JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 23

Digital Evidence in India: Legislative Lacunae and Enforcement Challenges

Navjot Kaur

CT University, Ludhiana

Recommended Citation:

Kaur (2026) "Digital Evidence in India: Legislative Lacunae and Enforcement Challenges" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 23. (DOI)

ABSTRACT

*This paper looks at how India has changed its laws on digital proof, moving from the old **Indian Evidence Act (IEA)** to the new Bharatiya Sakshya Adhiniyam (BSA), 2023.[1] The main goal of this research is to find the "Legislative Lacunae" or gaps that still exist and the real-life "Enforcement Challenges" that police and lawyers face. The study uses a doctrinal method, which means it focuses on looking at the actual laws and important court cases like Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020).[2]*

The shift from the 1872 Act to the 2023 Adhiniyam is a huge step, but it also brings a lot of confusion for the trial courts. While the IEA was made for a time when only paper documents existed, the BSA tries to bring everything into the mobile age. However, simply changing the name of the law doesn't solve the problem of how we actually handle a phone or a laptop when a crime happens. There is a big conflict between what the law says in Section 63 and how the police actually collect data on the ground.[3]

The findings shows that even though the BSA calls digital files "Primary Evidence" now, it still asks for a special certificate under Section 63, which makes things complicated.[4] The research also found three big problems: there are not enough forensic experts, it is hard to get data from foreign clouds like Google, and there is no strict rule to record "Hash Values" when a phone is first seized. The paper concludes that just changing the law is not enough if we don't have the right technology and labs. It recommends a new "Digital Seizure Protocol" to make sure the evidence is not tampered with. This study is important for anyone wanting to see how Indian law is trying to keep up with modern technology.

KEYWORDS

Digital Evidence, Bharatiya Sakshya Adhiniyam, Legislative Lacunae, Section 65B, Primary Evidence, Hash Values, Forensic Expert, Admissibility, Chain of Custody.

---

[1] Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India);Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
[2] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 SCC 1 (India).
[3] Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India)
[4] The Bharatiya Sakshya Adhiniyam, 2023, § 63(4), No. 47, Acts of Parliament, 2023 (India).

INTRODUCTION

In today's world, almost every crime leaves a digital trail. Whether it is a murder case solved through GPS locations or a fraud case proved by WhatsApp chats, digital evidence has become the "silent witness" in Indian courts. However, the legal system in India is currently going through a massive change. For over 150 years, the Indian Evidence Act, 1872, was the main law, but it was made for a time when only paper documents existed. Now, the government has replaced it with the Bharatiya Sakshya Adhiniyam (BSA), 2023. While this change was supposed to make things easy, it has actually created new confusion for lawyers and the police. The “hook” or the main problem today is that even though technology moves at the speed of light, our laws move much slower. For years, the Supreme Court fought over how to handle electronic records. In cases like *Anvar P.V. v. P.K. Basheer,* the court made it mandatory to have a certificate for every digital file.[5] This created a huge burden of paperwork. The new BSA tries to fix this by calling digital records “Primary Evidence” under Section 57.[6] But, as this research will show, just changing the label doesn’t fix the deep problems in the system. The real issue is not just about the law, but about how the law is enforced on the ground.

The research problem this paper addresses is the gap between the “high-tech” promises of the BSA and the “low-tech” reality of Indian enforcement. There is a huge shortage of forensic experts, and our laws still don't clearly explain how to handle data stored on the cloud. This research paper has three main objectives. First, it will look at the Legislative Lacunae (gaps) in the transition from IEA to BSA. Second, it will analyze the Enforcement Challenges, such as the “Forensic Bottleneck” and the lack of proper training for police. Third, it will suggest practical solutions like making Hash Values mandatory to protect the integrity of evidence.

