and legal issues. Digital data is extremely volatile as digital documents, logs and records can easily be altered by a few simple keystrokes and this can be done without leaving manifest traces. For example, by changing the internal clock in a laptop, one can change the time a document was created.
- Secondly, this also means this data is sensitive and prone to destruction. Improper or inexperienced handling of digital evidence can lead to its complete loss, such as data being lost on hard drives via electromagnetic forces within the storage units of police stations. Investigators often have to recover data that has been deleted and the Court has to believe that the data retrieved by investigators are in fact legitimate and untampered. "This is the reason why the computer and its media must be handled in a way that ensures that no possible evidence is damaged, destroyed or altered."[8] This creates a high skill ceiling barrier as only forensic experts, those trained in both the law and computer science can handle such data and exposure to untrained parties leads to the evidence becoming polluted and unusable.
- Finally, digital data is easily transferrable and highly mobile. This makes it very easy for confidential digital evidence to be leaked to the public or transferred to malicious parties, which can bias juries and lead to mistrials and ultimately result in the evidence being inadmissible or discarded despite its relevance.

**The Principles of Digital Forensics in Handling Digital Evidence**

As outlined above, due to the issues caused by the nature of digital evidence, for such evidence to be used in court, certain standards need to be maintained. As Olivier Leroux has emphasised, "these particularities do not exempt the electronic evidence from legal requirements relating to the evidence in the real world. Computer-derived evidence must have all attributes of

[8] Olivier Leroux, *supra* note 2

conventional evidence"[9] There have been efforts to make internationally accepted principles which applies to India as well. Moussa has concluded after extensive research into various international best practices such as those in the guidelines of the council of Europe that there are two key principles – "first, the electronic evidence must be legally obtained based on written permission from the competent investigation authorities; second, it must be verified as valid by computer science and information technology experts."[10] This can be rephrased as two key principles, authenticity, and accountability.

1) **Authenticity**– Evidence must be collected in a way that does not allow alteration of crucial data. To prevent contamination:[11]

    - All files in a computer system that are not encrypted are copied and only copies of the data are worked on. Copy is made using software specifically designed for such purposes.
    - Any deleted information is retrieved and copied to an external source.
    - Contents of hidden files are revealed using specific software to identify hidden data and protected files are decrypted and accessed.
    - Inaccessible parts of computer disks are analysed to locate files that could contain crucial data.
    - Only professionals and experts should have access to original digital evidence.

**Accountability** – To maintain accountability, all steps of the procedure are documented. The process of obtaining and verifying electronic evidence which consists of access, seizure, storage, and transfer should be documented and reported, conserved, and made available for inspection. Sometimes individuals or agencies oversee the production of technical report. The report aids the court to evaluate the evidence and decide the matter. The report is supplemented by expert testimony which provides the reasoning behind the authors findings and allows for cross examination. All this maintains a 'chain of custody' which essentially allows courts to be sure of the fact that the data was handled by individuals who can be held accountable.

[9] Olivier Leroux (2004) Legal admissibility of electronic evidence , International Review of Law, Computers & Technology, 18:2, 193-220, DOI: 10.1080/1360086042000223508 [https://doi.org/10.1080/1360086042000223508] (Last accessed Jan. 10, 2022)

[10] Moussa, A.F. Electronic evidence and its authenticity in forensic evidence. *Egypt J Forensic Sci* **11,** 20 (2021). https://doi.org/10.1186/s41935-021-00234-6

[11] IvyPanda. (2018, November 28). *Computer Forensics and Other Information Technologies. Principles of Computer Forensics.* https://ivypanda.com/essays/computer-forensics-and-other-information-technologies-principles-of-computer-forensics/

## THE PROCESS TO UPHOLD THE PRINCIPLES

As we can see, the forensic process with regards to digital evidence must be tightly controlled to adhere to the principles mentioned above. The process can be broken down into steps as shown by the image below.[12]

In the 'Identification' phase, depending on the type of forensic investigation, the purpose and resource requirement will vary. In criminal forensic matters there may be multiple possible crime scenes, each scene with a multitude of devices. The first step is to identify all the potential digital media that could contain digital evidence. A single investigation may need to cover phones, tablets, laptops, cloud storage spaces, routers, hard drives, USB, etc.

