SCOPE OF ELECTRONIC EVIDENCE: DIGITAL FORENSICS, DATA INTEGRITY, AND TECHNOLOGICAL FRONTIERS

Mridul Bhatt, LL.M. (Cyber and Security Law), ICFAI University Dehradun, Uttarakhand[1]

ABSTRACT

Under the Bharatiya Sakshya Adhiniyam (BSA) 2023, the standard for admitting digital evidence is no longer just about producing a file — it is about proving how that file was collected, preserved, and transported from the crime scene to the courtroom. The law's requirement that electronic records be "primary evidence" has made forensic method central to admissibility: courts now demand a full bit-stream copy — a mathematical mirror image of an entire storage device, capturing even deleted files and hidden data — rather than a simple copy-paste, because the latter alters timestamps and destroys latent data, technically amounting to contamination. Cryptographic hash values, particularly SHA-256, serve as the judicial stamp of integrity, proving a file is untouched since collection; however, this tool is "content-blind" — it confirms the container is intact but cannot detect whether the content inside was AI-generated before it was ever hashed, leaving courts fatally exposed to deepfakes. Social media and encrypted messaging evidence compounds this problem: WhatsApp and Signal use end-to-end encryption meaning even the platforms cannot read the messages, forcing courts into a constitutional standoff between demanding decryption keys and the accused's right against self-incrimination under Article 20(3). Cloud-stored evidence adds a sovereignty layer — data scattered across foreign servers requires Mutual Legal Assistance Treaties that routinely take 12–18 months, by which time logs are overwritten and evidence lost. Blockchain records and IoT data from smart homes and wearables push this further still, as neither fits the BSA's assumption that a named human custodian can certify the "original" source, revealing that India's otherwise progressive evidentiary law was drafted with a smartphone in mind, not a decentralised network or a smart refrigerator.

Keywords: Digital Forensics, Electronic Evidence Admissibility, Chain of Custody, Data Integrity, Deepfakes and AI-Generated Evidence

[1] LL.M. Cyber and Security Law, ICFAI University Dehradun, Uttarakhand, India

1.1. The Science of Digital Proof: Bit-stream Copies and Forensics Images

In the "post-BSA era," the admissibility of electronic evidence has transitioned from a question of mere procedure to a rigorous inquiry into forensic science. The *Bharatiya Sakshya Adhiniyam (BSA), 2023*, creates a distinct legal ecosystem where the "originality" of data is paramount. This is legally codified in the reclassification of electronic records as "Primary Evidence" under Section 57[2]. However, for a digital record to command the status of primary evidence, it must withstand the forensic scrutiny of "originality," which relies heavily on the technical distinction between a "Logical Copy" and a "Bit-Stream Copy."

In traditional legal practice, a photocopy of a document is accepted as a faithful reproduction. In the digital realm, however, a standard "copy-paste" operation (a logical copy) is legally insufficient for forensic purposes. A logical copy only captures "active data"—the files visible to the user—while failing to capture latent data such as deleted files, hidden partitions, or file fragments located in the "slack space" and "unallocated clusters" of the hard drive. Furthermore, a logical copy inherently alters critical system metadata, such as the "Last Accessed" timestamp, effectively contaminating the evidence at the moment of collection. This alteration, though unintentional, technically constitutes "tampering," rendering the evidence vulnerable to exclusion under the strict conditions of Section 63(2) of the BSA, which demands that the computer output be a faithful reproduction of the original[3].

To satisfy the evidentiary burden in 2026, forensic protocols necessitate the creation of a "Bit-Stream Copy" or a "Forensic Image." This process involves a bit-by-bit replication of the source media, copying every binary digit (0 and 1) from the first sector to the last. This creates a mathematically identical "mirror image" of the storage device, preserving not just the visible files but the entire digital environment, including the "digital residue" of past user activity. By capturing the ambient data, forensic experts can reconstruct the "res gestae" of the digital crime—the context, sequence, and method of execution—providing the court with a holistic view that a simple file printout cannot. Defence counsels in the BSA era are increasingly challenging the admissibility of evidence where a bit-stream copy was not preserved, arguing that the failure to secure the "slack space" constitutes a break in the chain of custody, thereby violating the "proper custody" mandate required for Primary Evidence status.

[2] Section 57, The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
[3] Section 63(2), The Bharatiya Sakshya Adhiniyam, 2023.

1.1.1. How Indian Police and State Forensic Labs Create Bit-stream Images

On paper, the BSA speaks in general terms about "electronic records" and "computer outputs". In practice, these phrases now map onto quite specific workflows inside Indian police cyber cells and State Forensic Science Laboratories (SFSLs). Instead of informal copy-paste, investigators now rely on specialised suites like **Magnet AXIOM, Cellebrite UFED and Forensic Toolkit (FTK)** to acquire evidence in a forensically sound way.

Magnet AXIOM is a commercial tool that can pull evidence from computers, smartphones and certain cloud services into a single case file. During acquisition it can create full forensic images from Windows and macOS systems, as well as from many mobile devices. At the same time, it calculates hash values (for example, SHA-256 and MD5) and starts parsing artefacts such as chat messages, browser history, cloud account activity and system logs. AXIOM is designed to work at the level of artefacts rather than just raw files, which means that it actively looks into slack space and unallocated clusters to recover deleted or partially overwritten data. From an evidentiary angle, this goes well beyond a simple file copy and is much closer to what Section 57 of the BSA expects when it speaks of primary electronic evidence.[4]

For mobile phones, Cellebrite UFED has become one of the most visible tools in India. Investigative reporting by MediaNama shows that Maharashtra Cyber, Hyderabad Police and other agencies have acquired and used UFED devices to unlock and extract data from a wide range of smartphones, including iPhones. UFED can perform physical and advanced logical extractions, which means it does not just read what the phone shows on the screen, but attempts to access the underlying storage directly. In practice, this results in images that contain not only current chats and photos but also deleted messages, app databases, call logs and other hidden artefacts which would otherwise not be preserved.[5]

On the computer side, many SFSLs and cyber units rely on FTK Imager and the full Forensic Toolkit (FTK) suite. FTK Imager is used to create sector-by-sector images of hard disks, SSDs and removable media, while FTK itself is then used to index, search and analyse those images. The manufacturer's documentation emphasises features such as automatic hashing during imaging, detailed acquisition logs and "defensible" workflows that can later be explained in

4 https://www.ijfmr.com/papers/2024/6/30679.pdf (last accessed on 12.02.2026 at 5:36 pm)
5 https://www.medianama.com/2022/03/223-how-indian-law-enforcement-uses-phone-cracking-tools-2/ (last accessed on 12.02.2026 at 5:45 pm)

court. These features directly support the BSA's requirement that a computer output be demonstrably identical to its source.[6]

In serious cases, the police do not work in isolation. Devices are usually imaged at SFSLs or at the National Cyber Forensic Laboratory (NCFL) under I4C, rather than at ordinary police stations. Cyber cells handle seizure and basic preservation, while the laboratories contribute the technical expertise and infrastructure. Ideally, this division of roles reduces the risk of tampering and makes it easier to narrate the chain of custody in court, because the number of people who actually interact with the raw data is limited and can be identified by name and role.[7]