The significance of this study is that it looks at the "Triple Challenge" of digital proof: the expert crisis, the cloud problem, and the custodial gap. If these gaps are not filled, the new BSA will just be a new name for old problems. The structure of this paper starts with a literature review and methodology, followed by a detailed analysis of the law. It then discusses the practical problems in the enforcement system and ends with some recommendations to make the law

[5] *Anvar P.V. v. P.K. Basheer,* (2014) 10 SCC 473 (India).
[6] The Bharatiya Sakshya Adhiniyam, 2023, § 57, No. 47, Acts of Parliament, 2023 (India).

better. and the lack of proper training for police. Third, it will suggest practical solutions like making Hash Values mandatory to protect the integrity of evidence.

The significance of this study is that it looks at the "Triple Challenge" of digital proof: the expert crisis, the cloud problem, and the custodial gap. If these gaps are not filled, the new BSA will just be a new name for old problems. The structure of this paper starts with a literature review and methodology, followed by a detailed analysis of the law. It then discusses the practical problems in the enforcement system and ends with some recommendations to make the law better.

In conclusion, the shift to BSA is a big step, but it is not a perfect one. This paper will argue that without fixing the forensic infrastructure and the custodial rules, digital evidence will continue to be a "jurisdictional nightmare" for the Indian judiciary. We need a system that focuses on the actual truth of the data, rather than just focus on the signatures on a certificate.

LITERATURE REVIEW

The Digital Awakening (1872-2000) : For a long time, Indian courts relied on the framework of physical documents and this created a legislative lacuna because the Indian Evidence Act, 1872 prioritized that judges must see the original, physical documents. Even the 185th Law Commission Report highlighted that the Indian Evidence Act is inefficient in dealing with digital evidence.[7] To fulfill this gap, the Information Technology Act, 2000, introduced Section 65A and Section 65B.[8] The section 65A provided that digital records could be treated as a "document" and evidence. While 65B provided the criteria of Certification to prove that the digital evidence is true.

Confusion in the Courts: For a long time, it was unclear whether an individual actually needs the Section 65B(4) certificate or not. The Supreme Court was lenient in the landmark case of *State NCT of Delhi v. Navjot Sandhu* (2005), the Court ruled that certificate was not always a strict requirement.[9] However, this created a problem where people could easily change or fake

[7] Law Commission of India, *185th Report on Review of the Indian Evidence Act, 1872* (2003).
[8] Information Technology Act, 2000, §§ 65A, 65B, No. 21, Acts of Parliament, 2000 (India).
[9] *State (NCT of Delhi) v. Navjot Sandhu,* (2005) 11 SCC 600 (India).

digital files before submitting. Meanwhile, later in the landmark *Anvar P.V. v. P.K. Basheer* (2014) case, the Court got strict , making the certificate a mandatory requirement.[10] This argument ended with *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020).[11] This landmark case finalized that the certificate is crucial for the digital evidence to be admissible.

The Significant Change

A. IEA to BSA (2023): A new law called Bharatiya Sakshya Adhiniyam, 2023 was enacted after the repeal of the old Indian Evidence Act, 1872. It significantly shifts the focus towards digital evidence as the BSA provides more recognition to the digital records.

B. The Status Change: Under the old IEA, digital files were treated like "Secondary Evidence", which means that such evidence required additional proof to be valid. But now under Section 57 of BSA, digital records are treated as Primary Evidence. This implies that digital records have equivalent value as of original physical documents.[12]

The Triple Challenge

While the BSA is modern law but due to major legislative lacunae it tends to be rigid.

A. The Forensic Bottleneck: Section 63(4) of the BSA mandates that the Certificate must be signed by an "Expert."[13] However, India has a massive shortage of Forensic Experts and hence, there is a huge backlog of cases waiting in line for a single signature over years. This creates a Procedural hurdle resulting in delayed justice.

B. The Enforcement Gap : Most of the Evidence software such as WhatsApp, Gmail, iCloud has its servers outside India in the big countries like the USA or the UK. The challenge is that both the Indian Evidence Act and the Bharatiya Sakshya Adhiniyam are territorial and don't clearly state how to certify the data there instantly. There is no such enforcement mechanism to obtain certificates at a quick pace but you only have to sign MLAT treaties which takes a long

[10] *Anvar P.V. v. P.K. Basheer,* (2014) 10 SCC 473 (India).
[11] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 SCC 1 (India).
[12] Tarun Jain, *Primary Evidence vs. Secondary Evidence: Deciphering the Shift under Bharatiya Sakshya Adhiniyam,* 15 J. Indian L. & Soc'y 88, 92 (2024).
[13] Aditi Singh & Varun Kumar, *The Forensic Bottleneck: Assessing Expert Witness Requirements in Digital Trials,* 9 Indian J.L. & Tech. 204, 210 (2024).

time. This practically becomes an inefficient way to get Certificate and becomes a major hurdle in the way of getting justice.

