

Supply of copy of electronic evidence - Suggested system for District Courts

Sanjay Rambhau Salkute

B.Sc.; LL.M.; M.B.A.; D.C.S.A.

Retired District Judge, Pune (Maharashtra), India

Abstract

The Bharatiya Sakhya Adhiniyam, 2023 [BSA 2023], Section 63(4) mandates hash value certificates while submitting electronic record for admission. It elevates the electronic record as primary evidence but for submission a proper custody is required. However, no procedural framework exists for courts to supply certified copy of exhibited electronic record.

Neither the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, nor the Bharatiya Sakhya Adhiniyam (BSA), 2023, contains specific provisions for supplying certified copies of exhibited electronic records. While BSA Sections 75-79 generally address certified copies, but there exists a procedural vacuum regarding the technical and legal framework for courts to supply hash-verified certified copies of electronic exhibits.

This preliminary study paper concept for law students, examines the gap between legal requirements under the Bharatiya Sakhya Adhiniyam, 2023 (BSA), 2023, and practical implementation for supplying certified copies of exhibited electronic record in District Courts. This study is based on BSA provisions, case law review, and examination of current court practices. It is studied that, without sound copying procedures, the primary evidence status of electronic records remains on paper for which copying sections will require little infrastructure, trained personnel, and standardized procedures to maintain evidential integrity when supplying certified copies of exhibited electronic record. It is studied that as the Section 63(4) certificates are mandatory and become part of court records, the solution in suggested system is simple because courts already possess the hash values needed, they simply lack procedural guidance on how to use them when supplying certified copies. The suggested system is complementary to, not contradictory with procedural law. This study is limited to supply certified copy of the exhibited electronic record only.

Keywords: secure hash value, electronic evidence copy, Section 63(4), court digital evidence, certified copy electronic records.

1. Introduction

In the Indian Evidence Act, 1872, section 65 (Amendment in 2000) speaks requirement of certificate for the admissibility of the electronic record and it was treated as secondary evidence. The requirement of Section 65-B of the Evidence Act was a general certificate by the person stated in it. Later on, the

requirement of hash value was also discussed in the judgments. Then the stage of filing of certificate was discussed in the case of Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020).

In the case Arjun Khotkar held that electronic evidence (computer output) must be furnished to the accused at the latest before trial begins under Section 207 CrPC, giving the accused a fair chance to prepare their defense. In the case of Tarsem Lal vs Directorate Of Enforcement Jalandhar, it is pleased to held that, once the trial stage begins (post-cognizance), the procedural safeguards of the CrPC apply, ensuring the accused is provided with all relevant documents to prepare a fair defense. The accused cannot be harassed by arrest once the court is seized of the matter; they must be treated as a participant in a judicial process with a right to all relied-upon information. In the case of Sameer Sandhir vs Central Bureau Of Investigation, the Hon'ble the Supreme Court clarified that the accused has the right to obtain all documents that the prosecution relies on. Despite the CDs not being initially included, the court allowed their inclusion on condition that the defense be permitted to bring witnesses for cross-examination regarding the CDs. It is held that, the court's primary duty is to ensure the accused is never "surprised" by evidence they haven't had the chance to contest.

In the case of Toman Lal Sahu S/o Panth Ram Sahu vs State of Chhattisgarh, WPS No. 5287 of 2012, 26.03.2021 it was held to provide CD /copy to the opponent in the matter of disciplinary enquiry also. There are few other precedents wherein the supply of copy of electronic record is directed with hash value to the opponent either pre-cognizance or post cognizance. The object to supply copy of electronic record is also to give sufficient opportunity to defend the other side.

Now BSA section 63(4) requires hash values when electronic record is submitted for admission. BNSS 2023 is silent on hash values or forensic procedure. BNSS 2023, Second Proviso speaks that, "if the Magistrate is satisfied that any such document is voluminous, he shall... furnish the copies through electronic means", it clearly stated that, the electronic supply must preserve integrity". But on plain reading it is clear that, supply of Copies" (Discovery) under BNSS 2023 and "Certified Copies" (Evidence) under BSA 2023, the standards for the BSA 2023 are much higher (Hash value required) than the BNSS 2023 (may be mere readability required).

