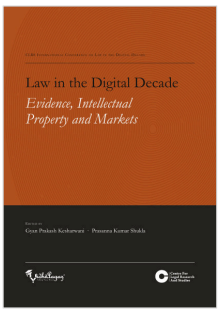
CHAPTER 3

When the Certificate Lies: Rethinking Authenticity Under the Bharatiya Sakshya Adhiniyam

Rachel Delfin



in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 23–30

DOI https://doi.org/10.63108/VAB.LDD.2.3

CITATIONS

BLUEBOOK (21ST ED.)
Rachel Delfin, *When the Certificate Lies: Rethinking Authenticity Under the Bharatiya Sakshya Adhiniyam*, *in* LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS 23 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)
Rachel Delfin, 'When the Certificate Lies: Rethinking Authenticity Under the Bharatiya Sakshya Adhiniyam' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 23.

CHICAGO (17TH ED.)
Delfin, Rachel. "When the Certificate Lies: Rethinking Authenticity Under the Bharatiya Sakshya Adhiniyam." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 23–30. Maihar: VidhiAagaz, 2026. https://doi.org/10.63108/VAB.LDD.2.3.

APA (7TH ED.)
Delfin, R. (2026). When the certificate lies: Rethinking authenticity under the bharatiya sakshya adhiniyam. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 23–30). VidhiAagaz. https://doi.org/10.63108/VAB.LDD.2.3

SOURCE

https://doi.org/10.63108/VAB.LDD.2.3

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

Law in the Digital Decade: Evidence, Intellectual Property and Markets, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026) · Open access under CC BY-NC 4.0 · https://doi.org/10.63108/VAB.LDD.2.3

CHAPTER 3

When the Certificate Lies: Rethinking Authenticity Under the Bharatiya Sakshya Adhiniyam

RACHEL DELFIN*

The Bharatiya Sakshya Adhiniyam, 2023 replaced Section 65B of the Indian Evidence Act with Section 63. Section 63 keeps the certificate-based method that has controlled whether electronic records can be used in court since the cases Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020). The paper asks whether Section 63's continuity is a strength or a blind spot. Section 63's certificate is a two-part Schedule requiring a hash value and two signatures, designed to verify the chain of custody of a record. The certificate shows that a computer output accurately reproduces what a device captured. Section 63 assumes that an authentic event exists and that the record can be traced back to that event. AI-generated deepfakes break that presumption. A synthetic video can meet every requirement of Section 63. The synthetic video can carry the correct device details, the correct hash, and the correct signatures yet it can show an event that never happened. During 2025–26, High Court injunctions against deepfakes of public figures show that courts are already improvising remedies under Article 21 personality rights. The lack of guidance on how to authenticate content instead of just certifying its custodial trail explains this. The paper argues that the BSA's electronic evidence provisions modernize the language used for admissibility but do not solve the underlying epistemic problem, and also argues that the IT Rules of 2026 which require labeling of content cannot replace a real authentication standard.[1] Drawing on the text of the certificate Schedule, recent case law and a comparison with the UK Forensic Science Regulator's Code of Practice, the paper proposes a narrower reform. The reform would add a supplementary authenticity threshold for content that is plausibly generated or altered by AI. This threshold would be separate from the custodial certificate.

Keywords: Electronic evidence, Bharatiya Sakshya Adhiniyam, Deepfakes, Section 63, Authentication.

1 INTRODUCTION

Imagine scrolling through media and seeing a video of a public figure saying something controversial. The image is sharp, the person looks real, the voice sounds like them and their movements are natural. There's no sign that anything is wrong. In a world where artificial intelligence can create videos, voices and images, the problem isn't just whether a digital file was changed after it was made. The bigger challenge is whether the event in the video actually happened at all. This question becomes especially serious when such content ends up in a courtroom. Today electronic evidence plays a role in legal cases. Courts regularly use CCTV tapes, phone recordings, emails, photos, social media posts, call logs and other digital materials to help determine what really occurred. Because of this the law needs rules for deciding when such material can be accepted as proof. For a time Indian law dealt with this by focusing on authentication

* Law Student at Christ (Deemed to be University), Bengaluru, Karnataka, India.

[1] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified Feb. 10, 2026 and effective Feb. 20, 2026, introducing mandatory labelling and provenance requirements for synthetically generated information.

and custody. If someone could show how an electronic record was created, stored, copied and handled properly and meet the conditions set out in the law, courts would accept it as reliable.