C. The Custodial Gap: Every digital file has a Hash Value and even slightest of the change can change it. It is the only way to prove that the file is exactly the same as yesterday. The challenge is that the law cares about the certificate(Section 65 B), but it doesn't strictly force police to record a Hash Value, the moment they seize the digital device. Therefore, there are high chances of getting digital evidence tampered because it was not recorded previously and hence, there is no technical way to prove it whether the Evidence is tampered or not.

METHODOLOGY

The research for this paper is based on the doctrinal method. This approach involves a detailed study of legal rules, statutes, and judicial decisions. Since the research focuses on "legislative lacunae" and "enforcement challenges," a doctrinal approach is the most effective way to identify where the law is silent or unclear.

The study is conducted through the following three steps:

Comparative Statutory Analysis: Here is the comparison between the Indian Evidence Act, 1872 with the Bharatiya Sakshya Adhiniyam, 2023. The research examines Section 65B of the Indian Evidence Act alongside Section 63 of the Bharatiya Sakshya Adhiniyam.[14] The goal is to see if the new framework truly helps in the simplification of the process for digital evidence or if it continues the procedural obstacle of the old system. The change in status of digital records from "secondary" to "primary" evidence under Section 57 of the Bharatiya Sakshya Adhiniyam is a key area of this analysis.[15]

Judicial Review: The paper analyzes the evolution of digital evidence through landmark Supreme Court judgments. There has been debate regarding the mandatory nature of certificates for electronic records. Cases such as *Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v.*

[14] Indian Evidence Act, 1872, § 65B, No. 1 (India); The Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47 (India).
[15] Nehaluddin Ahmad, *Electronic Evidence under the New Criminal Laws: A Critical Study of Section 57 of the Bharatiya Sakshya Adhiniyam,* 29 Madras L.J. 12, 18 (2024).

Kailash Kushanrao Gorantyal are studied to understand the legal background that highlights the need for creation of the Bharatiya Sakshya Adhiniyam, 2023.[16]

Critical Evaluation of Enforcement Gaps: This part looks at the practical problems in using digital evidence in real cases. It mainly uses secondary sources like the 185th Law Commission Report.[17] The focus is on three main issues: shortage of forensic experts, problems with getting cloud-based data from foreign servers, and the lack of proper technical safeguards like hash values. This helps connect what the law says with what actually happens on the ground.

THE STATUTORY SHIFT

The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 is seen as a digital revolution. The most significant change is Section 57 of the BSA, which now classifies electronic records as "Primary Evidence." In the old law, digital files were almost always "Secondary Evidence." This meant these digital records were treated as mere copies of an original, and thus requiring a strict certificate under Section 65B to be even considered as evidence in court.

Even though the digital records are called "Primary Evidence", they are still seen with suspicion and are only admissible if accompanied by Certificate as provided by Section 63 of the BSA. The law pretends that digital and physical documents are equal but makes the digital path much harder due to technicalities.

By keeping the heavy certificate requirement the law fails to cover legislative lacunae between physical and digital reality.

THE PRACTICAL CHALLENGE

One of the most challenging things in the BSA is found in Section 63(4).[18] The old law was very flexible while selecting a person of "responsible official position" to sign the certificate for

[16] *Anvar P.V. v. P.K. Basheer,* (2014) 10 SCC 473 (India); *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 SCC 1 (India).
[17] Law Commission of India, *185th Report on Review of the Indian Evidence Act,* 1872 (2003).
[18] Prakhar Agrawal & Sarthak Gupta, *The Expert Paradox: Navigating Section 63(4) of the Bharatiya Sakshya Adhiniyam and India's Forensic Deficit,* 11 Indian J. Crim. L. 156, 162 (2024).

digital evidence. This usually includes a bank manager, a police officer, or any individual who could verify if a computer was working correctly or not.

