THE GHOST IN THE MACHINE: NAVIGATING THE SELF GENERATED EVIDENCE DILEMMA UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Sai Shetye, Thakur Ramnarayan College of Law

Sanika Parab, Thakur Ramnarayan College of Law

ABSTRACT

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents more than a mere legislative update, it is an ontological shift in the Indian legal system. By replacing the 151-year-old Indian Evidence Act, 1872 (IEA), the BSA purports to decolonize Indian jurisprudence while simultaneously grappling with the Silicon Revolution. This research provides a high density, comparative analysis of the transition from Newtonian, human-centric evidence to the era of Autonomous Machine Evidence. It critiques the BSA's internal contradictions, specifically the paradox of labelling electronic records as Primary Evidence under Section 57 while retaining the restrictive human centric certification of Section 63. The paper argues that the BSA suffers from an Epistemic Crisis it recognizes digital facts but remains tethered to a Victorian philosophy of accountability. Through a comparative study of the UK's Presumption of Reliability and the US Machine Hearsay doctrine, this work proposes a new framework for Algorithmic Integrity to protect the Constitutional guarantees of Fair Trial and Privacy in an age of deepfakes and automated prosecution.

Keywords: Autonomous Machine Evidence, Epistemic Crisis, Algorithmic Integrity Framework, Primary vs. Certified Electronic Records, Fair Trial.

1. INTRODUCTION: THE DEATH OF THE NEWTONIAN WITNESS AND THE BIRTH OF THE ALGORITHMIC FACT

1.1. THE LEGACY OF SIR JAMES FITZJAMES STEPHEN AND VICTORIAN RATIONALISM

The Indian Evidence Act of 1872 was not merely a code, it was a monument to the 19th-century belief in human agency and physical causation. Its architect, Sir James Fitzjames Stephen[1], viewed the courtroom as a controlled laboratory of human behaviour. In Stephen's Newtonian universe, evidence was always a traceable byproduct of a human decision: a witness observed an event and spoke from memory, a merchant decided to record a transaction and put pen to paper. The ultimate tether of truth was the Person[2].

Stephen's philosophy was rooted in Benthamite utilitarianism the idea that the law should facilitate the search for truth through a rigid set of rules that filtered out the unreliable (hearsay). This human-centricity was a philosophical necessity. The law was built on the assumption that for every fact introduced in court there was a Declarant whose motives could be probed whose biases could be unmasked, and whose reliability could be weighed through the crucible of cross-examination[3]. Truth was seen as a carbon-based phenomenon, inseparable from the human mind.[4] The Victorian lawyer operated in a world of physical substrates paper, ink and wax seals. The transition from these tangible artifacts to the ephemeral world of digital packets is not just a change in medium, it is a change in the very nature of legal reality.

1.2. THE 'BHARATIYA' TRANSITION: DECOLONIZATION OR RE-BRANDING?

The transition to the Bharatiya Sakshya Adhiniyam (BSA), 2023, is framed by the legislature as a decolonizing act, intended to shed the colonial mindset that permeated the IEA. However, a critical analysis reveals a deeper tension. While the BSA removes archaic references to the British Crown, the Privy Council and the UK it retains approximately 90% of the textual DNA of the 1872 Act. The decolonization here is linguistic rather than philosophical. The BSA still

[1] Sir James Fitzjames Stephen, A Digest of the Law of Evidence (1876).
[2] John Henry Wigmore, A Treatise on the System of Evidence in Trials at Common Law (1904).
[3] Kenneth W. Graham, Jr., The Right of Confrontation and the Hearsay Rule: Sir Walter Raleigh Loses Another One, 8 Crim. L. Bull. 99 (1972).
[4] Ronald J. Allen, The Evolution of the Hearsay Rule to the Comprehensive Exclusion of Relevant Evidence, 1982 U. Ill. L. Rev. 231 (1982).

relies on the 19th-century Master-Slave relationship between humans and machines[5]. It treats the computer as a dumb tool of a human master, ignoring the reality of the 21st century where the master (the human) often has no understanding of how the tool (the algorithm) generated the result.

