LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Apr- June, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Apr- June, 2026

Lex Scripta Journal

Admissibility and Evidentiary Challenges of Digital Evidence in Criminal Trials in India: A Critical Legal Study

Authors
Wajida Naseem
Dr. Cheena Abrol

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

Admissibility and Evidentiary Challenges of Digital Evidence in Criminal Trials in India: A Critical Legal Study

Wajida Naseem
LLM -1year-criminal
CT university ferozpur road ludhiana
Registeration no: CTU2503002/72521373

Dr. Cheena Abrol
Supervised by Assistant Professor

Abstract
The digital age has revolutionized the entire investigation and prosecution process, whereby the foundation of evidence collection has evolved from tangible documentation to intangible data. In this research paper, an evaluation of the development of electronic evidence rules in India from the traditional provisions of the Indian Evidence Act of 1872 to the contemporary Bharatiya Sakshya Adhiniyam of 2023 is undertaken. Through critical analysis of the history of development of electronic evidence laws in India, characterized by the inconsistent judicial decisions surrounding mandatory Section 65B certifications, this study will examine the approach by which the BSA, 2023 attempts to update the legal framework for the classification of electronic documents under Section 57 (Explanations 4-7) as well as the secondary admission rules for electronic evidence under Section 63.
Through a qualitative research methodology, this study offers a comparative examination of legislative progress achieved in India vis-à-vis the United States Federal Rules of Evidence and the United Kingdom Police and Criminal Evidence Act 1984. This reveals an important friction within the system where there is the contradiction between the high-level standards that are expected to be fulfilled in India, such as the necessity to have cryptographic hash values and dual-signature certificate, with the reality on the ground where there are shortcomings in training in forensics, in maintaining the chain of custody, and a lack of registered cyber-examiners. Lastly, this paper suggests some recommendations on how the policy can address this issue, including the establishment of a standardized operational approach to forensics and training for both the courts and forensic officers.

Keywords: *Bharatiya Sakshya Adhiniyam, 2023; Section 63; Section 65B; Digital Evidence Admissibility; Cryptographic Hash Values; Chain of Custody; Comparative Cyber Forensics.*

1. Introduction

It is a common feature of the current digital age that the very nature of criminal acts has changed. Digital devices and virtual networks have become a key tool in carrying out conspiracy crimes, financial scams, cyber warfare launched by nation-states, terror acts, and inter-personal crimes. Hence, digital evidences such as emails, social media communications, database hosted on cloud infrastructure, coordinates, metadata of instant messaging application, and server logs have gained prominence and form the base of today's criminal investigation.

Regarding India, there has been a major change in the way of regulating electronic evidences since the enactment of Information Technology Act, 2000. The admission of digital records has been regulated by the elaborate and highly complicated process of Section 65B of the Indian Evidence Act, 1872.[1] From requiring an unambiguous mandatory certificate for the admissibility of digital records to being merely directory in nature in Shafhi Mohammad v. State of Himachal Pradesh[2] and again stringent in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,[3] the process was highly inconsistent and dependent on the opinion of the judges.

The introduction of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) aims to modernize the law in the field of cyberevidence.[4] The provisions of the BSA widen the scope of the term "documentary evidence" to include digital and electronic documents in Section 2(1)(d) and allow for oral evidence to be electronically captured. Notably, under Section 57 of the BSA, some specific types of electronic documents that are located within several files, temporary files, or originate from 'proper custody' are considered primary evidence.[5] In addition, while the procedural aspects of the previous Section 65B of the IEA have been incorporated into the Section 63 of the BSA, 2023, this section also includes stringent requirements for a dual-signature certificate procedure (for both the producing entity in Part A and a cyber forensics expert/system administrator in Part B), along with mandatory cryptographic hash values (SHA-1, SHA-256, MD5). While the BSA represents substantial progress from the legislative standpoint, its practical implementation poses a serious challenge to Indian law enforcement agencies. Law enforcement personnel working on first response calls do not necessarily have any cyber-forensic training resulting in compromised information flows, metadata corruption, and broken chain of

---

[1] Indian Evidence Act, 1872 (Act 1 of 1872).

[2] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801

[3] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

[44] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[5] *Id.*, s. 57.

custody. Additionally, Section 79A of the IT Act, 2000 does not recognize enough qualified cyber-examiners by the Government of India to make the new dual certification procedure feasible. This research critically investigates this friction between cutting-edge legislative mandates and the ground realities of India's criminal justice infrastructure.