1.1.2. Triage Tools and the Place of TINV

In theory, every seized device could be sent for a full bit-stream image as soon as it is seized. In reality, Indian labs face a serious capacity problem: they simply cannot image and analyse every phone, laptop and USB drive that comes through the door within a reasonable time. To cope with this, many agencies have started using triage tools that allow trained officers to do a quick, controlled scan of a device to decide whether it needs full imaging.[8]

Tools like Triage-Investigator (often marketed as Triage-Investigator PRO) are designed for this purpose. They are usually run from a forensic USB stick or external environment, so that the suspect machine is not booted into its own operating system. The officer can then run pre-defined searches for relevant file types (e.g. pictures, spreadsheets), keywords, time ranges or known hash values, without making a complete copy of the disk. The goal here is not to finish the whole investigation on the spot but to decide which devices should be given priority at SFSL.[9]

From an evidentiary standpoint, this is a compromise between the ideal (everything is imaged) and the practical (labs have limited staff and hardware). If used correctly—meaning with write-blocking, proper logging and minimal on-disk changes—triage tools like TINV can help reduce backlogs, so that truly important devices are imaged and analysed in time. But they also

6 https://www.medianama.com/2022/03/223-how-indian-law-enforcement-uses-phone-cracking-tools/ (last accessed on 12.02.2026 at 5:45 pm)
7 https://i4c.mha.gov.in/ncfl.aspx (last accessed on 12.02.2026 at 5:48 pm)
8 https://papers.ssrn.com/sol3/Delivery.cfm/5226380.pdf?abstractid=5226380&mirid=1 (last accessed on 12.02.2026 at 5:54 pm)
9 https://digitalforensicsdubai.com/product/triage-investigator-pro/ (last accessed on 12.02.2026 at 5:58 pm)

come with risks. If officers use such tools casually, for example by booting devices normally or writing case notes into the same drive, the triage step itself can become a source of contamination. For this reason, high-quality triage tools stress that they are "forensically sound" and include configuration options that disable any write-back to the suspect media.

1.1.3. Evidence Alteration in Transit and at the Laboratory

Even when advanced tools are available, many Indian studies point out that the transit phase—the period between seizure and imaging—is often the weakest link in the chain of custody. Once a device is seized at the scene, it may be handled by the first responding officer, the station house officer, the district cyber cell, and only then by the SFSL or NCFL. Each transfer is a fresh opportunity for someone to interact with the device in a way that leaves unintended traces.[10]

Common mistakes include: turning a laptop on just to "check what is inside"; scrolling through a phone gallery to see if there are any "obscene" or "incriminating" photos; connecting a phone to an ordinary office computer to save some screenshots into the case diary; or leaving a seized device charging on a desk while it is still connected to the mobile network or Wi-Fi. Any of these actions can change log files, update apps, download new data from the cloud, or even trigger a remote wipe command if the suspect has set up such a feature.[11]

Laboratory conditions are not always ideal either. Academic and professional commentaries on Indian forensic practice describe overcrowded labs, limited secure lockers, and incomplete logging systems. In some SFSLs, digital evidence may be stored in general rooms, without continuous CCTV coverage, and without detailed access logs recording exactly which examiner accessed which drive at what time. Once again, this does not automatically mean that evidence has been manipulated, but it becomes difficult to rebut such an allegation if the documentation is thin.[12]

For a court applying the BSA, this poses a real problem. A bit-stream image created in the lab three weeks after seizure might be technically perfect, but if the defence can show that the

10 https://humanrightlawreview.in/wp-content/uploads/2025/05/The-Intersection-of-Digital-Forensics-and-Criminal-Investigation-in-India-Legal-and-Procedural-Dimensions-of-Evidentiary-Standard.pdf (last accessed on 12.02.2026 at 6:24 pm)
11 https://www.lawjournals.net/assets/archives/2025/vol7issue3/7067.pdf (last accessed on 12.02.2026 at 6:34 pm)
12 https://www.centurylawfirm.in/blog/the-role-and-admissibility-of-forensic-evidence-in-the-indian-criminal-justice-system/ (last accessed on 12.02.2026 at 6:34 pm)

device was handled casually during those three weeks—without Faraday isolation, without logs, and without early hashing—the prosecution will struggle to argue that the image enjoys the "proper custody" and "faithful reproduction" presumptions that primary electronic evidence is supposed to carry.

1.1.4. JTAG and Chip-off as Last-Resort Imaging Methods

There are many cases where normal imaging tools like AXIOM or UFED cannot access a device in the usual way. The screen may be shattered, the USB port may not work, the operating system may be corrupted, or the phone may have been deliberately damaged by the suspect. In such situations Indian labs and specialist vendors increasingly rely on **JTAG and Chip-off techniques**.[13]

JTAG forensics uses the Joint Test Action Group hardware debugging interface that many phone manufacturers leave on their circuit boards. The examiner opens the device, identifies the relevant test pads, solders fine wires to them and connects the board to a JTAG controller. If successful, this allows the examiner to read the contents of the memory chip directly, without booting the operating system. In effect, it is a hardware-level way of doing a bit-stream image, and it can work even when the screen or other components are damage.[14]

Chip-off forensics goes a step further. Here, the memory chip itself is physically removed (desoldered) from the board, cleaned, and placed into a chip reader that extracts a raw binary image. This method is destructive: once the chip is removed, the original phone will never work again. However, published case studies show that Chip-off can successfully recover SMS messages, call logs and application data from heavily damaged phones that would otherwise be considered beyond repair.[15]

Because JTAG and Chip-off involve direct physical manipulation, they raise particularly sharp questions about tampering and transparency. Defence lawyers can argue that a person who has the skills and tools to desolder a chip also has the skills and opportunity to alter or insert data at that level. To reduce this risk, forensic guidelines insist on strict documentation: high-quality photos of the device and board before and after the procedure, continuous video recording of

13 https://www.ijprems.com/ijprems-paper/data-recovery-using-chip-off-forensics-with-jtagufi-tool (last accessed on 12.02.2026 at 6:46 pm)
14 https://journal.nielit.edu.in/index.php/01/article/download/104/35/261 (last accessed on 12.02.2026 at 6:57 pm)
15 https://journal.nielit.edu.in/index.php/01/article/download/104/35/261 (last accessed on 12.02.2026 at 6:59 pm)

soldering and desoldering, detailed written logs of each step, and immediate hashing and write-protected storage of the extracted image. Where such precautions are followed and can be shown to the court, JTAG and Chip-off images can be treated as reliable last-resort equivalents of more routine bit-stream copies.[16]

1.2. Hash Values (SHA-256): The Digital Fingerprint as a Legal Standard

If the forensic image represents the *corpus delicti* (body of the crime), the "Hash Value" serves as its immutable digital fingerprint. The BSA framework relies heavily on cryptographic hash functions to ensure data integrity. A hash function is an algorithmic process that maps data of any size to a fixed-size string of characters. In modern forensic practice, the SHA-256 (Secure Hash Algorithm) standard is the benchmark.