We must ask: can a law truly be decolonized if it retains the evidentiary hierarchies established by the colonizer? The IEA was an instrument of colonial control, designed to standardize the rules of truth across a diverse subcontinent[6]. By essentially re-packaging these rules with new names, the BSA risks carrying the ghosts of Victorian control into the digital age.

1.3. THE SILENT REVOLUTION: FROM CARBON TO SILICON EVIDENCE

We have moved from the era of the Scribe to the era of the System[7]. Today, the most critical evidence in a murder trial might be the heart-rate logs of a smartwatch, in a fraud case, it might be the high-frequency logs of a trading bot, in a trespass case, it might be the autonomous telemetry of a drone. The BSA decolonizes the terminology, but it maintains a haunting silence on the agency of machines.

We are witnessing a transition from a law of Witnesses to a law of Processes, yet the BSA continues to treat the machine as a mere tool ignoring that modern algorithms, especially Artificial Intelligence (AI), generate facts that no human anticipated or intended[8]. This creates an Agency Gap that threatens the very foundation of adversarial truth-finding. If an algorithm makes a mistake, who is the liar? If an autonomous sensor fails, who is the witness? The BSA offers no answers to these fundamental questions.

II. THE DEFINITION OF A 'DOCUMENT' AND THE MACHINE-AGENCY PROBLEM

2.1. ANALYSING SECTION 2(1)(D): THE DIGITAL CATCH-ALL AND ITS FAILURES

The BSA expands the definition of a document to include electronic and digital records, citing

[5] Law Commission of India, Review of the Indian Evidence Act, 1872, Report No. 185 (2003).
[6] Abhinav Chandrachud, Republic of Rhetoric (2017).
[7] Luciano Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality (2014).
[8] Susan Haack, Evidence and Inquiry: Towards Reconstruction in Epistemology (1993).

server logs, locational data, and messages[9]. However, this definition remains conceptually flat. It fails to distinguish between two fundamentally different types of digital evidence:

1. **Digitized Evidence**: A human scans a physical deed. The mind behind the fact is human, the digital format is just a carrier.

2. **Native Autonomous Evidence**: A sensor logs an environmental change or an AI creates a composite image. Here the mind is an algorithm[10].

By treating both as identical documents, the BSA applies a Victorian logic to a Silicon reality. In the 19th century, a document was an extension of a person's mind. Today, an autonomous log is an extension of a mathematical probability. Treating them the same allows Hearsay by Proxy, where machine outputs enter the record without the ability to cross-examine the algorithm that produced them[11]. This lack of nuance means that a human's email and a machine's automated log are governed by the same rules of relevancy, even though their origins are fundamentally different.

2.2. THE 'DECLARANT' CRISIS: COMPARATIVE US JURISPRUDENCE

In the United States, the Federal Rules of Evidence (FRE) have had to grapple with whether a machine can be a declarant.

(A) **The Lizarraga-Tirado Standard**: In ***United States v. Lizarraga-Tirado*** (2015), the 9th Circuit held that GPS data generated by Google Earth is not hearsay because a declarant must be a person[12]. The court reasoned that machines do not have the same incentives to lie or forget.

(B) **The BSA Friction**: India, under the BSA does not recognize this distinction. It forces all electronic records through the human-centric authentication of Section 63. This leads to a technical absurdity, we require a human to vouch for a machine's honesty, even though the human has no access to the machine's internal state or logic[13]. This turns the witness box into a stage for performative technicality rather than factual verification. If a human cannot explain

[9] Bharatiya Sakshya Adhiniyam, 2023, § 2(1)(d) (defining "document").
[10] Jack M. Balkin, The Path of Robotics Law, 6 Calif. L. Rev. Circuit 45 (2015).
[11] Jennifer L. Mnookin, The Image of Truth: Photographic Evidence and the Power of Analogy, 10 Yale J.L. & Human. 1 (1998).
[12] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015).
[13] Christian Chessman, A "Source" of Error: Computer Code and the Hearsay Rule, 48 Hofstra L. Rev. 1 (2019).

why the machine logged a specific data point, the testimony is essentially hearsay, yet the BSA mandates it as the primary path to admissibility.