1.1 Research Objectives

1. To trace the historical evolution of digital evidence admissibility in India, analyzing the transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023.
2. To conduct a structural analysis of Sections 57 and 63 of the BSA, evaluating how the new primary and secondary electronic evidence classifications affect judicial procedures.
3. To identify the systemic, infrastructural, and forensic challenges faced by Indian law enforcement agencies in complying with the technical mandates of the BSA.
4. To perform a comparative legal analysis of digital evidence admissibility standards in India, the United States, and the United Kingdom.
5. To formulate structural and legislative recommendations to bridge the gap between statutory standards and ground-level technical capabilities in India.

1.2 Research Questions

1. How did the persistent judicial contradictions surrounding Section 65B of the Indian Evidence Act, 1872 necessitate the statutory overhaul under the BSA, 2023?
2. To what extent does the categorization of decentralized digital storage as "primary evidence" under Section 57 of the BSA resolve the conceptual struggle between "originals" and "copies" in forensic computing?
3. What are the key forensic and infrastructural limitations in India that impede compliance with the dual-signature and cryptographic hash requirements of Section 63 of the BSA?
4. What legislative and operational lessons can India integrate from the Federal Rules of Evidence (United States) and the Police and Criminal Evidence Act, 1984 (United Kingdom) to optimize its digital forensic regime?

1.3 Research Methodology

This research is conducted using a doctrinal and analytical approach for qualitative research methodology. Domestic legislations, including the Bharatiya Sakshya Adhiniyam, 2023, Indian Evidence Act, 1872, and Information Technology Act, 2000, together with the relevant judicial precedents from the

Supreme Court of India, constitute the major source of primary data analysis. In terms of comparative legal analysis, foreign statutory sources, which include the United States Federal Rules of Evidence (FRE) and the United Kingdom Police and Criminal Evidence Act, 1984 (PACE), are considered.

Secondary sources of data analysis include reports from the Law Commission of India, scholarly commentaries such as Law of Evidence by Sarkar, scholarly articles on forensic sciences and law, as well as digital forensics standards internationally (for instance, ISO/IEC 27037). The collected data is subject to critical legal analysis to discern any internal contradictions among statutory rules, any inconsistencies among judicial decisions, and friction between legal requirements and technical capacities for cyber forensics.

1.4 Review of Literature

To establish a solid academic baseline, the existing literature is categorized into three core thematic areas:

A. The Classic Regime of Section 65B of the Indian Evidence Act, 1872

- **The Certificate Debate:** The early works concentrated on the statutory construction of Section 65B. Commentaries on the subject, such as Law of Evidence by Sarkar[6], had argued whether secondary electronic evidence could be established without any certificate at all. Early legal opinion believed that Section 65B was a complete code itself, thereby completely supplanting any secondary evidence provisions.
- **Judicial Oscillations:** The literature after State (NCT of Delhi) v. Navjot Sandhu[7] suggested that the relaxation of certification requirements undermined the authenticity of digital evidence since it permitted the oral evidence to be given without going through the technical procedure of verification. The later works have been critical of Anvar P.V[8]. since they suggest that the decision of Anvar P.V. takes a very technical approach, which resulted in ignoring the real evidences based on procedural lapses. Literature after Arjun Panditrao[9] pointed out that it is impossible to get certificates from the adversarial third party.

B. Cyber Forensics, Chain of Custody, and Technical Vulnerabilities

- **Technical Volatility:** The technical literature on digital forensics like Eoghan Casey's "Digital Evidence and Computer Crime"[10] states that digital files are inherently volatile and highly prone to manipulation/deletion/alteration which can't be traced. Absence of SOPs at

---

[6] P.C. Sarkar and M.C. Sarkar, *Law of Evidence* 1240 (LexisNexis, New Delhi, 15th edn., 2020).

[7] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

[8]

[9] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, *supra* note 4.

[10] Eoghan Casey, *Digital Evidence and Computer Crime* 89 (Academic Press, London, 3rd edn., 2011).

local police stations leads to compromising the integrity of the physical evidence during the act of search and seizure.

- **Grassroots Investigation Challenges in India**: The delay in FSLs has been noted by forensic and police administration researchers for quite some time now. It is standard practice to use hardware write-blockers during imaging in the forensic process; but according to the literature emerging from within the country, grassroots-level investigative officers do not even have access to write-blockers, thus merely by booting up the seized mobile/computer.[11]

C. The Transition to Bharatiya Sakshya Adhiniyam, 2023

- **The Primary Evidence Loophole:** New commentaries on the law with regards to the BSA raise a number of serious concerns about the possibility that evidence obtained via 'proper custody' be considered as primary evidence under Section 57(Explanation 5)[12]. Legal experts say that 'proper custody' can be highly subjective in police-controlled storage rooms (malkhanas), thereby posing the threat of admitting potentially compromised evidence devoid of the protection of a Section 63 certificate.