The second phase 'Preservation' is one of the most important ones as it is at this stage that investigators need to acquire the identified devices in a manner that maintains the integrity of the evidence and store it in a way that prevents contamination. Once a valid warrant from the court or permission from the owner of the devices is obtained, the investigator must decide how each device, which is running, or which is static is to be dealt with. If the device is static a bit-to-bit copy of the data is to be made. This bit copy is obtained through specialist tools that prevent modification during the collection. These devices that stop modification are called write blockers. These can be hardware or software. Hardware devices are considered more reliable and are becoming industry standard. This copy is what the next phase, analysis takes place on. Working from a copy and not the original is one of the fundamental steps to making the forensic audit acceptable to the courts. After acquisition there needs to be verification and by leaving the original device and the evidence as it was found, the copies or forensic images that were made can later be verified and shown to be accurate. A common method to show that a forensic image or copy of the evidence is the same as the original is through hashing. Forensic tools are used to create a verification hash (MD5, SHA 256) of the media, and this creates a unique mathematical algorithm that produces a unique value. Any changes made to the data in the forensic image/copy will result in a different hash from the original digital evidence. If both the original and image produce the same hash value, then the accuracy of the image is verified

---

**[12] Lawrence Williams, What is Digital Forensics? History, Process, Types, Challenges [10 September 2021],<https://www.guru99.com/digital-forensics.html>**

in court. Forensic images are put into secure storage, and this can be via various proprietary formats, a popular one being "Encase Evidence File Format" (EEFF) or RAW.

The third phase, 'Analysis' is the most time consuming. The copy is verified again, and deleted files are checked for and recovered, timelines are established and the time zone setting of the suspected device is checked, a keyword list is made to make the search for evidence quicker. It requires an individual with special skills that have an investigative mind to find relevant digital evidence to support a case theory. The technicality of this phase is a topic that is beyond the scope of regular lawyers and law enforcement.

The fourth phase, 'documentation' is an ongoing step. A creation of all visible data is to be made. Crime scene may be recreated and reviewed through this process. Documentation includes crime scene photographing, sketching and crime-scene mapping. The stage is essential in proving authenticity to the court as any challenge as to the handling of the digital evidence is resolved using this documentation.

The final part is presentation. In criminal cases, normally simple factual conclusions are presented, in a manner that is digestible to common people and speculative assessments are left for law enforcement. The contents of a common forensic report are "glossary with explanations of all technical terms, the analysis and its description and summary of findings." Expert testimony is provided by the author in support of the report being presented.

**Application in Law Enforcement**

Digital forensics is critical to law enforcement in resolving conflicts in both civil and criminal cases by providing vital and relevant evidence. Examples of its applicability in civil cases include those involving Intellectual Property theft, Industrial espionage, Employment disputes, Bankruptcy investigations, etc. Examples of its applicability in criminal cases include cybercrimes such as unauthorised hacking, theft of data, Digital Fraud investigations, Cyber terrorism, DDOS attacks, etc. As Moussa states in his findings, "Cybercrimes are among the most serious criminal activity of the present day."[13]

[13] Moussa, A.F. Electronic evidence and its authenticity in forensic evidence. *Egypt J Forensic Sci* **11,** 20 (2021). https://doi.org/10.1186/s41935-021-00234-6

Evidence adduced can have a wide variety of uses due to the diversity of data that can be obtained from devices nowadays. These applications are listed below[14]

**Attribution –** Digital data helps in identification of an individual from the personal documents found on the computer drive. In the famous case of the BTK Killer from Wichita, Kansas, USA, the use of digital forensics allowed law enforcement, who thought he was dead, to be able to obtain a drive from the serial killer in the early 2000s as he left an intentional trail for police to follow, proving he was still alive.[15]

**Alibis and statements -** Digital Evidence can assist in confirming the validity of alibis or witness statements. For example, mobile phone logs can prove whether a person was out of the country during a particular time.