The (BSA),2023, replaced the Indian Evidence Act,1872. On July 1, 2024 the BSA 2023 came in force with section 170 Repeal and saving. As per BSA, Section 57, primary evidence, section 57(Explanation 5) speaks that, "where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed". The explanation 6 and 7 are also relevant. The term 'proper custody' is not statutorily defined in BSA 2023. Based on established principles of evidence law and digital forensics, proper custody may be understood to mean that electronic records must be handled carefully and safely, with proper chain of custody documentation, protection from unauthorized access, and safeguards against alteration. But it is clear that only when this proper custody is proved can electronic records be treated as primary evidence in court. Here proper custody while supplying certified copy by court means, whether the chain of custody documentation, protection from unauthorized access is reasonable.

In Mr. Virendra Khanna S/o Shri Ram Khanna vs State of Karnataka, Writ Petition No.11759 of 2020, the Hon'ble Karnataka High Court issued clear guidelines as to how electronic evidence should be

handled. In the case of CBI v. Mahesh Kumar Sharma, the Hon'ble Delhi Court declared the findings in Virendra Khanna regarding the compulsion to provide passwords/passcodes as per *incuriam*. But it was declared *per incuriam* Biometrics (Fingerprints/Face ID) and Voluntary Disclosure.

The “Section 63(4) requires submission of certificates as per clauses (a), (b), and (c). Clause (c) deals with matters relating to subsection (2) conditions and requires signatures by both the person in charge and an expert. The Schedule to BSA 2023 (referenced in Section 63(4)) prescribes the certificate format in Part A and Part B, which includes the requirement for recording Hash Values. Section 63 (4) introduced a specific technical requirement and Section 63(4)(c) speaks that prescribed format of certificate, as per schedule Part A [To be filed by the party- The person who has lawful control over the device/ To be filled by the party producing the evidence.] and Part B [To be filed by the Expert- An expert who can verify the technical integrity of the record.] require the recording of Hash Value. The specification of Secure Hash Value is SHA1, SHA 256, MD5, other legally acceptable standard. Both certificate shall also bear date, time stamp and place. It also speaks dual certificate with clear words, “ purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate;” The word, ‘Shall’ makes it mandatory and format given in schedule is much stricter.

The above certification is a mandatory procedural requirement, therefore the legal position regarding the stage at which certificate under section 63(4) shall be filed is clearly mentioned with word, “ at each instance”, ‘admission’. This implies that whenever the electronic record is extracted and submitted to the court for admission, it must be accompanied by dual certificate. Thus, BSA has shifted the ‘burden of readiness’ at the stage of admission.

Concept of Certified copy by the court: A certified copy of a court document / paper is a duplicate of an original file that has been verified by the court’s clerk or custodian of records as being a "true and correct" copy. For supplying paper-based copy or true copy or certified copies provisions are made in court manual, where ordinary and urgent copy concept is described along with the requisite charges for it.

Now, the BSA 2023 refines electronic records to the status of primary evidence and retains the dual certification requirement. But, the BSA 2023 remains completely silent on the point of preservation, copy, supplying copies of such electronic record that is exhibited by the court, to the parties though the section 74 to 76 is nearly identical to Indian Evidence Act. The definition of a "document" in Section 2(d) of the BSA now includes electronic and digital records. Therefore, as per section 75 to 79, the “certified copy” can now also be issued in digital format.

Current Situation: It is noticed that, when party seek copy the court supplies copy-paste. But such supplied copy-paste may be challenged because it may not copy material properties of the files. Though there is no case or judgment that, due to supply of copy-paste observations are made for post-exhibition. But now the BSA 2023 itself mandates secure hash value concept.

There is also a provision for inspection of the document. Under right to inspect the electronic record filed by party relying on it, wherein the opponent can view(access) but it depends upon various factors.