2. Historical Evolution of Digital Evidence: From IEA to BSA, 2023

2.1 The Pre-IT Act Era

Document Admissibility under the original 1872 Act

In order to establish the history of digital evidence in India, it is necessary to start with a deconstruction and analysis of the classical nineteenth century framework of the Indian Evidence Act, 1872 (hereinafter referred to as 'IEA'). Conceived by the Victorian era jurist Sir James Fitzjames Stephen, the Indian Evidence Act, 1872 was a major codification exercise intended to translocate, arrange, and simplify the extremely intricate and confusing rules of English common law in order to make them operational in the courts of British India.[13] The underlying philosophy of Stephen's draft was one of certainty, which was attained by the creation of a meticulous taxonomy based on the notions of relevancy and admissibility of evidence. The cornerstone of the nineteenth century statutory regime was the Best Evidence Rule a rule of common law requiring the production of the most authentic piece of evidence available.[14]

---

[11] G.S. Bajpai, "Scientific Investigation in Indian Criminal Justice: A Ground Reality Check" 12 *Indian Journal of Criminology* 45 (2021).

[12] S.S. Prasad, "Deciphering the Digital Trial: Challenges under Bharatiya Sakshya Adhiniyam" 66 *Journal of the Indian Law Institute* 45 (2024).

[13] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, *supra* note 32, at 41.

[14] Gaurav Bhawnani and Aditya Mehta, 'Admissibility and Proof of RTI Documents under the Indian Evidence Act' 32 *National Law School of India Review* 1 (2020).

'Document' means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter. [15]

The Failure of Traditional Oral and Physical Evidence Frameworks

One-way courts handled oldstyle tape recordings was by stretching meanings within the 1872 law. Yet moving from those fixed analog setups to scattered, unstable digital forms revealed how weak past rules really were. Tapes held steady waves on visible strips you could hold; digital data jumps in bits, vanishes fast, lacks form, spreads easily. That change broke longheld ideas about what counts as solid proof under the IEA's care requirements.

2.2 The IT Act, 2000 Amendments

Introduction and Intent behind Sections 65A and 65B of the IEA

Out of nowhere, the early 2000s saw global business and messaging shift fast fueled by the web, EDI, and digital links between machines. Because oldschool paperwork slowed down crossborder deals, UNCITRAL stepped in during 1996 with a sample law pushing countries to treat online messages as legally valid[16]. Riding that wave, India's lawmakers passed the IT Act in 2000 to cover everything from esignatures to hacking, shaping how digital exchange works under Indian law[17]

A single printout from a machine can stand as proof in court, if it meets what Section 65B(2) demands. Meeting those rules listed under subsections (a) to (d) keeps the system's trustworthiness intact. Only when the process stays unbroken does the result count as valid.

What matters most is how steadily the technology runs during creation: [18]

- The computer output containing the information must have been produced by the computer during a period when the device was used regularly to store or process information for the purposes of any activities regularly carried on by a person having lawful control over the computer;[19]
- During that period, information of the kind contained in the electronic record was regularly fed into the computer in the ordinary course of those activities;[20]
- Throughout the material part of the period, the computer must have been operating properly, or, if it was out of operation or malfunctioning, such

[15] The Indian Evidence Act, 1872 (Act 1 of 1872), s. 3.

[16] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996 (United Nations Publication, Vienna, 1999).

[17] The Information Technology Act, 2000 (Act 21 of 2000), Preamble.

[18] The Indian Evidence Act, 1872 (Act 1 of 1872), s. 65B(1).

[19] *Ibid*, s. 65B(2)(a).

[20] *Ibid*, s. 65B(2)(b).

incident must not have been of a nature to affect the electronic record or the accuracy of its contents; and[21]

- The information contained in the electronic record must reproduce or be derived from information fed into the computer in the ordinary course of the activities.[22]

Recognizing that courts could not easily verify these complex technical conditions on their own, the legislature introduced the mandatory 'paper gatekeeper' under Section 65B(4): the certificate.[23]

This provision mandates that a party seeking to rely on a computer output must submit a certificate that:

1. Identifies the electronic record containing the information;
2. Describes the manner in which it was produced;
3. Gives particulars of the device involved in the processing of the data; and
4. Is signed by a person occupying a 'responsible official position' in relation to the operation of the device or the management of the relevant activities.[24]

The legislative intent behind this certificate was to assign human authorship and legal accountability to electronic outputs, assuring the court of the systemic integrity of the digital extraction without requiring the physical production of the master computer or server.

