Page 1507 - 1522 **DOI:** *https://doij.org/10.10000/IJLMH.114200*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 1

2023

Comparative Analysis of Digital Evidence in India and USA

NEHAA V.[1]

ABSTRACT

Most democratic nations build their legal systems on the idea that a person is innocent until proven guilty. The prosecution is responsible for establishing the accused's guilt beyond a reasonable doubt. Law, science, and technology are all dynamic and evolving with the advancement of society. Evidence is an essential component of every legal system in the administration of civil and criminal justice. We practically cannot survive without utilising digital devices in this digital age. It supports both domestic and international communication. Even the transactions, way of life, and employment of the majority of people now require technological devices.

E-commerce, digital information storage, and reliance on electronic forms of communication are all growing quickly worldwide. Regulations governing information technology and the use of digital evidence in both civil and criminal actions have developed as a result. E-evidence includes things like emails, digital pictures, ATM transaction records, papers, instant messaging histories, GPS tracks, digital video and audio files, and other kinds of digital data. These kinds of proof are potentially more expressive, more difficult to alter, and simple to copy. So, Conflicts and criminal activity are unavoidable in our technological age.

Using case laws and elucidations from India and the United States of America, this study attempts to analyse the laws governing digital evidence, its admission, and the significance and issues related to its admissibility. Finally, the precautions and practices that the Indian judiciary must implement while managing electronic evidence.

Keywords: *Digital evidence, Types, Admissibility, Relevancy, Challenges.*

I. INTRODUCTION

The type of evidence to be focused on is digital evidence which is also called electronic evidence or computer evidence. When the information of the physical world is transformed into binary numeric information like digital audio and digital photograph, the term digital is utilised. Data that could raise or lower doubts about the veracity of either party's version of the events and that is processed or saved. Information of probative value that may be relied upon in court that

[1] Author is a student at Tamil Nadu National Law University, Tiruchirappalli, India.

 [ISSN 2581-5369]

is kept or communicated in binary form is referred to as digital evidence. [2]

Digital evidence can be explained in the way that the data have been created or stored in electronic equipment like mobile phones, computers, smart TVs, etc. All electronic evidence that is joint with IoT technology is the probable basis of digital evidence and is vital for forensic investigations. To find the criminals and bring them before a court of law, forensics experts collect, identify, and preserve the evidence from various sources. Generally, computer forensic experts require digital evidence in cases, including gathering, protection, recovery, examination, and reporting.[3]

(A) Characteristics of Digital Evidence

- The below-mentioned aspects are the characteristics of Electronic Evidence.
- It is imperceptible by nature.
- It can be ruined or changed very easily.
- More protection is necessary to prohibit the alteration of electronic evidence.
- Specific tools and instruments are necessary to extract and protect the evidence.
- Special training is necessary to deal with this evidence.
- Producing electronic evidence in court testimony of an expert is essential.[4]

(B) Sources

- The External, Physical and Electronic sources are three different types of fundamental sources of electronic evidence.
- External source comprises social media data and the cloud.
- The Physical source consists of PDAs, Wristwatches, smartphones, computers, etc.
- The electronic source includes the records such as CDRs and server logs, emails etc.

The above-stated sources contain electronic evidence in date format. Even the smallest yet most important elements concerning data have been upheld as critical information in foreign courts.[5]

[2] Sathish Kumar P and Arya R, *A Study on Electronic Evidence Act under Law of Evidence*, 120 (5), IJPAM, 169 -182 (2018) url: http://www.acadpubl.eu/hub/

[3] Varsha Karbhari Sanap and Vanita Mane, *Comparative Study and Simulation of Digital Forensic Tools*, (ICAST 2015) 8 (2015)

[4] Dubey V. *Admissibility of electronic evidence: an Indian perspective*. Forensic Res Criminol Int J.4(2):58-63, (2017) DOI: 10.15406/frcij.2017.04.00109

[5] Jitendra Kumar Gautam & Dr. Yogendra Singh, *Proving Electronic Evidence in Court: A Challenge*, 6 I (II) AD VALOREM- JOL,39(2019).