The legal potency of the hash value lies in its "Avalanche Effect." This cryptographic property ensures that a microscopic alteration to the input data—such as changing a single pixel in a video or a comma in a document—results in a completely different, non-correlating hash value. This provides the judiciary with a mathematical guarantee of integrity that human testimony cannot match. Under the *Arjun Panditrao* regime, and continuing into the BSA framework, the verification of hash values has become a standard condition for admissibility[17]. When a device is seized, a "seizure hash" is generated; when the evidence is produced in court, a "verification hash" is computed. A match between these two values is scientifically irrefutable proof that the data has not been tampered with during custody.

However, this reliance on hashing creates a "fragility of evidence" paradox. While hash values protect against tampering, they also render digital evidence brittle. Legitimate forensic interactions, such as booting up a seized laptop without a hardware "Write-Blocker," can alter system files and change the hash value. Consequently, courtroom debates in 2026 have shifted from substantive questions of guilt to technical disputations regarding "hash mismatches". Furthermore, while the hash value proves that the file has not changed *since* it was hashed, it remains "content-blind". It validates the integrity of the file container but cannot verify the veracity of the content itself. This limitation is critical in the context of the "Deepfake Crisis," where a perfectly hashed, untampered file may still contain AI-generated fabrications, allowing

16 https://journal.nielit.edu.in/index.php/01/article/download/104/35/261 (last accessed on 12.02.2026 at 7:09 pm)
17 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

defendants to exploit the "Liar's Dividend" by casting doubt on genuine evidence.

1.2.1. Automatic Hashing in Tools like AXIOM, FTK and UFED

In modern practice, computing hashes is no longer an optional extra; it is built directly into the tools. Magnet AXIOM automatically calculates SHA-256 (and, if configured, MD5 and SHA-1) when it acquires an image. These hash values are stored as part of the case metadata and are printed in the final forensic reports. Because they are generated automatically at acquisition, the risk that an examiner will "forget" to hash an image is greatly reduced.[18]

FTK Imager works in much the same way. When an examiner images a disk, FTK Imager immediately calculates one or more hash values and stores them in the log. Later, FTK can verify that the stored image still has the same hash, which gives confidence that the file has not been corrupted or altered during storage or transfer.[19]

On the mobile side, Cellebrite UFED generates hash values for its extractions and includes them in detailed extraction reports. These reports have already been relied upon in Indian cases involving cybercrime and serious offences, where the defence was given a copy of the extraction along with the hashes so that they could verify the integrity independently.[20]

This kind of automated, tool-level hashing is important for BSA compliance because it gives courts more than just the examiner's word. It provides a clear, machine-verifiable record of what the "original" looked like, which can be checked by calculation at any later point in the trial.

1.2.2. Hash Mismatches and the "Transit Problem"

Despite these improvements, hash mismatches still occur. Indian scholarship on digital forensics identifies the main cause as improper handling between the time a device is seized and the time it is imaged.[21]

For example, if an officer at the police station powers on a laptop to see "what is there" before

18 https://www.magnetforensics.com/products/magnet-axiom/ (last accessed on 12.02.2026 at 7:21 pm)
19 https://www.exterro.com/digital-forensics-software/forensic-toolkit (last accessed on 12.02.2026 at 7:29 pm)
20 https://scroll.in/article/1019695/why-phone-cracking-tools-used-by-indias-law-enforcers-are-increasingly-raising-privacy-concerns (last accessed on 12.02.2026 at 7:35 pm)
21 Ibid.

it reaches the lab, the operating system may update logs, change last-accessed times, or install patches. If a preliminary hash was computed immediately after seizure, that hash will no longer match the hash obtained when the lab makes an image a few days later. Unless there is very clear documentation of what happened in between, the defence can argue that this unexplained difference proves that the evidence has been altered.[22]

Under the BSA, courts are no longer willing to ignore such mismatches as mere "technicalities". Section 63(2) demands that the computer output be a faithful reproduction; if the prosecution cannot give a convincing account of why the hash changed, the logical inference is that the reproduction might not be faithful at all. Some academic commentary warns that this could lead to more acquittals in cyber cases, not because the accused are innocent, but because procedural irregularities create enough doubt about the integrity of the evidence.[23]

1.2.3. Documentation Burden and Limited Resources

The BSA also adds to the paperwork of forensic work. Under Section 63(4), any computer output that is tendered as evidence must be accompanied by a certificate from a responsible person explaining how it was produced. For labs, this means that examiners have to record not only the hash values but also the exact tools used, their versions, the date and time of imaging, the hardware used, and any deviations from the standard SOPs.[24]

Reports on NCFL and State labs show that preparing such certificates and maintaining BSA-compliant logs can take up a large part of an examiner's working time. When lab staff are already few in number and overloaded with cases, this documentation burden contributes to delays. There is a real danger that, to clear backlogs, investigators will quietly fall back on quick screenshots or partial exports for lower-priority cases, even though such methods are much easier to challenge under the BSA.[25]

22 Ibid.
23 https://www.ijfmr.com/papers/2024/6/30679.pdf (last accessed on 12.02.2026 at 7:41 pm)
24 https://www.centurylawfirm.in/blog/the-role-and-admissibility-of-forensic-evidence-in-the-indian-criminal-justice-system/ (last accessed on 12.02.2026 at 7:46 pm)
25 https://www.ijprems.com/ijprems-paper/data-recovery-using-chip-off-forensics-with-jtagufi-tool (last accessed on 12.02.2026 at 7:51 pm)

1.3. Metadata Analysis: Proving Context, Authorship, and Chronology

Beyond the visible content of a file lies "Metadata"—the data about data. In the absence of physical eyewitnesses in cybercrimes, metadata acts as the silent witness, crucial for establishing the "mens rea" (guilty mind) and "actus reus" (guilty act). Under the BSA, metadata is pivotal for proving three elements: Context, Authorship, and Chronology.

Authorship: In cases of anonymous cyber-stalking or defamation, metadata provides the digital link to the perpetrator. "Application Metadata" embedded within files (e.g., Microsoft Word documents or JPEG images) often contains the "Author Name," "Device Model," or "GPS Coordinates" (Geotags) of where the file was created.

Chronology: In conspiracy cases, the sequence of events is vital. Metadata fields such as "Date Created," "Date Modified," and "Date Accessed" provide an objective timeline that exists independently of human recollection. This forensic timeline is essential to corroborate or refute alibis.

However, the forensic reliance on metadata is fraught with challenges. The primary threat is "Time-Stomping"—a sophisticated anti-forensic technique used to alter timestamps. A knowledgeable perpetrator can modify the system clock or use specialized utilities to backdate incriminating files, making them appear to have been created prior to a crime. While "System Metadata" (generated by the Operating System) is harder to forge than "Application Metadata," discerning the difference requires high-level expertise. The "Expert Bottleneck" identified in Chapter 2 is severely felt here; the nuanced interpretation of conflicting metadata layers requires a forensic acumen that is scarce within the current investigation infrastructure. Without a qualified expert to interpret the "MAC times" (Modified, Accessed, Created), courts risk misinterpreting the timeline of events.