State (NCT of Delhi) v. Navjot Sandhu (Relaxing the Rule)

Right after the IT Act began in 2000, Indian trial courts spent ten years tangled in messy uncertainty. Because judges, lawyers on both sides hadn't dealt with digital evidence before, old ways clashed hard with new rules tucked into Sections 65A and 65B of the IEA. Trouble built up until it boiled over during State (NCT of Delhi) v. Navjot Sandhu often called the Parliament Attack Case[25]. That moment hit differently, given what happened: terrorists attacked India's Parliament on December 13, 2001, triggering an investigation that crossed many state lines. Facts unfolded under intense public eyes, making everything about procedure feel heavier than ever.

Anvar P.V. v. P.K. Basheer[26] (Restoring Mandatory Certification)

Almost nine years passed while courts in India followed the loose rules set by Navjot Sandhu, favoring paperwork over careful checks for digital evidence. Paper copies often replaced proper tech verification because investigators skipped

---

[21] *Ibid*, s. 65B(2)(c).

[22] *Ibid*, s. 65B(2)(d).

[23] Shikhar Goel, 'Paper in the Age of the Digital: The Curious Case of 65-B Certificates in India' 11 *Asian Journal of Law and Society* 435 (2024).

[24] The Indian Evidence Act, 1872 (Act 1 of 1872), s. 65B(4).

[25] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

[26] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

tough steps like forensic recovery or getting official certification under Section 65B. Instead, they leaned on printed sheets plus spoken words from police or junior IT workers to back up digital activity. But once computers, phones, and editing tools spread widely, ignoring flaws in unchecked electronic data grew too risky. A shift arrived in 2014 when three top judges at the Supreme Court stepped in through a key ruling in Anvar P.V. v. P.K. Basheer. That moment wiped out the earlier precedent firmly, bringing back tight legal standards for handling digital records.

2.3 The New Legal Architecture: Admissibility under Section 57 and Section 63 of the BSA, 2023

Structural Analysis of Electronic Evidence under the BSA, 2023

istory shifts when old rules fade into new ones. Paper trails once ruled courtroom truths across India for more than a hundred years. Now lawmakers swap parchment-based proof for digital traces under fresh statutes named Bharatiya Sakshya Adhiniyam, 2023. Physical form used to define what counted as a document back in colonial times. Electronic files struggled within those limits even after tech updates arrived through earlier laws like the IT Act. Digital records were always seen as second-class compared to paper notes and ledgers until now. This outdated split between ink and pixels fades with updated wording inside section three of current reform measures. A file on screen holds equal weight to one stamped by hand because boundaries blur where data flows freely. Change arrives quiet but certain in how facts are verified moving forward.[27]

Out of nowhere, the BSA tears down the old system built on paper. Not only that, but Section 2(1)(d) reshapes what counts as a 'document,' treating digital files just like handwritten notes. This part states:[28]

A thing gets called a document when it uses symbols, numbers, or signs on some material paper, screen, stone, whatever to hold information. It counts if someone made it to preserve details, even if nobody ends up using it later. The form does not matter much; carved words or typed files both qualify.[29] Electronic forms like emails or digital logs fit right in too, nowhere was the old paperonly mindset more obvious than in how laws once treated digital files. Digital information stands equal to printed pages because lawmakers rewrote the rules to include them upfront. Instead of squeezing electronic messages into outdated boxes meant for paper, they admit what everyone knows people write, sign, and share through

---

[27] Parliamentary Standing Committee on Home Affairs, *Three Hundred and Eightieth Report on the Bharatiya Sakshya Bill, 2023* (Rajya Sabha Secretariat, New Delhi, 2023).

[28] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 2(1)(d).

[29] *Ibid*, s. 2(1)(t).

devices today. A file on a screen carries weight just like one in a folder. This change didn't happen by accident it reflects how life actually works now.[30]
Now picture this: the BSA lays out a broad, techagnostic take on what counts as an electronic or digital record Section 2(1)(t) pulls in existing meanings from the IT Act, 2000, then stretches further. Think cloud storage, chips that store data, live databases running on devices, even signals sent through modern gadgets. That inclusion didn't exist before. It just quietly covers today's reality[31]

Deciphering Section 57 (Explanations 4 to 7)
Out here, the BSA shakes things up big time Section 57 widens what counts as 'Primary Evidence'. Before, under Section 62 of the old IEA, only the actual paper handed to court made the cut. Now think about data living online; showing the true original file meant tearing into faraway servers hardly doable. That rigidity fell apart fast once everything went digital[32].
The BSA resolves this structural impasse by inserting four revolutionary explanations Explanations 4, 5, 6, and 7into Section 57, creating a comprehensive statutory framework that recognizes the decentralized nature of modern digital storage.[33]