 [ISSN 2581-5369]

(C) Types

In court, evidence is the foremost vital element to prove the facts. The information or data is gathered from electronic evidence gathered from two types of sources, namely

- Volatile or non-persistent

The data which cannot be reached if not connected to the computers, like the data available in devices like Hard disks and removable devices and the data that exist in these sorts of devices can easily be ruined. Memory that requires electricity to be stored its contents, such as RAM chips, is often referred to as volatile memory. In the event of a power outage, the content of memory is lost.

- Non-volatile or persistent

In this case, data is kept in memory permanently, and the absence of power does not destroy the data. For instance, information on a CD, DVD, cassette, or ROM (Read-only memory). (CISOMAG, n.d.) [6]

II. RELEVANCY AND ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA AND USA

India

The situation with the coronavirus has made it abundantly evident how essential electronic communication has become to both the public and business sectors. Documents and various digital evidence types are thus increasingly employed in both civil and criminal proceedings.[7]

(A) Indian Evidence Act 1872

- Evidence is defined in Section 3, which consists of written, verbal, and visual records created for the court's consideration. All records presented for verification by the Court were changed to All papers produced for the scrutiny of the Court, including electronic data.[8]
- The term "admission" has been redefined in accordance with Section 17 to include a remark made orally, in writing, or electronically that draws attention to a relevant fact.[9]
- Section 22-A permits the relevance of oral testimony with regard to the substance of

[6] *Nueangnong*, V.& Damsanit, P. *Issues of Credibility in Digital Evidence*. Rangsit JLS, 1(3), 60–74 (2022).
[7] Anshul Yadav, *Relevancy and Admissibility of Digital Evidence: A Comparative Study*, I(I) IJILR, 22 – 32 (2020) **https://www.ijilr.org/**
[8] Indian Evidence Act, 1872, Section 3
[9] Indian Evidence Act, 1872, Section 17

 [ISSN 2581-5369]

electronic documents. [10]

- Entries in the books of accounts, including those kept electronically, are covered under Section 34.[11]
- The provisions relating to digital evidence in India are also included in Section 45A, Section 136, Section 65A and 65 B, and the Second Schedule of the IT Act. [12]
- As per Section 5 of the Evidence Act, only relevant facts can be used as evidence, and other facts cannot be used.[13]
- Section – 136 authorises a judge to determine the acceptability of evidence.[14]
- According to section 65A, electronic evidence may be proven as per the provisions of section 65B's regulations. If the correspondent has access to the electronic record, Section 65B defines the types of electronic record which can be admitted as evidence without further justification of the production of the original.[15]
- If section 65 (B) applies, electronic evidence can be used as evidence in court. Based on the certificate, the legitimacy of the data may be easily demonstrated. According to section 65(B) said Act, the court must determine whether or not the document can be established to be authentic. If the conditions in the section are fulfilled, information in electronic form that is available in the forms mentioned in section 65(B) can also be considered as a document. These documents are admissible in any proceedings of the court without producing the original or any contents of the original.

(B) Conditions for the Admissibility of Electronic Evidence under Section 65(B)

For the admission of computer evidence, certain conditions are stated in section 65(B) of the act.

- The output received from the computer in the said period during which the computer is usually utilised to store the data, and the individual must have lawful control of the computer.
- During the aforementioned activities, the information therein derived was routinely

[10] Indian Evidence Act, 1872, Section 22A
[11] Indian Evidence Act, 1872, Section 34
[12] Chhatrapati, M. D., & Prasad, D. A. B. *Electronic Evidence–Admissibility and Authentication: A Judicial Perception of Apex Court of India*. 3(1) GLS Law Journal pp.1- 9 (2021). https://glslawjournal.in/index.php/glslawjournal/article/view/39
[13] Indian Evidence Act, 1872, Section 5
[14] Indian Evidence Act, 1872, Section 136
[15] Indian Evidence Act, 1872, Section 65 A and 65 B

 [ISSN 2581-5369]

input into the computer during the aforementioned period.