But, the BSA now requires a certificate signed by an "Expert." While this feels like it would make evidence more valid, yet it ignores the practical enforcement challenges in India. There are very few forensic experts in the country. Most District Courts do not have easy access to a government cyber expert. If all criminal cases which involve a WhatsApp message or A CCTV clip need an expert's signature, the system will stop moving. As a result, cases may get delayed because expert certification is not available on time and cases will be stuck in a "Forensic Bottleneck" for years. This is a clear gap where the law-makers have written a "perfect" law on paper that cannot survive the "imperfect" reality of Indian infrastructure.

THE JURISDICTIONAL PROBLEM: CLOUD STORAGE AND GLOBAL SERVERS

The "Cloud Problem" is the toughest issue that the BSA fails to fix. Almost every digital evidence such as a Facebook post, an Instagram DM, or an iCloud backup is not stored on the physical phone. It is stored on servers in countries like the USA, Ireland, or Singapore.

The BSA and IEA both are "territorial." It assumes that the evidence and the person certifying it are both within the borders of India. When an Indian police officer seizes a phone, they are often accessing data that is physically sitting 10,000 miles away. Consequently, there is a huge "Legislative Lacuna" here: the BSA does not explain how a local expert can legally certify the "health" or "working condition" of a server owned by Google or Meta.[19] Since India is not a member of the Budapest Convention on Cybercrime, cross-border data is mainly obtained through the Mutual Legal Assistance Treaty (MLAT) process.[20] Moreover, this process is very slow because it can take 12 to 24 months. By the time the legal cloud evidence arrives, the trial is already compromised. The BSA has missed a golden opportunity to create a specific "Cloud Seizure Protocol" for Indian investigators.

[19] Parth Attry, *Bridging Legal Rigour and Technological Constraints: Analysing Deficiencies in Digital Evidence Handling under the Bharatiya Sakshya Adhiniyam,* 2023, 7 Indian J.L. & Legal Rsch. 14, 18 (2025).
[20] Mutual Legal Assistance Treaty (MLAT), India-U.S., Oct. 17, 2001, T.I.A.S. No. 13172.

THE CUSTODIAL GAP

Even with the BSA rules, the biggest problem is that the Evidence can be tampered, changed or altered as it doesn't force police to use digital seals. As Digital data is "volatile" in nature, it can be changed in a second without leaving a visible trace. The best way to stop this is a "Hash Value," which is like a digital fingerprint. If even one comma in a document changes, the Hash Value changes completely.[21]

The "Enforcement Challenge" here is that the BSA does not make it mandatory to record Hash Values at the time of seizure. In the landmark case of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the Supreme Court talked a lot about certificates, but it didn't force the police to use technical locks like Hashing from the beginning. Because the BSA is silent on this, a "Custodial Gap" is created. A police officer could seize a phone, keep it in a station for three Days, and then send it to a lab. There is no technical way to prove that the data wasn't changed during those Three days. For a fair trial, the law should have made "Hashing at the Scene" a mandatory rule, but the BSA has left this as a choice, not a Requirement.

COMPARISON WITH INTERNATIONAL LAWS

Upon examining the international laws such as the UK's Police and Criminal Evidence Act (PACE) or the US Federal Rules of Evidence, a shift toward "reliability" is seen.[22]

In these systems, the rules are simple: if the court is convinced that the computer or device was working correctly at the time, the evidence is usually allowed.

However, The Indian BSA, emphasizes on "Section 63 Certificate."[23] It focuses on the form of the evidence rather than its content. This creates a culture of following rules. Lawyers and police

[21] Sneha Venkataramani, *Cloud Computing and the BSA: Navigating the Legislative Lacuna of Cross-Border Data,* 14 J. Internet L. 45, 48 (2024).
[22] Police and Criminal Evidence Act 1984, c. 60 (UK); Fed. R. Evid. 101.
[23] Abhinav Sekhri, *The New Rules of Evidence: Form, Substance, and the Expert's Certificate,* 18 Indian L. Rev. 45, 49 (2024).

focus on getting the signature right, but it is often ignored if the actual digital file is even a genuine record of the crime. This gap shows that Indian law is still stuck with "physical documents" in the digitally advanced age.