1.4. Chain of Custody: Standard Operating Procedures (SOPs) for Police Seizure under BNSS

The integrity of digital evidence is inextricably linked to the Chain of Custody. With the enactment of the *Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023*, the police powers of search and seizure have been expanded, necessitating strict Standard Operating Procedures

(SOPs) to prevent contamination[26].

The digital chain of custody differs fundamentally from the physical one. It involves not just the security of the hardware, but the isolation of the signal. The "Golden Rule" of digital seizure in 2026 is the immediate isolation of the device from all networks to prevent "Remote Wiping." If a seized smartphone remains connected to a cellular or Wi-Fi network, a suspect (or an accomplice) can issue a remote "kill command" (e.g., via iCloud or Google Find My Device), erasing all evidence before the device reaches the forensic lab. To counter this, SOPs now mandate the use of "Faraday Bags"—shielded containers that block all radio signals—at the point of seizure

A critical failure point identified in recent legal analysis is the "First Responder Problem." Police officers, often the first to handle the device, may lack specialized training. Common errors, such as scrolling through a gallery to "check" for evidence or attempting to guess a passcode, can permanently alter dynamic system data and invalidate the hash value. Such actions compromise the integrity of the evidence before it is even certified, leading to exclusion under Section 63 conditions. Therefore, the BNSS mandates that seizure memos must now include technical specifics, such as the status of the device (powered on/off) and the hash value if generated on-site, to create an unimpeachable record of custody.

1.4.1. Custodial Infrastructure and Real-World Weaknesses

Beyond individual mistakes, there are structural problems in how many police stations and labs handle digital property. Commentaries and empirical studies note that seized phones, laptops and drives are often stored in the same malkhana as physical items, with paper registers that record little more than a general description of the item and the case number. Technical details such as battery state, connection status, serial numbers or visible screen content at the time of seizure are often omitted, making it impossible to reconstruct the original state later.[27]

Within SFSLs, similar issues arise. Examiners in some States operate with limited secure lockers, incomplete CCTV coverage and manual logbooks, all of which make it harder to prove that only authorised persons accessed the evidence. These systemic issues do not automatically

[26] The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India)
27 https://scroll.in/article/1019695/why-phone-cracking-tools-used-by-indias-law-enforcers-are-increasingly-raising-privacy-concerns (last accessed on 12.02.2026 at 7:58 pm)

mean that evidence is being forged, but they give defence counsel realistic grounds to raise doubts. When the prosecution cannot show an unbroken and well-documented chain of custody, courts may hesitate to treat digital exhibits as robust primary evidence, even if the technical analysis itself appears sound.[28]

1.4.2. Digital Evidence Response Teams (DERTs) and Network Isolation

In response to these concerns, policy discussions around the Indian Cyber Crime Coordination Centre (I4C) have pushed the idea of Digital Evidence Response Teams (DERTs). The idea is to create small, trained squads at regional level who are specifically responsible for handling digital devices at the seizure stage.[29]

DERTs are supposed to carry standard equipment: Faraday bags, hardware write-blockers, portable imaging tools, cameras for documenting device state, tamper-evident bags and basic documentation templates. Rather than every local officer improvising their own methods, the DERT can be called to the scene or to the station to take over responsibility for digital evidence.[30]

The central principles of such teams are:

1. Immediate network isolation (by switching to airplane mode, turning the device off when appropriate, or placing it in a Faraday bag).

2. Minimum interaction with the device's user interface, especially in locked or encrypted devices.

3. Early hashing where equipment allows it, so that a "seizure hash" is on record before any transport or further interaction occurs.

Reports suggest that some metropolitan forces—such as those in Delhi, Mumbai and Hyderabad—have made more progress towards such specialised units than smaller or rural jurisdictions. This produces an uneven landscape in which the quality of digital evidence handling, and therefore the strength of the prosecution's case, can vary significantly depending

28 Ibid.
29 https://www.ijprems.com/ijprems-paper/data-recovery-using-chip-off-forensics-with-jtagufi-tool (last accessed on 12.02.2026 at 8:09 pm)
30 Ibid.

on where the crime happens. From a constitutional perspective, this raises questions of equality before the law, because accused persons in well-resourced jurisdictions may face stronger, better-handled electronic evidence than those in under-resourced areas.[31]

1.5. Identifying and Preventing Digital Tampering: Techniques and Tools

The ultimate challenge for digital forensics under the BSA is the detection of "Anti-Forensics"—techniques employed specifically to thwart forensic analysis. As the legal standards for admissibility tighten, the methods of tampering have evolved in sophistication, requiring courts to be vigilant against deceptive practices.

Steganography: This is the art of concealing data within other data. A suspect may hide a text file containing criminal conspiracy plans inside the binary code of a harmless image or audio file. To the naked eye, and often to standard hash checks of the "carrier" file, the evidence appears benign. Only through specialized "steganalysis" tools can the hidden payload be detected.

Data Wiping: Beyond simple deletion, suspects use "Secure Deletion" tools that overwrite data clusters with random binary patterns multiple times. This makes recovery via bit-stream copies impossible, destroying the evidence permanently.

The Deepfake Crisis: The apex of digital tampering in 2026 is the proliferation of AI-generated content. Current forensic tools that rely on analysing pixel inconsistencies or compression artifacts are struggling to keep pace with Generative Adversarial Networks (GANs) that continuously "learn" to avoid detection. This leads to the "Crisis of Trust" identified in the Problem Statement. The law can verify that a video file came from the suspect's phone (via Chain of Custody) and has not been altered since seizure (via Hash Value). However, the current framework struggles to verify if the content itself is a fabrication generated *before* the seizure. This gap—where the law authenticates the *container* but cannot definitively validate the *content*—remains the most significant forensic challenge in the BSA era, creating a "content-blind" spot in the judicial vision.

31 Ibid.

1.6. Admissibility of Social Media and Encrypted Messaging (WhatsApp, Signal)

In the contemporary theatre of criminal litigation, the evidentiary landscape has shifted seismically from physical artifacts to digital footprints. The "smoking gun" of the 21st century is rarely a weapon seized from a crime scene; it is increasingly likely to be a digital artifact—a deleted WhatsApp message, a vanishing Signal chat, a retrospective Instagram story, or a geolocated tweet. The scope of the *Bharatiya Sakshya Adhiniyam (BSA), 2023*, is severely tested by the ephemeral, ubiquitous, and encrypted nature of these platforms. While Section 2(1) of the BSA broadly defines "electronic records" to encompass data generated, sent, received, or stored in electronic form, the practical admissibility of social media evidence faces a unique constellation of jurisprudential hurdles that the *Indian Evidence Act (IEA)* never contemplated.