- In the period the computer must operate efficiently; if not, the period in which the computer was failure must be specified.
- The information in the electronic record must be originated from the ordinary course of action.[16]
- Section 65 B (4) highlights that a certificate must be presented for the originality of electronic evidence with the signature of an official responsible individual. The certificate must recognise the statement, the method in which the evidence presented must be specified, and information about the device needed to produce the electronic evidence, that is, the computer used for the production of the electronic record. [17]

(C) Judicial interpretation on Relevancy and Admissibility of Electronic Evidence

- **Anvar vs. Basheer[18]**

In this instance, the court determined that the Information Technology Act of 2000 added section 65B to the Evidence Act, and this section governs digital Evidence.

- **Ram Singh v. Col. Ram Singh[19]**

In these cases, certain rules have been put forth by the apex court for the admission of tape-recording evidence. The sound of the chatterer must be recognised by the individual who recorded it, and strict proof of the voice must exist. The Exactness of the evidence must be verified by the evidence, and tampering must not exist. The relevant evidence is only admissible, and the recording must be clear and auditable.

- **State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru[20]**

The defence raised the issue of acceptability and questioned the validity of the evidence on the mobile phone since the certificate mandated by section 65B was missing. The prosecution didn't produce a certificate. The Apex court held that the appropriate witness who was part of taking the print of the evidence had been examined, so the evidence is valid and admissible.

[16]Jain, Naman, *Admissibility of E-evidence in India: An Overview* (March 31, 2021) https://ssrn.com/abstract=3816724 or http://dx.doi.org/10.2139/ssrn.3816724
[17] Tejas D. Karia, *Digital Evidence: An Indian Perspective*, 5 Digital Evidence and Electronic Signature Law Review,214 – 220 (2008) https://ials.sas.ac.uk/
[18] (2014) 10 SCC 473.
[19] AIR 1986 SC3
[20] (2005) 11 SCC 600

 [ISSN 2581-5369]

- **Tukaram S. Dighole v. Manikrao Shivaji Kokate**[21]

As technology is developing speedily, necessary precautions must be taken during the admission of electronic evidence, as tampering with evidence can happen in an easy method.

- **Tomas Bruno v. State of U.P.** [22]

The court stated that when the whole issue depends on the vital problem, then the vital evidence need not be ignored. CCTV footage was vital evidence, and it has been found that there was a gap in the chain of circumstantial evidence. It has also been noted that this evidence was very vital and cannot be ignored. Sections 65A & 65B mandate the procedural need to be met. The certificate is not necessary for every piece of evidence. It was found that the evidence presented was authentic and reliable. The evidence should be collected promptly and must satisfy the court.

- **Shafi Mohammad v. State of H.P.**[23]

In this case, the court stated that a certificate is not necessary for the individual who does not have possession of the electronic evidence produced as the evidence. The necessity of the certificate may be waived in the interest of justice. Emphasis was made on delivering justice rather than following the procedure of the law.

- **State v. Mohd. Afzal and Ors** [24]

Here the court pointed out that electronic data produced via computer is admissible as electronic data in the trial if the progression under section 65(b) is accomplished.

- **State (NCT of Delhi) v Navjot Sandhu**[25]

A certificate related to the electronic evidence is presented in the said case; it does state that the evidence which is eligible to be produced in the court as per sections 63 and 65 need not be presented in the court.

(D) Analysis

Sections 65A and 65B constituted special legislation that supersedes the law of documentary evidence as per the Supreme Court presiding. The IT Act added a special clause known as "proof of electronic record" that modifies numerous sections.

[21] (2010) 4 SCC 329
[22] (2015) 7 SCC 178
[23] (2018) 2 SCC 801
[24] 2003 DLT 385.
[25] AIR 2005 SC 3820

 [ISSN 2581-5369]

- **Jagdeo Singh and Ors vs. The State of Maharashtra**[26]

In this instance, the court dealt with the admissibility of telephone intercepts in CDs and CDRs without a certificate required by section 65B of the said act. In the lack of a certificate, electronic evidence cannot be allowable.