III. THE PRIMARY EVIDENCE PARADOX: SECTION 57 VS. DIGITAL REALITY

3.1. The Elevation to Primary Evidence: Explanation 4

One of the BSA's most lauded features is Section 57, Explanation 4, which declares that where an electronic or digital record is created or stored, such record including any output is primary evidence[14]. This was intended to solve the decade-long confusion in Indian courts regarding the Secondary Evidence status of digital files[15]. By promoting digital records to the status of originals, the legislature hoped to bypass the complex Best Evidence Rule hurdles.

3.2. THE ORIGINALITY FALLACY IN DECENTRALIZED SYSTEMS

However, Primary Evidence is a concept rooted in Originality. In modern computing, the original is a misnomer.

(A) Distributed Ledger Technology (DLT): In a blockchain transaction, where is the original? The data is replicated across thousands of nodes[16]. The BSA's reliance on computer resources (implying a localized or centralized source) fails to account for the decentralized nature of the modern cloud.

(B) Volatile Memory and Cyber-Forensics: Much of modern evidence exists only in RAM (Random Access Memory). If this is primary evidence, but it disappears the moment a device is switched off, the law provides no mechanism for the Forensic Snapshot[17] to be treated as a co-equal to the original.

(C) The Problem of 'Ephemeral Truth': In a cybercrime scenario, the evidence is often a temporary state of a network. The BSA's focus on records (which implies storage) excludes the states of a system that are often more telling than the logs they leave behind. The Act assumes a static nature of digital evidence that is simply not supported by the fluid nature of

[14] Bharatiya Sakshya Adhiniyam, 2023, § 57, expl. 4.
[15] Tomaso Bruno v. State of U.P., (2015) 7 SCC 178.
[16] UNCITRAL Model Law on Electronic Commerce, art. 5 (1996).
[17] Eoghan Casey, Digital Evidence and Computer Crime (3d ed. 2011).

modern computation.

IV. SECTION 63(4): THE IMPOSSIBLE CERTIFICATE AND THE 'BLACK BOX' CRISIS

4.1. THE PERSISTENCE OF THE CERTIFICATE REQUIREMENT

The BSA retains the mandatory requirement for a certificate signed by a responsible official to authenticate electronic records. This is a direct carryover from Section 65B (4) of the IEA. While this was a useful safeguard for 1990's databases where a local admin could vouch for the hardware, it is an absolute disaster for 2020's AI and Cloud computing.

4.2. THE 'RESPONSIBLE OFFICIAL' AS A LEGAL FICTION

In the age of Deep Learning, this requirement is a legal fiction.

(A) Explainability Gap: If a facial recognition AI produces a match, the IT officer signing the Section 63 certificate cannot verify the internal logic of the neural network[18]. They are certifying the hardware (the shell), but the evidence is produced by the software logic (the ghost).

(B) Proprietary Opacity: Most forensic tools and AI models are proprietary. The responsible official often has no legal right to see the source code of the tool they are certifying[19].

(C) The UK Comparison: The UK recognized this futility and repealed Section 69 of the PACE 1984[20]. They moved to a Presumption of Reliability[21], shifting the burden to the challenger. By retaining the certificate, the BSA has ensured that Indian trials will remain bogged down in the Certificate Fetishism that has plagued our courts for twenty years, where the format of a signature is more important than the truth of the crime[22]. We are asking investigators to sign a statement that they are technically incapable of verifying.

[18] Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249 (2008).
[19] Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343 (2018).
[20] Police and Criminal Evidence Act 1984, c. 60, § 69 (UK) (repealed).
[21] Civil Evidence Act 1995, c. 38, § 8 (UK).
[22] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

V. DEEPFAKES, SYNTHETIC MEDIA, AND THE EROSION OF TRUTH

5.1. THE SILENCE OF THE BSA ON GENERATIVE AI

We have entered the post-truth era of deepfakes, where the evidence of the eyes is no longer reliable. The BSA is dangerously silent on Synthetic Media. Treating a deepfake of a confession and a real video of a confession as identical electronic records[23] is a recipe for judicial disaster. The law assumes that if the storage is verified, the content is true. This is a fatal flaw in the age of AI.