Section 63 of the BSA: Deconstructing Statutory Requirements
Whereas, however, the electronic record does not meet the requirements of the broadened concept of the evidentiary standard in Section 57, its admissibility is strictly regulated under Section 63 of the BSA. Under Section 63 of the BSA, the admissibility of electronic secondary evidence finds a new statutory basis, taking the place of Section 65B of the repealed IEA. According to Section 63(1), the deeming fiction is introduced by stating that any information contained in an electronic record that is printed on paper, or is stored, recorded, or copied in optical or magnetic media generated by a computer (the 'computer output'), is deemed to be a document.[34]

In order for this deeming fiction and admissibility in litigation to be achieved, the following four strict technical criteria, cumulatively required by Sections 63(2)(a)(d), should apply to the computer output:

- **The Regular Use Condition (Section 63(2)(a)):** The computer output containing the information must have been produced by the computer during a period when the device was used regularly to store or process information for the purposes of any activities regularly carried on by a person having

[30] Sir James Fitzjames Stephen, *The Indian Evidence Act, 1872* (Thacker, Spink & Co., Calcutta, 1872) 12.
[31] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 2(1)(t).
[32] The Indian Evidence Act, 1872 (Act 1 of 1872), s. 62.
[33] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 57.
[34] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63(1).

lawful control over the computer.[35] This condition is designed to ensure that the device was not set up on an adhoc, temporary basis to fabricate evidence for a specific dispute, but was rather part of a continuous, legitimate dataprocessing routine.

- **The Ordinary Course Condition (Section 63(2)(b)):** Throughout the said period, information of the kind contained in the electronic record was regularly fed into the computer in the ordinary course of those activities.[36] This requirement targets the systemic input integrity of the system, ensuring that the data was entered as part of a regular business, administrative, or personal routine, which reduces the likelihood of manual, retrospective data manipulation.
- **The Operational Integrity Condition (Section 63(2)(c)):** Throughout the material part of the said period, the computer must have been operating properly, or, if it was out of operation or malfunctioning, such incident must not have been of a nature to affect the electronic record or the accuracy of its contents.[37] This condition requires the court to evaluate the hardware and software stability of the device, ensuring that system crashes, database corruptions, or hardware failures did not compromise the binary integrity of the stored data.
- **The Reproduction Accuracy Condition (Section 63(2)(d)):** The information contained in the electronic record must reproduce or be derived from information fed into the computer in the ordinary course of the activities.[38] This condition mandates that the output presented to the court must be an accurate, unedited, and mathematically faithful reproduction of the data stored on the source system, ensuring that no unauthorized editing, truncation, or contextual distortion occurred during the extraction or printing process.

Section 63(2), through this technical rigor, therefore provides for a sound legal framework that allows for the assessment of the mechanical reliability of computerbased storage systems. This section accepts the fact that in the field of digital computing, the only means by which the reliability of any output can be assessed is if the input and processing processes remain consistently reliable.[39]

4. Comparative Analysis: India, the United States, and the United Kingdom

In order to understand the practicality and effectiveness of the recently passed Bharatiya Sakshya Adhiniyam, 2023 (BSA), there is a need for understanding the context of the legal framework in India against an international legal regime. Comparing the BSA to the Federal Rules of Evidence (FRE) in the United States and Police and Criminal Evidence Act, 1984 (PACE) of the United Kingdom,

---

[35] *Ibid*, s. 63(2)(a).
[36] *Ibid*, s. 63(2)(b).
[37] *Ibid*, s. 63(2)(c).
[38] *Ibid*, s. 63(2)(a).
[39] *Ibid*, s. 63(2).

along with other reformative amendments made later, shows that their approaches differ in nature..

4.1 The United States Paradigm: FRE Rules 901 and 902 and the Gatekeeping Doctrine

The process of handling digital evidence within the U.S. Federal judicial system involves procedural flexibility, judicial discretion, and an incredibly efficient self-authentication procedure. Contrary to the Indian mandatory certification regime under Section 63 of the BSA, and prior to Section 65B of the IEA, the rules of evidence concerning electronic evidence in the U.S. fall under the general rubric of 'authentication' under the ambit of FRE Rule 901 and Rule 902.[40]

As per FRE Rule 901(a), the authentication rule is met when there is sufficient evidence to prove that the item is indeed as represented. The standard to authenticate the item is considerably lower than the Indian 'condition precedent' model. Under FRE Rule 901, the item may be authenticated in several ways, including testimonial evidence from witnesses with personal knowledge (Rule 901(b)(1)), distinctive characteristics such as meta-data, IP addresses, and hashing considered in conjunction with the context (Rule 901(b)(4)).