In India, section 65B of the Indian Evidence Act must be followed for electronic evidence like emails, websites, or any other electronic record to be admissible in a civil or criminal prosecution. This was forced by the supreme court to maintain the reliability and worth of electronic records as they can be tampered with or altered very easily. Hence the computer record cannot be especially depended on. Indian Evidence act has to be amended to eliminate manipulation to ensure the basic legitimacy of the evidence of the electronic record by stating that this evidence needs to be created by the individual who has no connection or link to the proceedings and advocates must not have any control over the creation of the evidence. By adopting this method, the risk of manipulation of the record can be decreased. The burden of proving the writer of an article in order to ascertain if any changes or adjustments were made after the fact must fall on the proponent, according to the law, which also needs to be creatively addressed. Records were produced, the records' generation program's dependability and whether or if the records are comprehensive. Electronic evidence can easily alter, but this issue is not dealt with in section 65 B. For instance, an email sent while forwarding can easily edit. Mere providence of certificate by the third party cannot be depended upon for the authenticity of the evidence. Due to the manipulation of information, many issues have been arising in the modern developed world. It might be prudent for the government or courts to assemble a specialised group of digital evidence specialists to assist courts with regard to the preciseness of electronic data.[27]

USA

In the olden days, when there was no scientific equipment to testify to the genuineness of digital evidence, it was regarded as honest. But in the modern situation, with the growth and adoption of technology, digital evidence has become more common, and its usage is also applicable to committing crimes. With the development of electronic evidence, the requirement for the admissibility of stored information was raised in the USA. For instance, as per Federal Rules of Evidence 803(6),[28] electronic and digital is an exceptions to the hearsay evidence by which

[26] AIR 1981 SC 648
[27] Gokul Sundar. K. Ravi, *Relevancy of Electronic Records and its Admissibility in Criminal Proceedings*, https://www.academia.edu/14343081/
[28] FED. R. EVID. 803(6) (USA)

 [ISSN 2581-5369]

electronic evidence is admitted in American Courts.[29]

(A) Conditions for the Admissibility of Electronic Evidence

Certain principles have been made by the USA for the accepting of electronic evidence. They are

(B) Background Evidence

The electronic evidence is made as a part of a regular course of business which is utilised to sustain the facts and conclusion in the process of investigation. This includes, but is not restricted to, data retrieved from network devices like routers, authentication records such as physical access systems, and data management solutions, which in and of themselves comprise, but are not restricted to, backups, archives, or classification.[30]

- **Foreground Evidence**

This is the electronically stored evidence that has been made as a consequence of the object's communication or actions that directly aids the investigation and identify perpetrators. This type of evidence includes but is not limited to: Real-time monitoring systems, IPS systems, application software such as file integrity monitoring, business process systems, address books, electronic communication channels, etc.[31]

(C) Judicial interpretation on Relevancy and Admissibility of Electronic Evidence

In the USA trial court, electronic evidence is accepted. Computer-stored records, computer-generated data, social media postings, digital photos, website material etc., are examples of electronic evidence. It also includes electronic communications like emails etc.[32]

Judge Grimm, in his verdict in the case *Lorraine v. Markel American Insurance Company*,[33] has given a directive regarding the acceptability of electronic evidence. It is a model regarding the acceptability of electronic evidence. The following elements should be closely examined: the relevance of the electronic evidence is examined, accuracy, originality, whether duplicate supporting secondary evidence must exist, authenticity, and the protagonist must address any hearsay issues with the electronic evidence. These include determining whether the statement