5.2. THE 'LIAR'S DIVIDEND' AND THE BURDEN OF PROOF

Section 22 of the BSA allows oral evidence on the contents of electronic records only when the genuineness is questioned. This creates what scholars call the Liar's Dividend: a guilty party can now easily claim that real evidence is AI-generated to create reasonable doubt[24].

(A) The Authenticity Crisis: How does a judge, untrained in forensics, decide if a video is a deepfake? The BSA suggests expert opinion (Section 39), but in an adversarial system, you will have two experts with two different opinions.

(B) Proposal for Technological Provenance: The Indian courts must move beyond the BSA's silence. We must require Cryptographic Watermarking and Hash History as a prerequisite for digital evidence[25]. Without a mandate for Provenance, the BSA's elevation of digital records to primary evidence actually makes the system more vulnerable to sophisticated forgery[26]. We are essentially handing the keys of the courtroom to those with the best AI-generation tools.

VI. TRANSNATIONAL DATA AND THE DELETION OF 'INDIA'

6.1. THE JURISDICTIONAL VACUUM

The BSA's removal of the definition of India (formerly Section 3 of the IEA) acknowledges the borderless nature of the internet[27]. But this creates a Chain of Custody nightmare for

[23] Robert Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).
[24] Bobby Chesney & Danielle Citron, Deepfakes and the New Disinformation War, Foreign Aff. (2019).
[25] European Parliament and Council, Artificial Intelligence Act, 2024/1689 (EU).
[26] Paul Grimm et al., Authenticating Digital Evidence, 69 Baylor L. Rev. 1 (2017).
[27] Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 Stan. L. Rev. 1005

investigators.

6.2 The Data Haven Loophole

If evidence is generated on a server in a jurisdiction with no data protection laws, can a Section 63 certificate from an Indian official truly validate it?[28] The BSA simplifies admissibility but ignores verifiability. We are now admitting global data with local and often inadequate, forensic safeguards[29].

(A) Mutual Legal Assistance (MLATs): The BSA fails to harmonize with international data-sharing treaties. If an Indian police officer cannot get a certificate from a Google admin in California, the evidence is technically inadmissible under Section 63, even if it is clearly relevant. This is a invitation for digital evidence laundering, where data is moved across jurisdictions specifically to evade the rigid certification rules of the BSA.

VII. REIMAGINING HEARSAY: THE MACHINE AS A WITNESS

7.1. THE CROSS-EXAMINATION DILEMMA

The core of the adversarial system is the right to confront your accuser[30]. But what if your accuser is an algorithm?

(A) Hearsay by Proxy: The BSA treats machine logs as Documents. This allows a human witness to testify about what a machine found, without the defence being able to cross-examine the algorithm's bias or error rate[31].

(B) Algorithmic Bias: Research shows that facial recognition and predictive policing algorithms are often biased against marginalized communities[32]. If we treat these outputs as facts rather than testimony, we are embedding systemic bias into the heart of the Indian justice system.[33]

(2010).
[28] Paul Schiff Berman, Global Legal Pluralism (2012).
[29] George L. Paul, Foundations of Digital Evidence (2008).
[30] Kenneth W. Graham, Jr., The Right of Confrontation and the Hearsay Rule: Sir Walter Raleigh Loses Another One, 8 Crim. L. Bull. 99 (1972).
[31] Christian Chessman, A "Source" of Error: Computer Code and the Hearsay Rule, 48 Hofstra L. Rev. 1 (2019).
[32] Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (2018).
[33] Brian Leiter, The Epistemology of Admissibility: Why Even Good Philosophy of Science Would Not Make

(C) The Silent Witness Theory: In some jurisdictions, machine output is treated under the Silent Witness theory, where the machine is viewed like a camera. But a camera only records, an AI interprets. The BSA fails to see the difference between a recording and an interpretation, leading to a dangerous admission of automated prejudice as objective truth.