The viewer must be intelligent, there must not be use of artificial intelligence in the files, media. Mere viewing is also depended upon the facts of each case and also needs to consider DPDP Act 2023.

It is noticed that, there is no specific procedure to supply certified copy of the exhibited electronic record. The Hon'ble Delhi High court issued a Notification April 22, 2024 for E-True Copy Rules of high court of Delhi, 2024, are regarding e-true copy of the digitized record. But the above rules do not speak for requirement of hash value. It was issued only for digitized record and it was not issued for original electronic record exhibited by the court in the court proceedings / trials.

2. International Practice:

(1) **United Kingdom:** Code of Practice for Forensic Science Providers and Practitioners provide detailed procedures.

(2) **United States:** Federal Rules of Evidence address electronic evidence; various states have specific protocols.

(3) **Singapore:** Has implemented comprehensive electronic evidence procedures.

None of these three technologically advanced jurisdictions have specific procedures for courts to supply hash-verified or forensically authenticated certified copies of exhibited electronic evidence. Instead, all three jurisdictions primarily rely on traditional certification by court officials, with electronic evidence being treated similarly to paper documents for copying purposes, even though admission standards for electronic evidence are stringent. They use secure cloud/ server evidence portals. In the secured portal system, once evidence is admitted, it is uploaded to a secure, write-protected server. Parties are given a "Download Link" with a pre-calculated hash. It is based on "Presumption of System Integrity."

But in India the centralized secure server [Digital Evidence Management Systems (DEMS)] is yet not developed. In future it will be definitely developed but the current system is a physical-media-based. This itself shows that; the solution does not require courts in India to become forensic laboratories but traditional certification needs to be adapted as per scheme provided in section 63 of the BSA 2023.

Need of Certified Copy of Exhibited electronic record: In practice, electronic record that is exhibited in one proceeding often needs to be produced in related or subsequent proceedings. The original exhibited electronic record cannot be physically present in multiple courts simultaneously, nor can originally court electronic record exhibits be removed from one case file and produced in another. Therefore, certified copies are not merely convenient but legally and practically necessary. Moreover, BSA Section 63(4) mandates certificates with hash values, but provides no mechanism for courts to create and certify copies for use in other proceedings, parties to file such certified copies in subsequent cases with verifiable integrity and courts in subsequent proceedings to verify such copies against originals electronic record that was filed in the original proceedings.

Illustration: Electronic record was exhibited in a criminal trial may be needed in a related civil defamation suit. The accused cannot produce the original exhibited electronic record because it is in the custody of the court. If the party obtains a "certified copy" from the criminal court, but without hash verification, the civil court questions its authenticity. The party is caught between two impossibilities:

cannot produce original exhibited electronic record, cannot prove copy's integrity in relation to the facts in other related proceedings based on the same exhibited electronic record.

Illustration: If Court A has the original and Court B needs a copy, the lack of a "Hash-Verified Certified Copy" protocol forces the litigant to call a forensic expert to Court A just to verify a copy for Court B.

Considering the above circumstances, in this preliminary study, concept is placed regarding supplying certified copy of the exhibited electronic record by the court. For this study, no empirical data / survey is carried out. The concept to supply certified copy has no concern with other concepts like to check the integrity, authenticity, reliability and proved of electronic record. This concept has no concern with the supplying copy to opponent before admission/actual trial including evidence etc.

Suggested System:

- (a) When supplying certified copies of electronic records, court staff access original in read-only mode to ensure the exhibited electronic record is not touched or modified during the copying process.
- (b) Copy using standard computer copying methods with secure hash value.
- (c) Compare with hash in Section 63(4) certificate, because courts already possess the hash values needed.
- (d) Supply copy with traditional certification: 'Certified that this is a true copy of [electronic record description] exhibited as [Exhibit No.] in [Case No.]'.
- (e) Label media with case details, exhibit number, date of copying. If the container is physical (e.g. CD or Pen Drive etc) then it needs to be physically labelled with case number, exhibit number, date of issue, verified secure hash value. If container is folder only then its hash value shall be supplied with the copy. The court may digitally sign the folder or container to prevent subsequent tampering.
- (f) Then container of the certified electronic exhibited document be supplied in sealed form.
- (g) Maintain register of certified copies issued. For this process, the court department issuing the certified copy has to maintain record for generated hash value (if any) and verified hash value and it should be recorded in court case record / proceedings daily notes, ensuring no modification during copying.