**Intent -** Sometimes digital evidence can be used towards establishing mens rea as well. The social media posts of a person, as well as internet search histories can provide indications as to what a person was thinking or looking in to before committing a crime. For example, there are many instances where killers look up guides to killing people or how to purchase illegal weapons.

**Evaluation of source and Document authentication –** To identify the origin of a certain piece of data file, artifacts and meta-data can be used. Figuring out whether a file was produced on the digital device being examined or obtained from elsewhere (e.g., the Internet) can be very important in criminal trials. In the same vein, it is important to understand when details in documents have been falsified. Meta data with digital documents can be easily modified and this can be crucial in many cases. The creation date of a file can be changed by fixing the computer clock or placing a digital signature for illegal authorization. Cyber Forensics can assist in such matters by validating the authenticity of important documents, which ultimately aids investigation and supplies evidence to the court of law.

**Section B – Approach to the Admissibility of Digital Evidence**

Hopefully, Section A has provided an outline on the concepts of digital forensic and digital evidence in a general sense. Section B intends to take a closer look at how these concepts work in practise. It would be prudent to note at this point that in commonwealth jurisdictions there

[14] Various. Eoghan Casey, *Handbook of Digital Forensics and Investigation*. Academic Press. ISBN 978-0-12-374267-4, pg – 567, 2009

[15] Rivera, A. (2018, February 12). *BTK Serial Killer: Power of Computer Forensics*. The Bakersfield Californian. Retrieved October 30, 2021, < https://www.bakersfield.com/kern-business-journal/btk-serial-killer-power-of-computer-forensics/article_dd8f0ad3-f833-50b6-8e25-dcf6d406d5c4.html.> (Last accessed Jan. 15, 2022)

are two core principles that present main barriers to the admissibility of digital evidence. They are the hearsay evidence rule and best evidence rule.

The Rule against hearsay essentially means a witness can testify to those facts which he had himself seen, heard, perceived or who holds the opinion himself. The statements of the witness are verified by cross-examination and any statement which is not firsthand is hearsay.

Since by nature the digital mediums which produce the digital evidence cannot be cross examined, the courts have always considered computer documents to be hearsay evidence and therefore inadmissible unless exceptions are made.

The Best evidence rule essentially means that greatest weight is given to evidence that is original. For computer documents the original is contained in the computer in electronic and magnetic form and the printouts are hearsay. While devices such as mobile phones, USBs and hard disks were producible as direct original evidence, it is not always possible to bring the device containing the original data as evidence to the court, such as with large cumbersome servers.

Let us now see how the law in India and the UK have evolved exceptions to admit digital evidence into the fold. This section will focus on Indian laws regarding digital evidence and comparisons will be made with the UK to offer a broader perspective. This is primarily because **Section 65B in The Indian Evidence Act, 1872** is taken from **Section 5 of the Civil Evidence Act 1968 in UK.**

**India – Admissibility of Digital Evidence**

The introduction of 'digital evidence' into our laws can be traced to the Information Technology Act, 2000 ("**IT Act**"). The IT Act along with the related amendments to the Indian Evidence Act 1872 ("**EA**") and the Indian Penal Code 1860 ("**IPC**") contain the bulk of statutory law relating to this type of evidence. Section 4 of the IT Act introduced the concept of electronic record and by virtue of Section 92 of the IT Act, EA was amended to include "electronic record", thereby allowing for admissibility of the digital evidence.

These provisions essentially created a dichotomy between the magnetic digital data contained on the device, which was the original and the copies produced from them. The electronic evidence retrieved by using cyber forensics is deemed to be the original document and the printed reproductions of the same are secondary evidence. Secondary evidence requires certification of authenticity by a competent authority who is subject to cross-examination. Section 65B of the EA deals exclusively with the admissibility of this 'secondary' digital

 ISSN: 2456-4605(O)

evidence. Since most digital evidence is of this nature, we should look at this section in more detail.