A key part of this process came from Section 65B of the Indian Evidence Act, 1872. Over time Supreme Court rulings in cases like State (NCT of Delhi) v. Navjot Sandhu, Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal helped shape how electronic evidence is admitted. The Anvar case made it clear that following Section 65B is essential to allow records into court—especially if they're presented in the way the law allows. The Arjun Panditrao decision reinforced the need for certification and clarified that the certificate is unnecessary where the original electronic record itself is produced. Now the Indian Evidence Act has been replaced by the Bharatiya Sakshya Adhiniyam, 2023. Section 63 of the law covers the admissibility of electronic records[2] and keeps much of the old structure from Section 65B. It includes a Schedule that requires information about the record itself, the device or source it came from and its hash value. This Schedule gives an organized way to verify the origin and integrity of digital files. But here's the issue: deepfakes break this system. A deepfake may be an authentic digital file, not edited after creation, correctly copied and verified through a hash value. The file could have come from a device, passed through proper channels and even have a valid certificate. Still the event it shows might never have taken place. A falsehood, even if preserved exactly as it was, is still a falsehood. That's where the current legal framework falls short.

This distinction forms the central argument of this paper. The existing certificate-based approach is primarily concerned with the authenticity and integrity of the electronic record as an object of evidence. Deepfakes introduce a different question concerning the authenticity of the reality represented by that record. Therefore, the issue is not whether certification is unnecessary. Rather, the issue is whether certification alone can remain sufficient when the real dispute concerns the truthfulness of the underlying event. The central research question of this paper is therefore: How far can a custody-based certificate regime remain adequate once the authenticity of the underlying event, not merely its custodial trail, is what is actually in dispute? This paper first examines the development of the law relating to electronic evidence under Section 65B of the Indian Evidence Act. It then considers the continuity between Section 65B and Section 63 of the BSA, particularly the importance of certification, device information and hash values. The paper then examines the challenge posed by deepfakes and distinguishes between what may be termed "custodial authenticity" and "substantive authenticity." Finally, it proposes a framework called C.A.S.E., or the Certification–Authenticity Split for Electronic Evidence, under which statutory certification remains the ordinary first layer of authentication, while a specific and credible challenge to the authenticity of the underlying content can trigger a second layer of substantive verification. The objective is not to argue that every electronic record should automatically be subjected to forensic examination. Such an approach would be impractical and could place an unnecessary burden on courts, litigants and already limited forensic resources. Instead, the proposed approach attempts to create a middle ground between complete reliance on certification and compulsory forensic verification of every digital record.

2 THE OLD REGIME COMPRISING SECTION 65B AND ITS CASE LAW

The legal treatment of electronic evidence in India developed in response to a basic difficulty. Traditional evidence law was largely designed around physical documents, while digital information could exist

[2] Bharatiya Sakshya Adhiniyam, 2023, § 63 and Schedule.

simultaneously in several forms and could be copied without an obvious physical distinction between an original and a duplicate. A photograph stored on a phone, for example, could be transferred to a computer, uploaded to a cloud service and reproduced on another device without the ordinary physical characteristics associated with conventional documents. The introduction of Sections 65A and 65B into the Indian Evidence Act tried to solve a problem by setting up a way to prove the contents of electronic records. At first the Supreme Court took a flexible view in the case of State (NCT of Delhi) v. Navjot Sandhu.[3] In that case it looked at whether electronic records could be admitted as evidence using the existing rules for evidence. Later the Supreme Court changed its position in the case of Anvar P.V. v. P.K. Basheer.[4] In this case the court treated Section 65B as the rule that controls how electronic evidence is accepted when the situation fits what the section describes. The court made it clear that any electronic evidence given in the way laid out by Section 65B must meet legal requirements. One of those requirements is the certificate mentioned in Section 65B(4). This decision was significant because it shifted the law away from treating records simply as another type of written document. Instead it acknowledged that electronic records need their own set of rules and protections. The value of the certificate becomes clear when we look at what Section 65B was meant to do. The certificate gives details about the record itself, how it was created and which computer or device was used. It acts like a kind of proof that shows how the record came to exist and how it was produced before being presented in court. This helps ensure that the record is reliable and trustworthy.

This approach was subsequently considered in detail in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. The Supreme Court reaffirmed the position in *Anvar* and treated the Section 65B certificate as an important requirement for the admissibility of electronic evidence falling within the provision. At the same time, the Court clarified that where the original electronic record itself was produced as primary evidence, the situation was different from the production of a computer output or secondary electronic evidence.[5]

The decision also recognised a practical difficulty. A party seeking to produce electronic evidence may not always have control over the device or computer from which the record originated. The Court therefore acknowledged that a court could assist in obtaining the necessary certificate in appropriate circumstances rather than allowing the absence of a certificate, where the party genuinely could not obtain one, to automatically defeat the claim. The development from *Navjot Sandhu* through *Anvar* to *Arjun Panditrao* demonstrates an important movement in Indian evidence law. The law became increasingly concerned with the reliability of the process through which electronic information was produced and brought before the court. The certificate was therefore not merely a technical formality. It functioned as a legal mechanism through which the court could be given assurance about the electronic record and the system that produced it. However, this model rests on an assumption that becomes increasingly complicated in the age of generative artificial intelligence. The certificate can provide evidence that a particular digital file came from a particular device or source and that the relevant statutory conditions were satisfied. It can therefore help answer the question: "Is this the same electronic record that was produced and preserved?" It does not necessarily answer a different question: "Does the event represented by this

[3] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[4] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[5] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

electronic record actually correspond to something that happened in the real world?" This distinction becomes crucial when the record itself is capable of being artificially generated.