[29] PAUL ROBERTS, ADRIAN ZUCKERMAN, (2004). CRIMINAL EVIDENCE. OXFORD UNIV. PRESS.
[30] STEPHEN MASON AND ALLISON STANFIELD, THE CHARACTERISTICS OF ELECTRONIC EVIDENCE, ELECTRONIC EVIDENCE, 18 – 34,University of London Press; Institute of Advanced Legal Studies,(2017) URL: https://www.jstor.org/stable/j.ctv512x65.9
[31] Prajwal Vasuki, *A Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence in Criminal Cases,* II (II) IJIRL 1 -11. (2022).
[32] Michael D. Gifford, *Admitting Electronic Evidence in Federal Court: I've Got All This Evidence Data – Now What Do I Do With It?* AM. B. ASS'N, 2 (2008), http://www.abanet.org/labor/basics/elist/papers/lied.pdf.
[33] Lorraine, 241 F.R.D. 534

is one made by the declarant and, if it is hearsay, deterring it from being used as evidence.[34]

- **Relevancy consideration**

Only appropriate evidence is admissible under federal rules of evidence; extraneous evidence is not. According to the definition, relevant evidence is any tendency to increase or decrease the likelihood that any fact that is significant to the resolve of the action is more true than it would be in the absence of the evidence. Logical relevance is dealt with in Rules 401 and 402 of the Federal rules of evidence.[35] It is not very difficult to show that evidence tends to confirm or refute any fact relevant to the decision on the action, as one might anticipate. The test for logical relevance stated by federal rules applies to electronic evidence the same as that of any traditional evidence. [36]

- **Pragmatic relevance**

If there is a risk of unfair bias, uncertainty over the issues, or jury misdirection, or if there would be an unreasonable delay or putting forth of superfluous presentation of cumulative evidence, the logically relevant evidence may be excluded from the trial. The focus of Federal Rule of Evidence Rule 403 is on the "pragmatic relevance" test, which addresses prejudicial bias. "Unfair prejudice" refers to an excessive propensity to make judgments frequently but not always on the basis of emotion.[37]

As per rule 403, electronic evidence is not admitted

- If the contents or language of the evidence is offensive.
- If the evidence has animation and exists, the possibility that the accurate act cannot be ascertained by the jury.
- Summarises extensive electronic writings, recordings, or images under Rule 1006.
- It may not be accurate or dependable.[38]

[34] STEPHEN MASON AND ALLISON STANFIELD, AUTHENTICATING ELECTRONIC EVIDENCE, ELECTRONIC EVIDENCE, 193 – 261.(2017) University of London Press; Institute of Advanced Legal Studies, URL: https://www.jstor.org/stable/j.ctv512x65.14

[35] FED. R. EVID. 401; FED. R. EVID. 402.(USA)

[36] Shiv N.S. *Scope of Electronic Evidence in India: A Comparative Study (UK, USA & Canada)* 24 Supremo Amicus [227] (2021)

[37] FED. R. EVID. 403

[38] GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation,2015.
https://www.rand.org/pubs/research_reports/RR890.html or https://www.jstor.org/stable/10.7249/j.ctt15sk8v3.1

- **Email and text messages**

In modern days all cases involve email and text messages. Such communication may be permitted if the sender acknowledges that he drafted or co-authored it. It is also admitted if the authentication by the service provider that the communication was transferred is provided. According to the New York Southern District Court, any residual questions regarding genuineness should go to the veracity of the evidence rather than its admissibility. Comparison of one email or text message to another provides authenticity to the issue.[39]

- **Website**

In accordance with Rule 901(b)(4), a petitioner may also certify the authenticity of a website if the printout establishes, in relation to circumstantial evidence, what it means to be.[40] Despite being an actual investigation, the equal of inspection Webpage outputs frequently differs depending on the specific website.[41]

III. ISSUES AND CHALLENGES IN THE ADMISSIBILITY OF DIGITAL EVIDENCE

India

There is various challenge to digital evidence. The experts who have the qualification and appropriate training are eligible to gather digital evidence. The assortment and maintenance of electronic evidence are much more difficult than the collection of actual evidence and are prevalent to many risks. The data stored is volatile and are predominant to alteration. The data in a phone may be altered by a software update, or suspects may delete their data from the cloud or wipe their phones clean to get rid of any traces of evidence. Conducting the investigation is very complicated for the investigator. Not only the analysis of the data but also acquiring the data from the devices also require expert knowledge and skills. Forensic experts must remain updated about the new alteration in the technology to examine the evidence.[42]

The important challenges are

- The rise in the use of PCs and wide range utilisation of the internet.
- Easy accessibility of the hacking tools.
- The absence of physical evidence enables the trial difficult.