**Section 65B of the Indian Evidence Act**

Section 65B deals with admissibility of electronic evidence. According to sub-section (1) electronic records which are printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be also deemed to be a document if the conditions mentioned in this sub-section (2) are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, if:

- Information was produced during the regular course of activities by the person having a lawful control over the computer's use…
- The computer was operating properly, or the improper operation did not affect the electronic record or the accuracy of its contents.

The above conditions are to create a two-fold impact, firstly, to restrict and ensure the unauthorized use of data and secondly to confirm that the device was functioning properly so that the accuracy and genuineness of the reproduced data is maintained.

According to Section 65B sub-section (3) of the Indian Evidence Act, 1872 if the user uses a networked device for storing or processing information, all the devices in the same network would be considered as a single device. Sub-section (4) provides for a certificate of authenticity to be provided by a competent authority for the purpose of proof checking and authentication of the compliance to be maintained in the preceding sub sections.

Leading advocates at Khaitan & Co have authored that "The certificate is to be executed/signed by a person occupying a responsible position in relation to the device through which the data has been produced. The certificate must identify the electronic record containing the statement, describe the manner in which it was produced and also give such particulars of any device involved in the production of the electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer. The certificate must also deal with any of the matters to which the conditions for admissibility relate. The entire idea behind the certificate is also to ensure the integrity of the source and authenticity of the data, so that

the Court may be able to place reliance on it. This is critical since electronic data is more prone to tampering and alteration."[16]

The application of Section 65B has led to a few interpretations and issues and an examination of the case law will follow to highlight this.

**Case law on admissibility of digital evidence in India**

The leading case law on this is the judgement of "Arjun Panditrao"[17], which considered three key issues with regards to Section 65B of the EA. These are:

A) Whether or not section 65B constitutes the complete code in India as to the admissibility of secondary digital evidence,

B) Whether the requirement of a certificate was mandatory in all cases and

C) Finally at which stage of the proceedings in a criminal or civil trial would the certificate need be produced.

Dealing with issue A, initially in the case of State *(NCT of Delhi) v Navjot Sandhu @ Afzal Guru*, **[**(2005) 11 SCC 600], it was stated that secondary digital evidence could be adduced under other Sections of the EA, mainly Sections 63 and 65 of the EA. This could be done irrespective of compliance with the requirements of section 65B and even without a certificate as specified in subsection 4 of 65B. However, this was not what the legislature had intended and later in *Anvar PV v PK Basheer and Others* [(2014) 10 SCC 473, this decision was reversed, and it was held conclusively that documentary evidence in the form of an electronic record can be proved only in accordance with the procedure set out under Section 65B. It was confirmed in Arjun Panditrao that Anvar was the correct legal statement, and it could be concluded that section 65B was indeed the complete code on this matter.

Requirement B also generated many issues. The strict requirement imposed by Anvar meant that in cases where certificates need to be procured from a third party, the litigant is not in position to dictate the language of the Certificate. This in turn has led to bona fide litigants suffering on several occasions. Due to this, the Division Bench of the Supreme Court went against the three-Judge Bench judgment of Anvar P.V in the case of ***Shafhi Mohammed v.***

[16] Ajay Bhargava , Aseem Chaturvedi , Karan Gupta and Shivank Diddi, 'India: Use Of Electronic Evidence In Judicial Proceedings' <https://www.mondaq.com/india/trials-appeals-compensation/944810/use-of-electronic-evidence-in-judicial-proceedings >(Last accessed Jan. 15, 2022)

[17] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors* 2019 SCC OnLine SC 1553