The primary challenge plaguing the admissibility of social media evidence is the dichotomy between "Attribution" and "Anonymity." Unlike physical documents, where handwriting or signatures provide a nexus to the author, social media accounts can be created with pseudonyms, utilizing spoofed IP addresses or temporary "burner" numbers. Proving that a specific individual sat behind a keyboard and sent a specific message at a specific time is a forensic challenge that transcends the mere production of screenshots. In the context of the BSA, a screenshot is merely secondary evidence of a digital display; it captures the *visual representation* of data but lacks the underlying *forensic integrity*—the metadata, server logs, and IP headers—that constitute the "electronic record" itself[32]. Courts in the post-BSA era are increasingly skeptical of "printouts" or "screen-grabs" of social media posts, identifying them as easily manipulatable. The judiciary now demands the production of the "electronic record" in its raw form—data exports containing timestamps, user IDs, and session logs—certified under Section 63(4).

However, the retrieval of this raw data is complicated by the ubiquity of End-to-End Encryption (E2EE) on platforms such as WhatsApp, Signal, and Telegram. This technological architecture presents a "Black Box" dilemma for the judiciary. As observed in recent precedents, the content of the message is often inaccessible even to the service provider (the intermediary). This creates an evidentiary vacuum. While the "metadata" (the "who, when, and where") might be retained

[32] Section 2(1), The Bharatiya Sakshya Adhiniyam, 2023.

and accessible under data retention laws, the "corpus" of the conversation (the "what") is encrypted.

The BSA framework, particularly Section 63, presupposes the availability of the content for inspection and certification. When the content is locked behind encryption keys held exclusively by the user, the court is forced into a constitutional confrontation with the Right against Self-Incrimination. The critical legal question arises: Can the court compel a user to unlock their application or provide the decryption key to generate the "source" evidence? If the act of unlocking the phone or decrypting the app is viewed as "testimonial compulsion"—forcing the accused to communicate information based on their personal knowledge—it may violate Article 20(3) of the Constitution. Conversely, if the password is viewed merely as a "key" to a physical locker (the phone), it may be compelled. This remains a contentious frontier where the statutory demand for "Primary Evidence" under the BSA clashes violently with the technological architecture of privacy and the constitutional shield against self-incrimination.

Furthermore, the "ephemeral" nature of modern messaging—where messages are designed to disappear after viewing or after a set time—challenges the concept of "preservation." Section 63(2) conditions require the computer to be operating properly and storing data in the ordinary course. But when the "ordinary course" of the software is to *delete* data, the evidence is often destroyed before a warrant is even issued. This necessitates a new jurisprudential approach to "spoliation of evidence," asking whether the use of "disappearing messages" in the context of a criminal conspiracy constitutes a deliberate destruction of evidence, thereby drawing an adverse inference against the accused.

1.6.1. How Indian Agencies Extract Social Media and Messaging Evidence

Because of these technical and legal limits, Indian investigators lean heavily on forensic tools like Cellebrite UFED and Magnet AXIOM working together with State Forensic Labs. MediaNama's reporting shows that State police units have bought UFED devices specifically to "crack" phones and pull out data from WhatsApp, Signal and social media apps. Once a phone has been lawfully seized and properly isolated from the network, the usual practice is[33]:

33 https://www.medianama.com/2022/03/223-how-indian-law-enforcement-uses-phone-cracking-tools-2/ (last accessed on 12.02.2026 at 8:34 pm)

1. Send it to a cyber cell or SFSL that has UFED or an equivalent tool.
2. Perform a full physical or advanced logical extraction (where supported).
3. Generate a report showing chats, attachments, contacts, call logs and app data, with hash values and timestamps.

At the same time, Magnet AXIOM is used to process both the device extraction and any warrant returns from service providers. For example, if Meta or Google return JSON or CSV exports of account activity in response to a lawful request, AXIOM can import those files, parse out the timestamps and IDs, and add them into a combined timeline alongside device-level artefacts. This allows investigators to show, in one coherent view, that[34]:

- a WhatsApp account sent a message,
- the same account logged into a Facebook/Instagram profile, and
- those events line up with device connections and IP logs.

When properly documented and certified, such combined timelines are much more persuasive than isolated screenshots because they show internal consistency across multiple data sources.

1.6.2. Screenshots, Certificates and the Attribution Problem

Even with all these tools, the attribution problem remains central. Social media accounts can be created with pseudonyms, temporary SIMs and VPNs. Merely showing that a message came from a particular handle does not, by itself, prove that the accused sat behind the screen and typed it. Courts therefore look for corroborating circumstances:

- Was that handle consistently accessed from IP addresses associated with the accused's home or workplace?
- Do the device-level logs on the accused's phone show that account being used at the relevant time?

34 https://www.ijfmr.com/papers/2024/6/30679.pdf (last accessed on 12.02.2026 at 8:41 pm)

- Do friends, co-workers or co-accused confirm that the handle belongs to that individual?

Here again, tools like AXIOM and FTK assist by correlating metadata: matching device IDs, Wi-Fi networks, browser artefacts and app logs with server-side data. But the final step—drawing the inference that "this was the accused"—is still a legal and factual exercise, not a purely technical one.[35]

1.6.3. Disappearing Messages, Ephemeral Stories and Spoliation

Another special challenge posed by social media and encrypted messaging is ephemerality. Apps now routinely offer disappearing messages, "view once" media and time-limited stories. From a legal perspective, this raises the question whether the deliberate use of such features in a criminal conspiracy amounts to spoliation of evidence.

Under Section 63(2) of the BSA, a computer is expected to operate in the "ordinary course" when producing a computer output. But if the ordinary course of an app is to auto-delete messages after a short time, then the record may vanish before any complaint is filed or any warrant is issued. Some scholars argue that, when such features are used specifically to frustrate later investigation, courts should be willing to draw adverse inferences, treating the deliberate design of communication channels as part of the criminal plan. This remains an open area where doctrine is still catching up with technology.

1.7. Cloud Computing and Multi-Jurisdictional Data: The "Sovereignty" Challenge

The traditional concept of "jurisdiction" in criminal law is territorial, grounded in the physical borders of the nation-state. However, the architecture of Cloud Computing is inherently extraterritorial and distributed. This dichotomy creates the "Sovereignty Challenge" in the admission of electronic evidence under the BSA. When a financial crime is committed in New Delhi, the relevant electronic evidence—email logs, cloud backups, AWS server access histories, or Google Drive documents—may physically reside in a data centre in Dublin, California, or Singapore.

Under the BSA, Section 57 allows for electronic records to be treated as "Primary Evidence" if they are produced from "proper custody." However, the definition of "proper custody"

35 https://www.magnetforensics.com/products/magnet-axiom/ (last accessed on 12.02.2026 at 8:47 pm)

becomes nebulous in a cloud environment. In a distributed storage system (utilizing techniques like sharding), a single file is often split into multiple fragments and stored across different physical servers in different jurisdictions to ensure redundancy and speed. In such a scenario, where is the "original"? The BSA attempts to resolve this via the "Simultaneous Storage" explanation, suggesting that data stored on a cloud server is deemed to be in the custody of the user who accesses it. This legal fiction treats the user's *access* to the data as equivalent to the user's *possession* of the data.