[39] United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).
[40] Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 2 (2009).
[41] Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 Rich. J.L. & Tech 5 (2011). Available at: http://scholarship.richmond.edu/jolt/vol17/iss2/2
[42] Shweta and Tauseef Ahmad, *Relevancy and Admissibility of Digital Evidence: A Comparative Study*, **I**I (I), 1 – 9, IJLMH (2019), https://www.ijlmh.com/relevancy-and-admissibility-of-digitalevidence-a-comparative-study/

 [ISSN 2581-5369]

- The existence of a huge storage facility makes the investigation process too complex.
- Development and growth of the technology result in the alteration in the solution.

Currently, digital forensics is used to resolve a variety of instances involving copyright theft, industrial espionage, employment conflicts, fraudulent probes, inappropriate utilisation of the Internet and email at work, forgery-related issues, liquidation investigations, and problems regarding monitoring acquiescence.

(A) Advantage

There are many benefits to digital forensics. It guarantees the honesty of the computer system. The presentation of electronic evidence can also result in the punishment of the criminal. Cybercrime can be easily traced from any part of the world. It also aids in protecting the many and time of the institution. To prove the cybercrime activity in court, the evidence is gathered, processed, and analysed.

(B) Disadvantage

Storing electronic evidence is very costly, and it is also to be proved in court that there is no tampering with the evidence. Efficient computer knowledge must be possessed by Legal practitioners to present reliable and substantive evidence. The court can disprove the evidence if the tool specified is not as per the required standards. If the investigating officer does not have the required digital knowledge, then the anticipated result cannot be obtained. [43]

Even though there are numerous changes being made in India to reduce the number of records, nothing is completely unrestricted. India still has to determine a mechanism for conforming to the accuracy of electronic evidence, which is prone to multiplication by gaining access to the place it is being stored. The court must ensure that the evidence produced must be under the three vital necessities, namely authenticity, reliability, and integrity.[44]

Supreme court in a case stated the regulation for the permissibility of the digital evidence, the Courts of India could follow the constant approach and undergo all precautionary requirements for accepting and appreciating the evidence. (Anvar v. Basheer) still, there exists a gap in the law of India with the commencement of the investigation on the person based on the mere presentation of chats or images without ensuring the authenticity of the digital evidence to even start a prima facie case of criminal nature. This will apply to civil cases also, like consumer protection cases, there must exist the expert opinion and verification of the evidence for

[43] *Nueangnong*, V., & Damsanit, P. *Issues of Credibility in Digital Evidence*. Rangsit JLS, 1(3), 60–74 (2022).
[44] Lewulis, P. *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*. Crim Law Forum **33**, 39–62 (2022). https://doi.org/10.1007/s10609-021-09430-4.

 [ISSN 2581-5369]

relevance before the court. [45]

USA

- **Legal issues**

With the development in technology, law enforcement must create updated policies to resolve the problems related to digital evidence. Law enforcement must concentrate on the courts and prosecutors when developing the rules in order to ascertain the legal criteria for the chain of custody and admissibility.

- **Search and Seizure Issue**

Unreasonable Search and Seizure by government officials are prohibited by the fourth amendment with a certain exception. A search warrant must be gained by the officials before the search. If consent is provided by the appropriate party, then the warrantless search is allowed. Limited search can also be conducted in case of arrest and to the prevention of destruction of the evidence. Search warrant may not be required for evidence that is in clear sight of the officers. *Horton v California*, [46]electronic evidence storage is not permitted by this rule. There are two stages to gathering evidence with a search warrant.

Seizure of the divide which has the information is the first stage. The initial seizure might have to be extremely broad and include a lot of information that isn't covered by the search order, as recognized by the courts. Thus, the second stage which is examination is very essential to call for the particular information covered in the evidence. The files on the seized device are analysed. During such activity, additional information with is not covered under the existing scope can be found. [47]

Many laws have been passed by the congress of the USA to maintain a balance between the necessity of the 4th amendment and the requirement of the criminal investigation. There are 4 code which is relevant to the digital evidence.