***State of Himachal Pradesh*** 2018 (2) SCALE 235. The Supreme Court observed that "Sections 65-A and 65-B of the Evidence Act, 1872 cannot be held to be a complete code on the subject." It further held that "in a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded." This decision was decisively overturned in Arjun Panditrao and therefore the certification requirement remained mandatory and this was justified on the basis that the courts had significant coercive powers to demand certifications from the relevant authorities. Therefore the maxim of "The law does not compel a man to do that which he cannot possibly perform" was not contravened, as via requests to the courts, the mandatory certificate can be attained with assistance or the party liable to provide the certification may incur fines or imprisonment. Reference was made to powers under under Order XVI of the Civil Procedure Code, 1908 ("CPC") and the Code of Criminal Procedure, 1973 ("CrPC"), to summons to produce documents.

Arjun Pandit also confirmed that Oral evidence cannot be a substitute to the certificate under Section 65-B. The Court also clarified with regards to primary evidence that, "the requisite certificate in sub-section (4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, a computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him."

The third confusion, issue C, was regarding the time as to when the certificate under Section 65-B would be produced in evidence. In this regard contradictory positions were taken by the Supreme Court in the case of Anvar P.V. At one place it was observed that such certificate shall be presented to the court when the electronic record "is produced in evidence". The other view is that certificate shall be obtained at the time of "taking the document". The contrary observations of the Supreme Court has led to various interpretations. In **Paras Jain v. State of Rajasthan**[18], the High Court opined that a Certificate under section 65B is not required to be filed with the police report (chargesheet), however, the only necessity is to complete the procedure is to procure and submit the certificate before the admissibility of evidence is considered by the court. The court referred to various provisions of Code of Criminal Procedure, to arrive at such conclusion that documentary evidence may be produced which has not been submitted with charge sheet.

[18] 2015 SCC Online Raj 8331

The Delhi High Court in the case ***Kundan Singh v. State***[19] of considered the same issue as Paras Jain's case, whether simultaneously certificate under section 65B can be issued with the production of computer output or whether the certificate be issued and produced when such document is admitted in evidence. The Division Bench observing P.V. Anvar held that it is not required to issue certificate simultaneously or contemporaneously. The Delhi High court distinguished admissibility and authenticity and clarified that section 65B deals with only admissibility and not authenticity as such there is no strict stage where the certificate must be produced.

It has been held the learned judges in Arjun Panditrao that "so long as the hearing in a trial is not yet over, the requisite certificate can be directed to be produced by the learned Judge at any stage, so that information contained in electronic record form can then be admitted and relied upon in evidence."

Thus, as the law currently stands, certification for secondary digital evidence is mandatory from forensic experts which can be called upon by the court in case of any questions as to authenticity if and when certification is not forthcoming, but this does not remove the prerequisite entirely. Let us now consider the legal position in the UK for comparison.

**UK Laws on Digital Evidence**

The law of evidence in the UK has recognised three types of computer-generated documentary evidence. The first type is 'real evidence', such as calculations or analyses generated by the computer itself. An example would be inbuilt clocks. Real evidence is admissible as direct evidence. In this respect, Smith (1981) wrote on computer evidence, and developed the ideas put forward in The Statue of Liberty [1968] 1 WLR 739 and crafted a rule which was later accepted by the courts. "Where information is recorded by mechanical means without the intervention of a human mind, the record made by the machine is admissible in evidence, provided of course, it is accepted that the machine is reliable." This was used in the case of Castlev. Cross [1985] 1 All ER 87. The prosecution sought to rely on a printout from a computerised breath-testing device. The Court held that the print-out was admissible evidence. The Court held that so long as it could be shown that the computer was functioning properly and was not misused, a computer record can be admitted as evidence.

[19] **(2016) 1 DLT (Cri.) 144**

Secondly, there are documents and records produced by the computer which are copies of information supplied to the computer by human beings. This evidence is treated as hearsay.

The third category of digital evidence is derived evidence which is information that combines real evidence with the information supplied by human beings to form a composite record. An example is the figure in the daily balance column of a bank statement since this is derived from 'real evidence' (automatically generated bank charges) and individual cheque and paying-in entries (supplied by human beings). This is also treated as hearsay evidence.