VIII. CONSTITUTIONAL DIMENSIONS: ARTICLE 21 AND 20(3)

8.1. THE RIGHT TO A FAIR TRIAL (ARTICLE 21)

If a person is convicted based on a machine log that is protected by Trade Secret laws (preventing the defence from seeing the code), the trial is no longer fair in the sense of Article 21[34]. The BSA fails to provide a Code-Discovery mechanism for the defence[35]. This creates a fundamental Inequality of Arms: the state can use proprietary algorithms for prosecution, but the citizen cannot scrutinize them for defence.

8.2. Digital Self-Incrimination (Article 20(3))

In the age of the Internet of Things (IoT), our devices are constantly testifying against us[36]. Does extracting data from a person's smartwatch or a connected pacemaker constitute compelling a person to be a witness against himself?[37] The BSA is silent on the Digital Right to Silence.

8.3. The Biometric Breach: If a machine is an extension of the person's biology, the BSA's rules on digital admissibility may inadvertently bypass the constitutional protections of Article 20(3). We are sleepwalking into a world of biometric prosecution without any corresponding biometric rights.

IX. JUDICIAL EVOLUTION: TRACING THE CHAOS OF DIGITAL CERTIFICATION (2000-2024)

10.1. THE INFORMATION TECHNOLOGY ACT AND THE BIRTH OF SECTION

for Good Philosophy of Evidence, 1997 BYU L. Rev. 803 (1997).
[34] Hock Lai Ho, A Philosophy of Evidence Law: Justice in the Search for Truth (2008).
[35] Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343 (2018).
[36] Nita A. Farahany, The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology (2023).
[37] Larry Laudan, Truth, Error, and Criminal Law: An Essay in Legal Epistemology (2006).

65B

The journey began with the IT Act, 2000, which introduced Section 65B to the IEA. For the first time, India acknowledged electronic records. However, the language was clunky, borrowed from the UK's outdated PACE 1984. The legislature did not anticipate the mobile revolution, let alone the AI revolution.

10.2. THE ERA OF CONFUSION: NAVJOT SANDHU (2005)

In ***State (NCT of Delhi) v. Navjot Sandhu***, the Supreme Court held that Section 65B was not mandatory[38]. If a certificate was missing, oral evidence could fill the gap. This led to a decade of Forensic Wild West where unverified printouts and manipulated call logs were admitted as evidence without any technical scrutiny. This era compromised the integrity of hundreds of criminal trials.

10.3. THE RADICAL U-TURN: ANVAR P.V. (2014)

The Court realized its mistake and overruled *Sandhu*. In ***Anvar P.V. v. P.K. Basheer*****,** the Court declared Section 65B mandatory[39]. No certificate, no evidence. This brought discipline but created a massive bottleneck. Legitimate evidence (like a victim's text message) was being thrown out because they didn't have a certificate from a mobile provider that no longer existed.

10.4. THE CONFLICT: SHAFHI MOHAMMAD (2018)

A two-judge bench tried to relax the *Anvar* rule for parties who didn't have access to the device[40]. This created a conflict between two Supreme Court benches, leaving lower courts in a state of paralysis for two years.

10.5. THE FINAL WORD (IEA): ARJUN KHOTKAR (2020)

A three-judge bench settled the matter[41]. Certification is mandatory, but if the party has done everything in their power to get it and the authority refuses, the court can waive the requirement. This was a pragmatic solution, but it placed a massive investigative burden on the

[38] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[39] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[40] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[41] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

party seeking to admit the evidence.

10.6. THE BSA SOLUTION: SECTION 63

The BSA attempts to codify, but fails to address the fundamental problem: Who is a 'responsible official' for a decentralized cloud server? By retaining the certificate, the BSA has ensured that the Certificate Crisis will continue into the AI era. We have simply changed the section number (65B to 63) while ignoring the twenty years of chaos that preceded it.

X. THE FUTURE OF FORENSIC TRUTH: FROM HASH TO MAC

11.1. THE SCIENCE OF AUTHENTICATION

The BSA mentions HASH values in its schedule. A HASH value is a digital fingerprint (MD5, SHA-256). If even one-bit changes, the HASH changes. This is the only true way to verify digital integrity[42].