3 CHANGES WHICH OCCURRED UNDER SECTION 63 BSA

The BSA attempts to modernise the law of evidence and specifically recognises electronic and digital records. Section 61 recognises electronic or digital records, while Section 63 deals with the admissibility of electronic records.[6] In this sense, the BSA acknowledges the increasing importance of digital information within the evidentiary process. Section 63 substantially continues the logic of Section 65B. It establishes conditions relating to the computer or communication device, the regular use of the device, the ordinary course of activities and the production of the electronic record. Most importantly for the present discussion, Section 63(4) is accompanied by a Schedule containing a prescribed certificate.

The Schedule requires the party producing the electronic record to provide details regarding the source of the record. These may include a computer, storage media, DVR, mobile phone, flash drive, CD/DVD, server or cloud. It also asks for identifying information relating to the device, such as the make and model, serial number and relevant identifiers. The certificate further addresses matters such as lawful control of the device, whether it was functioning properly and whether information was regularly fed into the device in the ordinary course of activities.[7]

One of the most notable aspects of the Schedule is its treatment of hash values. A hash may be understood, at a basic level, as a kind of digital fingerprint for a file. When a particular electronic file is processed through a hashing algorithm, it produces a corresponding value. If the file is subsequently changed, even in a small way, the resulting hash may change. The Schedule therefore provides a mechanism for recording the hash value of the electronic or digital record and identifying the algorithm used to generate it. This is an important development because it strengthens the ability of the legal system to establish the integrity of an electronic file. However, it is important not to give the hash function a role that it cannot perform. A hash can assist in establishing that a particular file has remained unchanged from the point at which its hash was calculated. It cannot establish that the contents of the file depict a genuine event. This can be illustrated through a simple example. Suppose a person creates a completely fabricated video using artificial intelligence and saves it on a mobile phone. The video is then copied from the phone and its hash value is calculated. If the file is later produced in court and the hash value matches the certified value, the integrity of that particular file may be established. But the hash does not establish that the person shown in the video actually said or did what the video depicts. In other words, the hash can demonstrate file integrity, but file integrity is not the same as event authenticity. This distinction suggests that Section 63 should be understood as an important procedural development rather than a complete conceptual transformation of electronic evidence law. The BSA provides more structured information regarding the device, the source and the integrity of the record. These safeguards are valuable. Yet they primarily address the history and integrity of the electronic record rather than the truthfulness of the reality represented by the record. This is where deepfakes create a particularly difficult evidentiary problem.

[6] Bharatiya Sakshya Adhiniyam, 2023, §§ 61–63.
[7] *Id.* Schedule to § 63.

4 WHERE THE REGIME BREAKS THROUGH THE DEEPFAKE ERA

A deepfake is synthetic or manipulated media created using artificial intelligence or other digital techniques to make a person appear to say or do something that they did not actually say or do. The technology itself is not limited to videos. Artificial intelligence can also be used to generate or manipulate photographs, audio recordings and other forms of digital content. The evidentiary difficulty created by deepfakes is fundamentally different from ordinary questions of tampering. Traditional digital evidence analysis often asks whether a file has been modified after its creation. Deepfakes complicate this assumption because the file may have been created as a manipulated representation from the beginning. Consider a hypothetical case involving a video allegedly showing a company director approving an unlawful transaction. The video is stored on a mobile phone and produced before a court. The party producing it obtains the necessary certificate under Section 63. The phone was functioning properly, the file was stored on the device and the hash value corresponds with the copy presented to the court. From the perspective of the statutory requirements, the record may appear properly authenticated. Yet suppose the video was generated entirely through artificial intelligence. The director never attended the meeting and never made the statement contained in the video. The problem is therefore not that someone altered the file after it was created. The problem is that the file itself was created to represent an event that never occurred.

This creates a distinction between two different forms of authenticity. The first may be described as custodial authenticity. It concerns whether the electronic record presented to the court is the same record that was obtained from the relevant device or source and whether its integrity has been maintained. Section 63 is particularly useful for this purpose. The device details, certification requirements and hash value can all contribute to establishing this form of authenticity. The second may be described as substantive authenticity. This concerns whether the content of the electronic record accurately represents the underlying event, person, statement or conduct that it purports to show. Substantive authenticity asks whether the person actually spoke those words, whether the event actually occurred and whether the recording is a genuine representation of reality.