Note: Locate the exhibited electronic record and its mandatory Section 63(4) certificates (Part A and Part B) in the case record. If certificates are missing, this indicates improper admission, certified copy cannot be supplied until defect is cured.

Note: If the secure hash value of the prepared copy meets with exhibited electronic record by the court, then only the certified copy can be issued.

Note: Ubuntu software like Caine, Deft can provides a legal audit trail. Such tools, if used, are only for generating and verifying hash values of already admitted exhibits and not for forensic analysis, interpretation, or extraction from original sources.

Advanced Technology: Use of Write-Blocker but it may require more infrastructures and training.

Note: A write-blocker is a hardware device or software tool that permits read-only access to data storage devices without compromising the original data. Hardware write-blockers are preferred in forensic contexts. NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response.

What the Party Receives:

1. Electronic record copy on media (CD/DVD/pen drive) or Folder.
2. Certified copies of both mandatory Section 63(4) certificates (Part A and Part B) from original admission, containing the hash values recorded at that time
3. Court certificate stating this is true copy of exhibited record, referencing the Section 63(4) certificates and hash value
4. (If enhanced procedure used) Verification that copy's hash matches original admission hash can be mentioned.

How to Use certified copy in Subsequent Proceedings:

Step 1: Submit the electronic record [container or folder] along with all received certificates (Section 63(4) certificates from original admission and court's certified copy certificate).

Step 2: It is admissible as secondary evidence under section 61 of BSA 2023 because:

- (a) original is in possession of court in another proceeding,
- (b) copy is certified by competent court,
- (c) integrity can be verified against hash values recorded at original admission.

Step 3: If court requires further verification, parties can:

- (a) engage forensic expert to independently generate hash of the copy and compare with Section 63(4) certificate,
- (b) request original court to provide additional certification,
- (c) in some cases, request transfer of original exhibit for inspection or court proceedings.

Prima facie evidentiary Status and Weight:

The certified copies remain secondary regardless of hash verification. However, the evidentiary weight is enhanced due to certification by competent court (presumption of official regularity), accompanying Section 63(4) certificates proving original admission standards, hash value enables independent verification.

Note: The status of the supplied document will be only certified copy and not forensic copy, but the secure hash value of the digital copy created by court authority shall match the secure hash value of the

electronic record - Exhibited document on court record. The issued certified copy will be admissible but not automatically treated as primary evidence and it remain secondary evidence unless the original exhibited electronic record is produced and verified and thereby already developed jurisprudence for paper based exhibited certified copy will apply.

Note: The Court's Copying Section, by using hash values, functions as a Verifying Authority rather than a mere duplicating unit. Certified Extractions, even hash-verified, remain certified secondary evidence, admissible but not equivalent to originals.

Note: The court, while issuing certified copies, does not conduct a fresh Section 63(4) compliance exercise, but merely verifies that the copied output corresponds identically to the already admitted electronic exhibit.

Practical Challenges in suggested system for supplying copies: -

a] Now the court computers are meant only for office work like typing orders, printing, court websites, Court case system software (CIS), e-filing and scanning. They are not designed for handling electronic exhibited documents. Therefore, little software infrastructure will be required suitable for supplying certified copy of the electronic exhibited document by the court.

In the above suggested system, a minimum standard of the secure hash value needs to be fixed for container or folder / media (from the schedule of the BSA). However, while supplying certified copy, balancing fair trial rights with data protection DPDP principles needs to be followed.

b] Giving training to court staff for hash value creation and hash value verification process. The court staff training shall include Emails, PDFs, WhatsApp (Export Chat), CCTV footage, DVRs, intercepted audio.