11.2. THE FAILURE OF SECTION 63 TO MANDATE HASHING

While the BSA mentions HASHING, it does not mandate it. It still allows a human to sign a paper certificate. In a digital world, a paper certificate is useless without a HASH value comparison.

11.3. THE FORENSIC GAP: The BSA should have mandated that for any Primary electronic record, the HASH value must be recorded at the time of seizure. Without this, the Section 63 certificate is just a piece of paper vouching for a system that could have been compromised at any point in the chain of custody. We are using 20th-century bureaucracy to verify 21st-century mathematics.

XI. SUGGESTIONS FOR LEGISLATIVE AND JUDICIAL REFORM

12.1. TRANSITION TO ALGORITHMIC AUDITABILITY AND CODE DISCOVERY

Courts must move beyond the Master-Slave metaphor of human-machine interaction. In cases where algorithmic output forms the basis of a charge (e.g., predictive policing or facial

[42] Paul Grimm et al., Authenticating Digital Evidence, 69 Baylor L. Rev. 1 (2017).

recognition), the defence must be granted a statutory Right to Code Discovery. This would allow independent experts to audit the software for systemic bias or logical errors, overriding the Trade Secret defence that currently shields proprietary systems from constitutional scrutiny[43].

12.2. MANDATORY CRYPTOGRAPHIC PROVENANCE AND WATERMARKING

To combat the Grok-Era deepfakes, the BSA should be amended to include a Negative Presumption for unverified digital media. Any electronic record that lacks a verifiable cryptographic watermark or an immutable HASH trail at the time of its creation/seizure should be demoted from Primary Evidence to Secondary Evidence, requiring extensive corroboration. This aligns India with the EU AI Act's transparency requirements[44].

12.3. RECOGNITION OF 'NON-HUMAN DECLARANTS'

The judiciary must adopt a Machine Testimony Doctrine similar to the US model. By recognizing that autonomous machines are not hearsay declarants, the law can stop the charade of human certification. Admissibility should depend on the Verification of the Process (how the data was generated) rather than the Accountability of the Official (who signed the paper).

12.4. HARMONIZING THE BSA WITH THE DPDP ACT

A Privacy-Admissibility Guardrail is required. Evidence obtained in gross violation of the DPDP Act, 2023, without a judicial warrant or pressing public interest, should be made per se inadmissible. This would prevent the Privacy-Evidence Paradox where the state incentivizes the violation of data protection norms to secure convictions.

XII. CONCLUSION: DE-GHOSTING THE MACHINE

The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023, is a journey from the Ink-and-Paper world of the Raj to the Cloud-and-Code world of the Digital Republic. However, the current iteration of the BSA is a statute of Colonial Architecture with a Digital Facade. By retaining the human-centric certification requirement of Section 63, the legislature has successfully modernized the law’s lexicon while failing to update its

[43] Rebecca Wexler, 70 Stan. L. Rev. 1343 (2018).
[44] European Parliament and Council, 2024/1689 (EU).

underlying evidentiary philosophy.

The Ghost in the Machine represents the autonomous data that currently haunts our courtrooms data that is admitted as truth but remains un-scrutinize under Victorian rules of accountability. As we have seen through the lens of the Grok AI controversies and the Jeffrey Epstein synthetic files, the Epistemic Crisis of the digital age is not just about lies, it is about the erosion of our collective ability to distinguish between a fact and an algorithmic projection.

For the BSA to fulfil its promise of decolonization, it must move beyond linguistic rebranding. It must recognize that in a post-human world, truth-finding is no longer a search for a credible witness but a search for Algorithmic Integrity. The law of evidence must evolve from a system that asks ***Who can we blame for this record?*** to one that ask **How can we mathematically verify this process**.

Only by embracing cryptographic provenance, code-discovery rights and inter-statutory harmony with privacy laws can the Indian legal system de-ghost the machine. The search for justice in the 21st century is no longer a search for a person's memory, but a search for the integrity of the code that now defines our reality. The BSA is a necessary first step, but without these reforms, it risks becoming an archaic artifact of the very era it seeks to replace.