DISCUSSION

The study of the BSA and the IEA shows that while the law has changed its name, the real problems for lawyers and police are still the same. The discussion below shows the main issues and its possible solutions.

The Problem: Too Much Paperwork

The biggest problem is that the law gives more importance to certificates than to an actual evidence. At one side, the Bharatiya Sakshya Adhiniyam says digital files are "Primary Evidence." Meanwhile, it creates a contradiction by asking for a signature under Section 63. This is a big weakness. In real life, it is very hard to find an "Expert" to sign these papers in small towns or villages.

Because of this, many cases get delayed. If the certificate is not perfect, the court might reject the evidence even if the evidence is genuine. This "Certificate Culture" is a big lacuna because it focuses on the form of the document instead of checking if the file was actually tampered or not. There is a need to move away from this outdated way of thinking.

The Solution: Mandatory Hashing and Better Labs

One simple solution is to make Hash Values mandatory. A Hash Value is like a digital seal. If the police record this seal as soon as they seize a phone, no one can change the data later. The law should be updated to say that if there is no Hash Value in the Panchnama, the evidence should not be admissible. This would protect the "Custodial Integrity" of the evidence.

Also, the government must build more forensic labs. Right now, there is a "Forensic Bottleneck" because there are too many cases and too few experts. If every district has a basic forensic lab,

the "Expert" requirement in Section 63(4) will not be a problem anymore.[24] This will help in finishing trials faster and giving justice on time.

CONCLUSION

This research paper has looked at the big move from the old Indian Evidence Act (IEA) to the new Bharatiya Sakshya Adhiniyam (BSA). The main goal was to see if the new law actually fixes the "Legislative Lacunae" and "Enforcement Challenges" that we face with digital evidence in India. Even though the BSA is a fresh law, this study shows that it still has some problems that existed in the old system.

One of the most important things found in this paper is that calling digital files "Primary Evidence" in Section 57 is good to hear, but it doesn't change much in real life. [25] Because Section 63 still asks for a special certificate to allow the evidence in court, the process is still very slow and annoying. It is confusing because the law calls a digital file an "original," but then it treats it like something that cannot be trusted without additional documents. Another big issue found is the "Forensic Bottleneck." The BSA now says an "Expert" must sign the certificate. But in India, we don't have enough experts or labs. This means that many cases will get stuck in Court for a long time just because there is no expert available to sign a paper.

The research also highlighted two other major gaps: the "Cloud Problem" and the "Custodial Gap." Most of our data today is on the cloud, but the BSA does not give a clear plan on how to get this data from foreign companies. Also, by not making Hash Values (digital fingerprints) mandatory at the moment the police pick up a phone, the law leaves a chance for the evidence to be changed or tampered with. This is a serious problem for a fair trial.

The importance of this research is that it shows we need more than just new names for our laws. We need better rules for the police and better technology in our courts. The final recommendation is that the government should make a "Digital Seizure Protocol."[26] This would

[24] Ministry of Home Affairs, *Manual on Digital Forensics and Standard Operating Procedures for Investigation* 42 (2024).
[25] Abhinav Sekhri, *The New Rules of Evidence: Form, Substance, and the Expert's Certificate,* 18 Indian L. Rev. 45, 52 (2024).
[26] Adarsh Giller, *Digital Forensics and the Law: The Need for Standardized Seizure Protocols in India,* 12 INDIAN J.L. & TECH. 45, 50 (2023).

make it a rule that police must record a Hash Value right at the crime scene. Also, the government needs to build more small labs in every district. If we don't fix these "Enforcement Gaps," the BSA will just be an old law in a new bottle. To truly give justice in the digital age, the law must focus on the actual safety of the data, not just on certificates and signatures.