In order to ease the administrative challenge posed by forensic experts testifying for digital extraction cases, the FRE was amended in 2017 with the incorporation of Rules 902(13) and 902(14).

These rules provide provisions for the self-authentication of electronic records:

- **FRE Rule 902(13) (Certified Records Generated by an Electronic Process or System):** Facilitates the authentication of data which is created using any process or system through electronic means, as long as such data is supported by a statement by an expert stating that the process used was effective.
- **FRE Rule 902(14) (Certified Data Copied from an Electronic Device, Storage Medium, or File):** It specifically helps the admission of forensic copies. Data extracted from any electronic device or document is self-authenticating if it comes with certification from a qualified forensic examiner who would have certified the hash value of the forensic copy and confirmed that it corresponds with that of the original data using cryptographic hashing (for example, $SHA-1$, $SHA-256$, or $MD5$).

What distinguishes this from the previous section is the definition of "qualified person." The American process does not face a state-monopoly bottleneck like India's Section 79A of the Information Technology Act, 2000. Any private

[40] Federal Rules of Evidence (United States), Rules 901 & 902.

forensic expert who is credentialed or even an enterprise IT manager could do the job on behalf of the party under penalty of perjury. In addition, the new scientific method employed in collecting forensic evidence would be evaluated based on the well-articulated Daubert Standard (Daubert v. Merrell Dow Pharmaceuticals, Inc.),[41] where the trial court acts as the gatekeeper in determining whether the new technique meets all the criteria of reliability, peer review, and error rate.

4.2 The United Kingdom Paradigm: The Repeal of Section 69 of PACE and the Common Law Presumption

The historical trajectory of the use of digital evidence in the United Kingdom is crucial to the Indian legislature. Initially, the United Kingdom's stance regarding digital evidence was very stringent under Section 69 of the Police and Criminal Evidence Act 1984 (PACE).[42]

Section 69 of PACE required that before a statement in a document produced from a computer could be considered admissible, it must be proven that:

1. There were no reasonable grounds for believing that the statement was inaccurate because of improper use of the computer; and
2. The computer was operating properly at all material times, or if malfunctioning, that the malfunction did not affect the production of the document or its accuracy.

The definition is nearly indistinguishable from Section 65B(2) of IEA and the newly introduced Section 63(2) of the BSA, 2023. But after ten years of experience in the courts, it became evident to English courts and legal reformers that Section 69 was simply impossible to apply in practice. As highlighted by the report published in 1997 by the Law Commission of England and Wales, Section 69 has no practical application whatsoever in the prevention of the admission of unreliable evidence but rather is an enormous procedural obstacle.[43]

In fact, the Commission highlighted that in the era of computers, it would be ludicrous for either the prosecutor or the administrator to have to show that an entire computer or software system was working without any defects during all material times. This would create an unfair situation in proceedings involving computers. Therefore, the UK Parliament enacted Section 60 of the Youth Justice and Criminal Evidence Act 1999 (YJCEA), which repealed Section 69 of PACE.[44]

Following the repeal of Section 69, the classic common law presumption was adopted by the UK; "Omnia praesumuntur rite esse acta" (all things are presumed

---

[41] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

[42] Police and Criminal Evidence Act 1984 (United Kingdom), s. 69.

[43] Law Commission of England and Wales, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997), para 13.12.

[44] Youth Justice and Criminal Evidence Act 1999 (United Kingdom), s. 60.

to have been done rightly and regularly). In light of this presumption, unless it can be shown to the contrary, it may be presumed that the computer system operated correctly at the relevant time. The burden is on the defense to establish any problem with the computer's operations by producing evidence of such a malfunction. Once such evidence has been produced, it falls on the prosecution to rebut such a presumption by showing beyond a reasonable doubt that the system had worked well.