A court with a proper justification can grant an order authenticating the inspection by enforcing the law. Without a court warrant if Government attempts to eavesdrop on communications. This may result in legal or criminal consequences, as well as the suppression of evidence. Restriction is placed on the collection of metadata from telephone and Internet communication by the Pen Registers and the Trap and Trace Device Statute. The Wiretap Act covers the matter of

[45] Prajwal Vasuki, *A Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence in Criminal Cases*, II (II) IJIRL 1 -11. (2022).
[46] *Horton v California*, 496 U.S. 128 (1990).
[47] Thomson, Lucy L., **Scitech Lawyer; Chicago**, *Mobile Devices: New Challenges For Admissibility Of Electronic Evidence*, 9(3), The SciTech Lawyer, 32 - 37 (2013).

 [ISSN 2581-5369]

communications, whereas the Pen/Trap Statute regulates various information viz. caller ID numbers, phone numbers called or received and email addresses. Law enforcement officials must obtain the prior permission of the court to look for communications metadata if no exception of the statute is applicable. [48]

IV. CONCLUSION

Digital evidence is recognised as the real relevant evidence in court by limitation exists in the laws in relation to the starting of an investigation against a person by the officials on the basis of mere presentation of chat or photo as evidence without ensuring the authenticity of contents of digital evidence. With the growth of the global world, the issues relating to digital evidence are increasing. To make digital evidence credible by international standards and reasonable and to acquire acceptance in the legal process, initiatives are being taken to build judicial forms and processes. Both Indian and USA laws are amended to reflect the necessary change. There exists a very minute distinction between primary and secondary evidence. But this distinction is made for documentary evidence, not for computer or digital evidence. As digital evidence is very complex and very complicated to be presented in tangible form, the required measure has to be taken by the legislature. It must also be remembered that it is not only difficult but also impossible to produce a word document in court on the same computer, so printouts and CDs should be accepted as primary evidence.

*****

[48] GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR890.html

 [ISSN 2581-5369]

V. REFERENCES

(A) PRIMARY SOURCES

CASES

- Anvar vs. Basheer (2014) 10 SCC 473.
- Ram Singh v. Col. Ram Singh AIR 1986 SC 3
- State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru (2005) 11 SCC 600
- Tukaram S. Dighole v. Manikrao Shivaji Kokate (2010) 4 SCC 329
- Tomas Bruno v. State of U.P. (2015) 7 SCC 178
- Shafi Mohammad v. State of H.P. (2018) 2 SCC 801
- State v. Mohd. Afzal and Ors 2003 DLT 385.
- Jagdeo Singh and Ors vs. The State of Maharashtra AIR 1981 SC 648
- State (NCT of Delhi) v Navjot Sandhu, AIR 2005 SC 3820
- Lorraine, 241 F.R.D. 534
- United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).
- Horton v California, 496 U.S. 128 (1990).

STATUTES

- Indian Evidence Act, 1872, Section 3
- Indian Evidence Act, 1872, Section 17
- Indian Evidence Act, 1872, Section 22A
- Indian Evidence Act, 1872, Section 34
- Indian Evidence Act, 1872, Section 5
- Indian Evidence Act, 1872, Section 136
- Indian Evidence Act, 1872, Section 65 A and 65 B
- FED. R. EVID. 401; FED. R. EVID. 402.(USA)
- FED. R. EVID. 803(6) (USA)
- FED. R. EVID. 403(USA)

 [ISSN 2581-5369]