Yet, the procedural mechanism for retrieving this data remains archaic and fraught with friction. Indian courts and investigating agencies still largely rely on Mutual Legal Assistance Treaties (MLATs) to request data from foreign jurisdictions. This process is notoriously bureaucratic and glacial, often taking months or even years to yield results. By the time the data is retrieved, the "digital volatility" of the cloud environment may have rendered the evidence corrupt, overwritten, or incomplete. The "Sovereignty Challenge" effectively creates a lag in the justice system—a temporal gap between the commission of the crime and the acquisition of the proof.

While the BSA modernizes the *definition* of evidence to include cloud-based records, it cannot unilaterally modernize the *international protocols* required to fetch it. Consequently, defence counsels in 2026 frequently mount challenges based on the "Chain of Custody." They argue that data retrieved from a foreign cloud server lacks a Section 63 certificate because the Indian investigating officer never physically handled the "source" server. The officer cannot certify the "integrity" of a server rack sitting in California that they have never seen. This forces the court to rely on "Foreign Certificates" or affidavits from the legal representatives of tech giants (like Meta or Google), introducing a layer of hearsay that is difficult to cross-examine. The tension between the BSA's strict certification requirements and the borderless reality of cloud data remains one of the most significant impediments to swift justice.

1.7.1. MLATs, Delays and Reluctance of Foreign Giants

At present, Indian agencies mostly rely on Mutual Legal Assistance Treaties (MLATs) and similar diplomatic channels to obtain data from major foreign providers like Meta, Google, Apple or Microsoft. A detailed study by the Centre for Internet and Society (CIS) found that MLAT requests to US-based companies frequently take 12–18 months to be processed, and many are rejected or returned for technical reasons. By the time data is handed over, logs may

have been rolled over, accounts may have been deleted, and the evidentiary value may be badly diminished.[36]

Apart from delays, there is also a more general reluctance on the part of foreign giants to cooperate beyond what their domestic law strictly requires. Providers must comply with privacy and data-protection laws in their home jurisdictions, and some of those frameworks make it difficult to hand over user data to foreign authorities unless strict conditions are met. This has led some commentators to describe the situation as a form of "digital colonialism", where the data of Indian users, and even critical infrastructure, is stored abroad and controlled by foreign legal systems.[37]

1.7.2. From IP-Based Thinking to Network-Centric Analysis

Traditional thinking often treated IP addresses as a kind of "digital fingerprint". If investigators could show that a certain IP was used in a crime, that was seen as strong evidence of identity. This idea is now widely recognised as too simple. VPNs, Tor, shared Wi-Fi and mobile NAT setups mean that a single IP can represent many users, and a single user can easily "hop" through multiple IPs.

Consequently, there is a shift towards network-centric forensics. Instead of treating IP logs as decisive in isolation, investigators look at the entire pattern of connections: which accounts logged in, from which devices, at which times, using which VPN or proxy services, and how these patterns line up with local device artefacts. Tools and services that specialise in network forensics, including some Indian providers, allow examiners to reconstruct session-level traffic, detect use of anonymisation tools and correlate local logs with ISP records.[38]

The focus is therefore no longer on "this single IP proves you did it", but on "this network of connections and devices is consistent with your known behaviour and contradicts your explanation". This is an important conceptual shift, and it goes hand in hand with the increased use of OSINT and cloud-forensic tools mentioned earlier.

36 https://cis-india.org/internet-governance/files/mlat-report (last accessed on 12.02.2026 at 9:16 pm)
37 https://www.docullyvdr.com/blog/data-room/digital-colonialism-are-you-letting-foreign-servers-control-your-corporate-secrets/ (last accessed on 12.02.2026 at 9:26 pm)
38 https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-network-forensics/ (last accessed on 12.02.2026 at 9:39 pm)

1.7.3. OSINT as a Partial Workaround for Sovereignty Gaps

Given the time and uncertainty involved in formal MLAT channels, Indian investigators often turn to Open Source Intelligence (OSINT) as an immediate, if partial, workaround. OSINT does not give access to private server logs, but it can reveal a surprising amount through public traces: usernames, public posts, leaked databases, domain registrations, forum activity, and so on.[39]

Companies like Innefu offer platforms that monitor and analyse social media, forums and other open sources in real time. Their tools, such as “Innsight”, have reportedly been used by law-enforcement agencies in India to track radicalisation, identify protest organisers and map criminal networks. OSINT also helps in cross-border cases where suspects flee to other countries: investigators can track their open profiles, photos with geotags, and travel-related posts to infer location and associates even when no cloud provider has yet returned formal data.[40]

Of course, OSINT has limits. It only sees what is publicly visible, and much serious crime now happens behind E2EE and closed groups. It also raises its own privacy and free-speech questions. But in terms of evidentiary strategy, OSINT has become a crucial supplement to traditional, legally certified electronic records, especially when foreign servers and MLAT delays leave gaps in the official record.

1.8. The Deepfake Crisis: Admitting AI-Generated Media and the Burden of Proof

Perhaps the most existential threat to the evidentiary integrity of the BSA framework is the proliferation of Synthetic Media, colloquially known as "Deepfakes." As identified in the Problem Statement of this dissertation, the legal system is facing a profound "Crisis of Trust," where the ancient maxim "seeing is believing" has been rendered obsolete.

The core of this crisis lies in the concept of the "Liar’s Dividend." This term refers to the strategic advantage gained by malicious actors who can dismiss genuine, incriminating evidence (such as video recordings of bribery or audio of conspiracy) as AI-generated

39 https://www.osint.industries/post/osint-in-india-conducting-osint-across-india-and-the-subcontinent (last accessed on 12.02.2026 at 9:44 pm)
40 https://www.innefu.com/blog/how-open-source-intelligence-is-empowering-law-enforcement-agencies-in-india (last accessed on 12.02.2026 at 9:52 pm)

forgeries. Because Deepfake technology—driven by Generative Adversarial Networks (GANs)—is becoming indistinguishable from reality, a defendant can plausibly claim that a video depicting them committing a crime is a high-fidelity generative simulation.

The current forensic tools sanctioned under the BSA—primarily Hash Functions (SHA-256) and Metadata analysis—are insufficient to counter this threat. As detailed earlier, hashing only verifies that the file has not been altered *since* it was hashed. It does not, and cannot, verify if the content was real *before* the hash was generated. If a Deepfake video is created and then immediately hashed, the hash value will confirm the integrity of the *file*, but it validates a lie. Similarly, metadata can be "scrubbed" or synthetically generated to match the timestamp of the alleged crime.

This technological reality forces a doctrinal re-evaluation of the "Burden of Proof." Traditionally, in criminal law, the prosecution bears the burden of proving the authenticity of the evidence beyond reasonable doubt. However, in the face of Deepfakes, legal scholars are debating whether the burden must shift. If a Section 63 certificate is produced, does the statutory presumption of genuineness hold until the defence proves it is a Deepfake? Or, given the prevalence of AI manipulation, must the prosecution proactively use "AI-detection" forensics (such as blood-flow analysis or phoneme-viseme mapping) to rule out synthetic manipulation before the evidence is even admitted?