4.3 Comparative Synthesis

The following matrix synthesizes the structural divergence between the three jurisdictions:

Parameter	India (BSA, 2023)	United States (FRE)	United Kingdom (YJCEA/ PACE)
Presumption of System Integrity	No presumption. The proponent must actively prove system integrity via Section 63 certification.	Rebuttable presumption of reliability; authenticated via sufficiency standards under Rule 901.	Strong rebuttable presumption (*omnia praesumuntur rite esse acta*). Presumed reliable unless disputed.
Certification Requirement	Mandatory dual-signature certification (Part A & Part B) under Section 63 for all secondary digital evidence.	Optional for self-authentication under Rules 902(13) & 902(14); otherwise authenticated via oral testimony.	No statutory certification required; general rules of admissibility and hearsay apply.
Expert Qualification Bottleneck	High. Part B requires signatures from system administrators or government-notified cyber examiners under Sec 79A IT Act.	Low. Any certified forensic examiner or IT professional can sign the Rule 902 certification.	Low. Disputed technical matters are resolved via standard court-appointed or party-retained expert witnesses.
Operational Flexibility	Extremely rigid. Technical failures in certification can lead to absolute exclusion of critical evidence.	Highly flexible. Promotes judicial discretion and "gatekeeping" of reliability rather	Prone to efficiency. Eliminates procedural bottlenecks, focusing trial time

		than hyper-technicality.	on substantive disputes of fact.

5. Suggestions and Recommendations

Inconsistency between the modern legislative framework provided by the Bharatiya Sakshya Adhiniyam, 2023 and the actual practices of the Indian law enforcement agencies, forensic services, and judiciary calls for immediate and thorough reform. In order to overcome these discrepancies, the below measures must be taken:

5.1 Structural Decentralization and Amendment of Section 79A, IT Act

The certificate prescribed under Section 63 of the BSA with dual signature must have Part B signed by an "expert" or "system administrator". In the current legal context, the term "expert" is limited in terms of its definition only to Section 79A of the IT Act, 2000, wherein certification can only be done by government-notified Examiner of Electronic Evidence labs.

- **Recommendation:** The Section 79A of the IT Act needs to be amended in order to create a decentralized licensing and accreditation system. The Central Government needs to empower the forensic laboratories at the state level, cyber forensics departments of universities, and certified private forensic experts to issue Part B licenses..
- **Operationalization:** There needs to be a creation of a National Registry of Certified Digital Forensic Practitioners (NRCDFP). Any person with internationally recognized digital forensics certification such as EnCE, MCFE, and CHFI, who also passes the national exam, must be able to legally sign the part B certification..

5.2 Mandatory Provisioning of Write-Blockers and Mobile Forensic Kiosks

Absolute integrity of a digital device needs to be preserved from the very moment of seizing the device. The present-day practice of turning on a device without write protection is bound to corrupt system metadata, thus destroying "system integrity" necessary for compliance with Section 63(2)(c)..

- **Recommendation:** It is imperative that the MHA directs that each police station across India be provided with basic hardware write blockers (like Tableau/WiebeTech write blocker devices) and mobile forensic kiosks (such as Cellebrite/MSAB kiosks)..
- **Operationalization:** There should be no accessing and imaging any digital device at a police station without physical presence of the write-blocker in place. The Standard Operating Procedure should include generating the hash value of $SHA-256$ of the target media before the media is moved from the scene of crime to the police station.

5.3 Codification of a National Standard Operating Procedure (SOP) for Digital Seizures

Section 57 of the BSA defines "proper custody" as the minimum requirement to admit electronic records as primary evidence. The use of "proper custody," however, is very subjective and can be easily abused in the malkhana (police storage room).

- **Recommendation:** The Central Government should develop and codify a compulsory and statutory National Guidelines for Seizure and Custody of Digital Evidence, bringing the national system on par with international guidelines like the ISO/IEC 27037.
- **Operationalization:** The rules must stipulate that:
    1. All the confiscated digital evidence must be kept in faradaic bags since the data can be erased by remote access via cell phone or Wi-Fi network.
    2. There must be a chain-of-custody record using an immutable database for every transfer of the physical evidence and its copy to/from the crime scene to the Forensic Science Laboratory (FSL).

5.4 Judicial and Prosecution Capacity Building

The technical complexity of Section 63 specifically regarding cryptographic hash matches and software integrity requires a highly technically literate judiciary and prosecution service.

- **Recommendation:** State Judicial Academies, in collaboration with premier technological institutions like the National Forensic Sciences University (NFSU) and Indian Institutes of Technology (IITs), must conduct mandatory, continuous technical training programs.
- **Operationalization:** Judges need to be made competent enough to look beyond the piece of paper that bears the certificate. Judges must ask for the generation of forensic acquisition logs (which consist of the validation check, system logs, and the match with mathematics of the hash value) as proof of certification submitted under Section 63. Defense lawyers too should be given access to state-funded independent forensic experts under Article 21 of the Constitution..