(B) SECONDARY EVIDENCES

JOURNALS

1. Anshul Yadav, *Relevancy and Admissibility of Digital Evidence: A Comparative Study*, I(I) IJILR, 22 – 32 (2020) https://www.ijilr.org/
2. Chhatrapati, M. D., & Prasad, D. A. B. *Electronic Evidence–Admissibility and Authentication: A Judicial Perception of Apex Court of India*. 3(1) GLS Law Journal pp.1- 9(2021). https://glslawjournal.in/index.php/glslawjournal/article/view/39
3. Dubey V. *Admissibility of electronic evidence: an Indian perspective*. Forensic Res Criminol Int J.4(2):58-63, (2017) DOI: 10.15406/frcij.2017.04.00109
4. Gokul Sundar. K. Ravi, *Relevancy of Electronic Records and its Admissibility in Criminal Proceedings,* https://www.academia.edu/14343081/
5. Jain, Naman, *Admissibility of E-evidence in India: An Overview* (March 31, 2021) https://ssrn.com/abstract=3816724 or http://dx.doi.org/10.2139/ssrn.3816724
6. Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence,* 17 Rich. J.L. & Tech 5 (2011). Available at: http://scholarship.richmond.edu/jolt/vol17/iss2/2
7. Jitendra Kumar Gautam & Dr. Yogendra Singh, *Proving Electronic Evidence in Court: A Challenge,* 6 I (II) AD VALOREM- JOL,39(2019)
8. Lewulis, P. *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*. Crim Law Forum 33, 39–62 (2022). https://doi.org/10.1007/s10609-021-09430-4
9. Michael D. Gifford*, Admitting Electronic Evidence in Federal Court: I've Got All This Evidence Data – Now What Do I Do With It?*, AM. B. ASS'N, 2 (2008), http://www.abanet.org/labor/basics/elist/papers/lied.pdf
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. *Nueangnong*, V., & Damsanit, P. *Issues of Credibility in Digital Evidence*. Rangsit JLS, 1(3), 60–74 (2022).
12. Prajwal Vasuki, *A Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence in Criminal Cases,* II (II) IJIRL |pp. 1 -11. (2022) https://ijirl.com/volume-ii-issue-ii/

13. Sathish Kumar P and Arya R, *A Study on Electronic Evidence Act under Law of Evidence*, 120 (5), IJPAM, 169 -182 (2018) url: http://www.acadpubl.eu/hub/

14. Shiv N.S. *Scope of Electronic Evidence in India: A Comparative Study (UK, USA & Canada)* 24 Supremo Amicus [227] (2021)

15. Shweta and Tauseef Ahmad, *Relevancy and Admissibility of Digital Evidence: A Comparative Study*, II (I), 1 – 9, IJLMH (2019)**,**https://www.ijlmh.com/relevancy-and-admissibility-of-digitalevidence-a-comparative-study/

16. Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 2 (2009).

17. Tejas D. Karia, *Digital Evidence: An Indian Perspective*, 5 Digital Evidence and Electronic Signature Law Review,214 – 220 (2008) https://ials.sas.ac.uk/

18. Thomson, Lucy L., **Scitech Lawyer; Chicago**, *Mobile Devices: New Challenges For Admissibility Of Electronic Evidence,* 9(3), The SciTech Lawyer, 32 - 37 (Winter 2013).

19. Varsha Karbhari Sanap and Vanita Mane, *Comparative Study and Simulation of Digital Forensic Tools*, (ICAST 2015) 8 (2015).

BOOKS

1. GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR890.html

2. PAUL ROBERTS, ADRIAN ZUCKERMAN, (2004). CRIMINAL EVIDENCE. OXFORD UNIV. PRESS.

3. STEPHEN MASON AND ALLISON STANFIELD, AUTHENTICATING ELECTRONIC EVIDENCE, ELECTRONIC EVIDENCE, 193 – 261.(2017) University of London Press; Institute of Advanced Legal Studies, URL: https://www.jstor.org/stable/j.ctv512x65.14

4. STEPHEN MASON AND ALLISON STANFIELD, THE CHARACTERISTICS OF ELECTRONIC EVIDENCE, ELECTRONIC EVIDENCE, 18 – 34, University of London Press; Institute of Advanced Legal Studies, (2017) https://www.jstor.org/stable/j.ctv512x65.9

*****

 [ISSN 2581-5369]