The BSA is currently "content-blind" regarding this distinction. It provides a robust mechanism to admit electronic records based on their *container* (the file) but lacks a specific statutory protocol to filter out AI-generated falsehoods within the *content*. This legislative gap leaves the judiciary vulnerable to admitting fabricated evidence that satisfies all procedural checks—proper custody, hash verification, dual-certification—but is substantively a digital forgery. This risk necessitates the development of a "Digital Voire Dire," a preliminary hearing specifically to test the "synthetic vs. organic" nature of audio-visual evidence before it is presented to the trier of fact.

1.8.1. Hashing vs. Content Authenticity

As already explained that cryptographic hashing can prove that a file is unchanged from the moment it was hashed. But suppose a suspect generates a deepfake video, copies it to his phone and never edits it again. If the police seize that phone and produce the video in court, all hash

checks will come back clean. The image is a "faithful reproduction" of a fake, and the law, as currently written, does not contain a ready-made test to draw this distinction.[41]

This is particularly troubling in contexts like bribery, sexual offences and communal violence, where video and audio recordings are often central. Courts are increasingly aware of the risk and have started to ask more probing questions about how an audio-visual file was generated, and whether any independent corroboration exists—such as witness testimony, metadata, or OSINT evidence of the recording circulating before the alleged fabrication date.

1.8.2. Emerging Detection Techniques and Resource Constraints

On the technical side, researchers and vendors are developing a range of deepfake detection techniques: examining subtle inconsistencies in lighting and shadows, checking blood-flow patterns under the skin, comparing lip movements (visemes) with detected phonemes in the audio, and analysing compression artefacts. Some commercial forensic tools and research prototypes are now integrating such checks, and vendors like Magnet have started to explore AI-based modules that flag suspect media within a case file.[42]

However, these detection methods are demanding. They often require high-quality original media, specialised software, and experts who understand both AI and forensic imaging. In India, where SFSLs already struggle with case volumes and basic digital forensics, expecting every lab to run advanced deepfake analysis on each contested video is unrealistic in the short term. This raises an uncomfortable policy question: should the prosecution be required to proactively "clear" important videos using AI-detection tools before trial, or should the burden lie on the defence to produce evidence that a given file is a deepfake? The BSA does not yet clearly answer this.[43]

1.8.3. Towards a "Digital Voir Dire"

One idea emerging in academic commentary is the concept of a "digital voir dire". Borrowing the language of jury selection, this would be a preliminary hearing focused only on the authenticity of contested digital exhibits, especially audio-visual ones. At such a hearing, the

41 https://www.medianama.com/2022/03/223-how-indian-law-enforcement-uses-phone-cracking-tools/ (last accessed on 12.02.2026 at 9:58 pm)
42 https://www.docullyvdr.com/blog/data-room/digital-colonialism-are-you-letting-foreign-servers-control-your-corporate-secrets/ (last accessed on 12.02.2026 at 9:59 pm)
43 https://www.ijfmr.com/papers/2025/5/57462.pdf (last accessed on 12.02.2026 at 10:04 pm)

court could hear from forensic experts, consider reports from deepfake detection tools, examine metadata and OSINT material, and then decide whether the file is reliable enough to be shown to the fact-finder at the main trial.

This would mirror, in the digital context, the way courts already conduct “mini-trials” on issues like confession voluntariness or admissibility of prior statements. It would also give both sides a structured forum to present technical arguments without overwhelming the main trial. For now, this remains more of a proposal than an established practice, but given the trajectory of deepfake technology, Indian courts may have to adopt something similar sooner rather than later.

1.9. Blockchain and Smart Contracts: Their Status as Evidentiary Documents

Blockchain technology introduces a unique evidentiary paradigm: the "Trustless Ledger." Unlike traditional databases (like SQL) that require a central administrator (such as a bank or a government registrar) to maintain and certify records, a Blockchain is a decentralized, distributed, and immutable ledger. In the context of the BSA, this raises a fundamental conceptual question: Is a Blockchain entry a "document," and if so, who has the authority to certify it?

Section 2(1) of the BSA is drafted broadly enough to include Blockchain ledgers within the definition of "electronic records." However, the application of Section 63(4)—the requirement for a certificate signed by a "person occupying a responsible official position in relation to the operation of the relevant device"—is conceptually incompatible with decentralized public networks [63]. In a public Blockchain (like Bitcoin or Ethereum), there is no "central administrator," no "official custodian," and no single "device" that holds the original. The network is maintained by thousands of anonymous nodes distributed globally. Who, then, signs the Section 63 certificate?

If the accused owns a "wallet," they can certify their own device, but they cannot certify the "ledger" itself, which exists on the network. Legal scholars argue that Blockchain records should be treated as "Self-Authenticating" documents. Due to their cryptographic immutability (secured by Merkle Trees and consensus mechanisms), the risk of tampering is negligible compared to a standard database which can be edited by an admin. Requiring a Section 63 certificate for a Blockchain record imposes a centralized procedural requirement on a

decentralized technology, effectively forcing a square peg into a round hole.

In 2026, courts are also beginning to grapple with "Smart Contracts"—self-executing code stored on the Blockchain that automatically runs when predetermined conditions are met. When a Smart Contract executes a fraudulent transaction or a "rug pull" (in decentralized finance), the code itself is the evidence of the crime. Admitting this requires the court to move beyond the "human certificate" model. It requires the judiciary to accept "mathematical consensus" as a valid form of verification—a leap that the text of the BSA does not explicitly authorize but arguably permits under a purposive interpretation of "proper custody" in the digital age. The challenge lies in explaining this "code-as-law" to a judiciary trained in "text-as-law".

1.9.1. Who Certifies a Public Blockchain?

If the prosecution wants to rely on a particular on-chain transaction—for example, to show that a certain wallet address received illegal proceeds—who signs the Section 63(4) certificate? The accused cannot credibly certify the entire network; exchanges are only partial intermediaries; and no central company controls the blockchain itself. Some scholars therefore argue that public blockchains should be treated as a special class of self-authenticating electronic records, where the combination of public verifiability, consensus protocols and cryptographic proof replaces the need for a human custodian.

This would require a certain amount of doctrinal flexibility. Courts would have to accept that anyone with a copy of the blockchain and the right software can independently verify that a given transaction exists at a given block height and has not been altered. In practice, prosecutors already work with blockchain-analysis companies, both global and Indian, who provide visualisations and expert testimony tracing the flow of funds between wallets and exchanges. Those experts can explain how they verified that specific on-chain entries exist and how they linked them to off-chain identities (for example, through KYC records at exchanges).[44]

1.9.2. Smart Contracts and “Code as Evidence”

Smart contracts—pieces of code deployed on blockchains like Ethereum that automatically execute when conditions are met—create another evidentiary twist. In many crypto-fraud and

44 https://www.ecsinfotech.com/the-ultimate-guide-to-network-forensics-in-india/ (last accessed on 12.02.2026 at 10:15 pm)

"rug-pull" cases, the smart contract code itself is the main evidence of the scam: it may contain hidden functions that divert investor funds or lock users out once a certain target is reached.