6. Conlcusion

The evolution of the framework of digital evidence in India, which follows the path of development from the foundation stones laid by the IEA in the nineteenth century to the present-day structure of the BSA, presents itself as a complex interplay between procedural norms and computational facts. The core question guiding this research was whether the legal code that operates on the principles of a paper-based reality could cope with the emerging digital environment. From the review of historical changes to the legislative, judicial, and technological

approaches to evidence in India, some vital insights have emerged that demonstrate the continuity of failures from the past to the new code of laws.
The primary conclusion reached within this research is that the classical framework of the original IEA, 1872 was essentially unsuitable for governing the domain of digital evidence. This is due to the fact that the Best Evidence Rule, which became the key point in the philosophy underlying Sir James Fitzjames Stephen's draft, was based exclusively on materialist assumptions.[45] A document in the context of this nineteenth-century understanding of architecture was understood not by its contents but by its physicality, whereby the only proof of contents required the creation of the physical document itself under Section 62.

When analog technologies were developed during the twentieth century, it became possible to assimilate magnetic tapes as documents by use of analogies where it was held in cases such as R.M. Malkani v. State of Maharashtra that impressions recorded on tapes magnetically were considered symbols made on a piece of paper.[46] However, the advent of computer technology and digital information proved problematic to this model of proof, as unlike information recorded on analog media, which existed as physical inscriptions on tapes or filmstrips, digital computing information exists as a configuration of zeroes and ones across several different devices including local hard drives, synchronized cloud databases, and remote servers.

The viewing or accessing of digital files necessarily involves the process of replication, rather than production, meaning that the proof of contents via 'primary evidence' was effectively impossible, as the original database or server system was unlikely to be physically present in court, and secondary evidence was unavailable due to intact systems.

The second main point of observation here is that the legislative response in the form of the Information Technology Act, 2000 which tried to address the problem by incorporating Sections 65A and 65B into the IEA, was unsuccessful in laying down a scientific approach to electronic evidence. Rather than formulating guidelines for admissibility of electronic evidence based on the principles of forensic computing, the legislation established a certification process that initiated a legal pendulum for two decades.

---

[45] Sir James Fitzjames Stephen, *The Indian Evidence Act, 1872* (Thacker, Spink & Co., Calcutta, 1872) 12.
[46] *R.M. Malkani v. State of Maharashtra*, AIR 1973 SC 157.

Bibliography

A. Primary Sources: Statutes and Legislative Documents

- Federal Rules of Evidence (United States).
- Police and Criminal Evidence Act 1984 (United Kingdom).
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023) (India).
- The Indian Evidence Act, 1872 (Act No. 1 of 1872) (India) [Repealed].
- The Information Technology Act, 2000 (Act No. 21 of 2000) (India).
- Youth Justice and Criminal Evidence Act 1999 (United Kingdom).
- Law Commission of England and Wales, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997).
- Law Commission of India, *185th Report on Review of the Indian Evidence Act, 1872* (2003).
- Parliamentary Standing Committee on Home Affairs, *Three Hundred and Eightieth Report on the Bharatiya Sakshya Bill, 2023* (Rajya Sabha Secretariat, New Delhi, 2023).
- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996 (United Nations Publication, Vienna, 1999).

B. Primary Sources: Judicial Decisions

- *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
- *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993) (United States).
- *R.M. Malkani v. State of Maharashtra*, AIR 1973 SC 157 (India).
- *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801 (India).
- *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600 (India).

C. Secondary Sources: Books and Treatises

- Casey, Eoghan, *Digital Evidence and Computer Crime* (Academic Press, London, 3rd edn., 2011).
- Sarkar, P.C. and M.C. Sarkar, *Law of Evidence* (LexisNexis, New Delhi, 15th edn., 2020).
- Stephen, Sir James Fitzjames, *The Indian Evidence Act, 1872* (Thacker, Spink & Co., Calcutta, 1872).

D. Secondary Sources: Journal Articles and Academic Papers

- Bajpai, G.S., "Scientific Investigation in Indian Criminal Justice: A Ground Reality Check," 12 *Indian Journal of Criminology* 45 (2021).
- Bhawnani, Gaurav and Aditya Mehta, "Admissibility and Proof of RTI Documents under the Indian Evidence Act," 32 *National Law School of India Review* 1 (2020).
- Goel, Shikhar, "Paper in the Age of the Digital: The Curious Case of 65-B Certificates in India," 11 *Asian Journal of Law and Society* 435 (2024).
- Prasad, S.S., "Deciphering the Digital Trial: Challenges under Bharatiya Sakshya Adhiniyam," 66 *Journal of the Indian Law Institute* 45 (2024).

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618