3. Conclusion:

The BSA mandates a Section 63(4) dual Certificates for submitting electronic record at each instance for admission. But it provides no blueprint for how a Court's "Copying Section" can supply a certified copy of the exhibited electronic record without destroying the very "Primary" status as it aims to preserve. If the "Copying Section" of a court remains illiterate, the "Primary Evidence" status of digital records will exist only on paper. Though certified copy word mentioned in section 75 to 79, but in fact the certified copy certificate / formal attestation issued by court would be formal (overall reliability and chain of custody) court attested copy and not as a forensic expert. A certified copy issued by court for exhibited electronic record will be admissible but not automatically treated as primary evidence and it remain secondary evidence unless the original exhibited electronic record is produced or it is verified. In India it is expected to move toward "System Custody" where the Ubuntu-based Forensic Workflow will act as a "Local DEMS." The suggested system may require a realistic roadmap for its implementation. Therefore, it requires further study in doctrinal, procedural, and empirical development before it can serve as a comprehensive framework.

Required Further Study: A more comprehensive study is required. Following are some key points: -

- 1] The BSA 2023 requires the hash to stay consistent. Therefore, more study is required, does the status of a court-issued electronic Certified copy of exhibited electronic record as a Judicial Record override its character as Secondary Evidence.
- 2] Need of certifying authorities (under section 11 of the Information Technology Act, 2000), system certification, supply of media / container with contents by the court.
- 3] Timeline for Implementation of process and procedure, infrastructure, training etc to supply certified copy of exhibited electronic record.
- 4] Judicial guidelines or amendment defining custody standards (logs, restricted access, protocols) for the system through which certified copy will be supplied.
- 6] Harmonize BNSS 2023 discovery rules with BSA 2023 certified copy rules.

Note: In the paper , Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach and like other papers, Section 63(4) BSA 2023 has been analyzed exhaustively for admission purposes but the post-exhibition copying procedure is not found therefore more study is required on this concept.

Citations:

1. Anvar P.V. v. P.K. Basheer (2014) <https://indiankanoon.org/doc/187283766/>
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) <https://indiankanoon.org/doc/172105947/>
3. Toman Lal Sahu S/o Panth Ram Sahu vs State of Chhattisgarh, WPS No. 5287 of 2012, 26.03.2021 <https://www.indianemployees.com/judgments/details/toman-lal-sahu-versus-state-of-chhattisgarh>
4. Mr. Virendra Khanna S/o Shri Ram Khanna vs State of Karnataka, Writ Petition No.11759 of 2020, <https://indiankanoon.org/doc/87379349/>
5. The Hon'ble Delhi High court issued a Notification April 22, 2024 for E-True Copy Rules of high court of Delhi, 2024, <https://www.delhihighcourt.nic.in/files/announcements/1543372878666302c0c45fa.pdf>
6. CBI v. Mahesh Kumar Sharma <https://www.casemine.com/judgement/in/636e8af71ce8394be46b8dc4>
7. NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response. <https://csrc.nist.gov/pubs/sp/800/86/final>
8. Tarsem Lal vs Directorate Of Enforcement Jalandhar <https://indiankanoon.org/doc/155382593/>
9. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach

https://www.academia.edu/150287956/Trial_Court_as_Guardian_of_Electronic_and_Digital_Record_Under_Section_63_of_the_Bharatiya_Sakshya_Adhiniyam_2023_A_Modern_Approach

<https://www.scribd.com/document/987429467/Trial-Court-as-Guardian-of-Electronic-Digital-Record>

https://www.linkedin.com/posts/yogesh-barude_trial-court-as-guardian-of-electronic-digital-activity-7421558005189705728-xVno?utm_source=social_share_send&utm_medium=android_app&rcm=ACoAABJS44ABvhVjOvbpCuY7EQtIDLXIKNeaL6I&utm_campaign=whatsapp

10. Sameer Sandhir vs Central Bureau Of Investigation <https://indiankanoon.org/doc/127715189/>