Admitting such code as evidence requires courts to become comfortable with treating source code and bytecode as documents within the meaning of the BSA, and with hearing from technical experts who can explain, in accessible language, what the code does. This is harder than it sounds, because many judges and lawyers are not familiar with programming concepts. But it is necessary if the legal system is to deal effectively with frauds that are embedded "inside" code rather than only in surrounding communications.

Here too, network forensics and OSINT play roles: investigators may rely on public repositories (like GitHub), forum posts, and blockchain explorers to show when a smart contract was deployed, who advertised it, and how it was used over time. All of this has to be pulled together into a narrative that the court can understand and that complies with the BSA's certification and authenticity requirements.

1.10. Internet of Things (IoT): Data from Wearables and Smart Homes as Evidence

The final frontier of emerging technology in the BSA era is the "Internet of Things" (IoT). In 2026, the silent witnesses in a criminal trial are no longer just bystanders or CCTV cameras; they are the devices worn by the victim and the accused, and the appliances that inhabit their homes. Data from wearables (like Fitbits, Apple Watches, or smart pacemakers) and smart home devices (like Amazon Alexa, Google Nest, or smart utility meters) is increasingly being proffered as evidence to corroborate alibis, establish timelines, or even record the physiological state of a victim at the time of death.

The admissibility of IoT data under the BSA presents a unique "Hearsay" challenge. Is data generated by a pacemaker recording a spike in heart rate "testimonial" evidence? Since it is machine-generated data produced without human intervention or assertion, it generally falls outside the hearsay rule (which applies to human statements). It is treated as "Real Evidence." However, the reliability of these sensors is often contested. A "step count" on a wearable device is not a definitive forensic fact; it is an algorithmic interpretation of raw accelerometer data. Defence counsels argue that these consumer-grade devices are not calibrated forensic instruments and thus their data should not be admitted with the same weight as a standard forensic tool.

Furthermore, the "Custody" issue resurfaces with complexity. Who is the "custodian" of the data generated by a smart fridge or a smart speaker? Is it the user, who owns the hardware? Or is it the manufacturer (e.g., Amazon or Apple), who hosts the data processing on their proprietary cloud servers? If the police seize a smart speaker to retrieve voice recordings of a domestic dispute, the Section 63 certificate must ideally come from the manufacturer's server administrator, not just the homeowner.

This returns the legal process to the "Sovereignty Challenge" and the "Expert Bottleneck," as accessing proprietary IoT data often requires bypassing complex proprietary encryption and enduring lengthy international legal requests. Moreover, unlike a phone which has a clear user interface, IoT devices are often "Black Boxes" of data. Extracting evidence from a smart lightbulb or a thermostat requires specialized IoT-forensic tools that are not yet standard in Indian forensic labs. The BSA's framework, designed primarily for "communication devices" (phones/computers), struggles to seamlessly integrate this "ambient computing" data where the environment itself is the witness. The "Right to Privacy" (Puttaswamy impact) is also severely implicated here, as the admission of IoT data effectively turns the user's home into a panopticon of constant surveillance, raising questions about the "reasonable expectation of privacy" in a smart home.

1.10.1. Is IoT Data “Real Evidence” or Hearsay?

Since IoT devices record information by sensors and microcontrollers rather than by human statements, this data is generally treated as “real” or “machine-generated” evidence, not hearsay. The hearsay rule is mainly about human assertions. A pacemaker that logs heart-rate data is not “saying” anything; it is just recording sensor readings.

However, the reliability of consumer-grade devices is open to debate. Wearable step counts, for example, are based on algorithms interpreting accelerometer data, and may miscount steps when a person waves their arms, rides in a vehicle or carries the device loosely. Smart speakers may mis-record or mis-trigger, recording snippets of unrelated conversation. Defence counsel can and do question whether such data is accurate enough to be treated as solid forensic evidence in a criminal trial, as opposed to an investigative lead or corroborating background.

1.10.2. Custody, Foreign Servers and Tool Gaps

IoT evidence also raises serious custody and sovereignty issues. Many devices store only

limited data locally while uploading detailed logs to company servers abroad. A smart speaker might keep a few recent commands on-device but send full audio clips and transcripts to cloud servers operated by companies like Amazon or Google. A fitness tracker might sync detailed history to a vendor's app, with the long-term storage physically sitting on servers outside India.

This means that, to get the full evidentiary picture, Indian investigators often need cooperation from foreign companies and may fall back into the same MLAT maze discussed under cloud computing. The question also arises: who is the custodian for Section 63(4) purposes—the device owner, the app provider, or the cloud host? In many cases, only the manufacturer or service provider can meaningfully certify how the data was collected, stored and protected against tampering, but those companies may be outside Indian jurisdiction.[45]

On top of that, there is a tooling gap. While mobile phones and computers are well-supported by suites like UFED, AXIOM and FTK, there are far fewer standard tools for extracting and interpreting data from the huge variety of IoT devices, each with its own protocols and data formats. Specialist IoT-forensic tools exist, but they are not yet widely deployed in Indian SFSLs. As a result, even when IoT data could, in theory, be very probative (for example, showing whether someone was at home, asleep, or moving around), investigators may avoid it because of the technical complexity and the lack of local expertise.[46]

1.10.3. Privacy, Puttaswamy and the Smart Home

Finally, IoT evidence directly implicates privacy concerns. In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court recognised the right to privacy as a fundamental right, including spatial privacy in the home. If every smart bulb, smart plug and smart speaker can become a potential prosecution witness, there is a risk of turning the home into a kind of digital panopticon.

Courts will likely have to balance the probative value of IoT data against the intrusiveness of the collection methods, the specificity of warrants and the risk of fishing expeditions. Warrants that demand "all data from all smart devices in the house for the last five years" may be seen as disproportionate, especially when less intrusive means are available. In the BSA era, then,

45 https://cis-india.org/internet-governance/files/mlat-report (last accessed on 12.02.2026 at 10:21 pm)
46 https://humanrightlawreview.in/wp-content/uploads/2025/05/The-Intersection-of-Digital-Forensics-and-Criminal-Investigation-in-India-Legal-and-Procedural-Dimensions-of-Evidentiary-Standard.pdf (last accessed on 12.02.2026 at 10:37 pm)

IoT does not just create new kinds of electronic records; it forces the system to revisit traditional ideas of what counts as a reasonable search in a technologically dense environment.

Conclusion

The way we think about proof in a courtroom has changed forever. As this study shows, digital evidence is no longer simply about presenting a file or a screenshot — it is about demonstrating that every step of its journey, from the moment it was found to the moment it is placed before a judge, was handled with care, honesty, and discipline.

India's Bharatiya Sakshya Adhiniyam 2023 is a sincere and ambitious attempt to bring the law into step with modern life. Yet the deeper we look, the clearer it becomes that the law has outpaced the people and institutions meant to carry it out. Investigators still lack proper training, laboratories remain under-resourced, and new challenges — from AI-generated videos to smart home devices — keep arriving faster than answers do.

What this article ultimately reveals is a human problem hiding inside a technological one. No law, however well-written, can deliver justice on its own. It needs trained hands, honest documentation, and a justice system willing to keep learning. The tools of the future will only be as trustworthy as the people who use them.