English case law has developed many exceptions to this rule so that the use of digital evidence is not so strictly limited. There are several exceptions to the hearsay evidence rule built into the UK legal system so that it can keep up with the growing need for digital forensic evidence in court. Several distinctions can be drawn from the strict requirement of certification found in Section 65B of the Indian Evidence Act.

In the provisions of general application, the Civil Evidence Act (1968) allows statements contained in electronic evidence to be admissible in civil proceedings regardless of how many removes there are between a copy and the original and it may be authenticated in a few simple ways as opposed to the stricter certification requirement in Indian law. For example, a document which was produced as part of the records of an ongoing business or public authority can be admitted without further proof or certification being required.

If a party cannot obtain an original piece of digital evidence the UK allows the admission of copies. This exception allows the removal of the obstacles created by the best evidence rule to the admissibility before the courts of computer documents. In order to deal with the specific issue of authenticity of electronic evidence in the courts of the UK, the British Standards Institute has published in 2008 a specific standard called Evidential weight and legal admissibility of electronic information. It ensures that any electronic information required as evidence of a business transaction is afforded the maximum evidential weight. India does not have similar standards integrated yet and this can be crucial in addressing some of the admissibility issues already discussed.

**Conclusion**

The acceptance of digital evidence in India can be seen through the admissibility of emails[20], call records[21], hard disks[22], statements of accounts[23] and more. However, by comparing the law as it stands in UK and India, it is clear that India lacks the flexibility and robustness enjoyed by our UK counterparts. As pointed out by the learned Authors at Khaiton & Co "a certificate under Section 65B of the Evidence Act neither does conclusively prove the facts contained in the electronic record nor amount to truth… despite various judicial precedents stressing on the importance of the certificate, the certificate has become a mere formality"[24]

The learned judge Ramasubramanian.J in Arjun Panditrao pointed out that "when our lawmakers passed the Information Technology Bill in the year 2000, adopting the language of Section 5 of the UK Civil Evidence Act, 1968 to a great extent, the said provision had already been repealed by the UK Civil Evidence Act, 1995 and even the Police and Criminal Evidence Act, 1984 was revamped by the 1999 Act to permit hearsay evidence, by repealing Section 69 of PACE, 1984." He concluded that "the major jurisdictions of the world have come to terms with the change of times and the development of technology and finetuned their legislations. Therefore, it is the need of the hour that there is a relook at Section 65B of the Indian Evidence Act, introduced 20 years ago, by Act 21 of 2000, and which has created a huge judicial turmoil."

Several other issues not discussed in Arjun Panditrao was highlighted by Stepehen Mason in light of the court's decision. He points out that in subsection 2(c) of 65B, the requirement of the computer "operating properly"[25] has not been defined by a single judge or item of legislation. This will inevitably become an issue at some point in the future. He also points to the lack of clarity in subsection 4 (c) of section 65B, "a responsible official position in relation to the operation of the relevant device or the management of the relevant activities." Arjun Panditrao provided some examples, however the matter is far from clear, as denoted by

[20] *Abdul Rahaman Kunji v. The State of West Bengal* 2014 SCC OnLine Cal 18816,
[21] *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600
[22] *Dharambir v Central Bureau of Investigation* 2008 SCC OnLine Del 336
[23] *Om Prakash v Central Bureau of Investigation (CBI)*, 2017 SCC OnLine Del 10249
[24] Ajay Bhargava , *supra* note 16
[25] *Stephen Masos* "Electronic Evidence and judicial consideration in India", Aug 12, 2021 | IALS, Legal News, Publications

 ISSN: 2456-4605(O)

Mason.[26] Another problem highlighted by the author was the incorrect presumption that computers are reliable.

It is evident that our laws on digital evidence must be ever evolving or risk falling behind the unwavering speed at which technology advances. It will be interesting to see where the law in India on digital evidence advances from here onwards.

[26] *Id.* at 25