The two forms of authenticity may overlap, but they are not identical. A court could therefore encounter a situation in which an electronic record is completely authentic as a digital object but completely false as a representation of an event. This is the central weakness that deepfakes expose in a purely custody-based approach. Recent Indian litigation demonstrates that courts are increasingly being confronted with the consequences of AI-generated and manipulated content. In *Shilpa Shetty Kundra v. Getoutlive.in & Ors.*, the Bombay High Court dealt with material involving AI-generated deepfake content and considered issues relating to privacy, dignity and personality interests.[8] Although such proceedings do not themselves resolve the evidentiary question posed in this paper, they demonstrate the increasing legal significance of synthetic media. The growing use of deepfakes also means that courts cannot simply assume that a visually convincing recording is reliable because it appears to have originated from a genuine device. At the same time, it would be equally problematic to assume that every digital record is potentially fabricated and therefore requires forensic examination.

[8] Shilpa Shetty Kundra v. Getoutlive.in (Bom. HC Dec. 26, 2025). *See also*, on AI-generated content and personality rights, Karan Johar v. Indiawaale.com (Del. HC Sept. 19, 2025); Aishwarya Rai Bachchan v. Vroniq Consulting Pvt. Ltd. (Del. HC Sept. 9, 2025); Hrithik Roshan v. Ashok Kumar (John Doe), CS(COMM) No. 1107 of 2025 (Del. HC).

This creates the need for a balanced framework. A blanket requirement that every video, photograph, audio recording or electronic document be subjected to forensic examination before being relied upon would be difficult to implement. It would increase litigation costs, delay proceedings and place considerable pressure on forensic laboratories and experts. It could also create an unnecessary barrier to the admission of ordinary electronic evidence where there is no genuine reason to doubt its authenticity. The better approach is therefore to retain certification as the ordinary first stage while recognising that certain circumstances should trigger additional scrutiny.

5 THE C.A.S.E. FRAMEWORK (CERTIFICATION–AUTHENTICITY SPLIT FOR ELECTRONIC EVIDENCE)

The central proposal of this paper is the C.A.S.E. Framework, or the Certification–Authenticity Split for Electronic Evidence. The framework is based on a simple proposition: certification and substantive authenticity should not be treated as if they answer the same question. The first stage of the framework is Certification. Section 63 should continue to operate as the ordinary starting point for electronic evidence. The certificate and the accompanying information regarding the source device, manner of production, working condition and hash value perform an important function. They help the court determine whether the electronic record has been properly identified and whether its integrity has been preserved. There is no need to discard this mechanism merely because deepfakes exist. In fact, doing so would create unnecessary uncertainty in the law of electronic evidence. The certificate remains valuable because an electronic record must first be identified and its custodial integrity established before questions concerning its substantive authenticity can meaningfully arise.

The second stage is Authenticity Challenge. Additional scrutiny should arise only when the opposing party raises a specific and reasonably credible challenge to the authenticity of the underlying content. The mere possibility that artificial intelligence could have been used should not be sufficient. If that were the rule, practically every digital recording could be challenged on the basis that it might be synthetic. Instead, the challenge should contain some identifiable basis for suspicion. For example, a party may point to unusual inconsistencies in the audio or video, unexplained changes in lighting or facial movement, inconsistencies between the metadata and the alleged circumstances, evidence that the person shown was elsewhere at the relevant time, discrepancies between the recording and independently established facts, or other circumstances suggesting manipulation.

The purpose of this stage is not to require the challenging party to prove the deepfake immediately. That would place an unrealistic burden on the party who is precisely seeking access to verification. The purpose is to establish a threshold at which the ordinary certification process is no longer sufficient to resolve the dispute. The third stage is Substantive Verification. Once a credible authenticity challenge has been raised, the court may require additional evidence concerning the substantive authenticity of the record. This could include forensic examination of the audio or video, analysis of metadata, examination of the source device, frame-level analysis, examination of encoding patterns, comparison with verified recordings of the relevant person, or other appropriate technical methods. Importantly, this stage should not assume that one particular AI-detection technology is always capable of determining whether a recording is genuine. Detection technologies themselves are developing and may produce inaccurate results.

Therefore, substantive verification should ideally be based on a combination of technical and contextual evidence rather than a single automated conclusion.

For example, if a video allegedly shows a person speaking at a particular conference, forensic examination might be combined with evidence concerning whether the person was actually present at the venue, recordings from other cameras, photographs taken at the event, witness testimony and original device information. The question before the court would then become broader than simply whether a file had been altered. The final stage is Evidentiary Responsibility. Once a credible challenge has crossed the threshold for substantive verification, the party relying upon the electronic record should ordinarily be expected to provide reasonable additional support for its authenticity, particularly where that party has greater access to the original device, source material or surrounding evidence. This should not be understood as an automatic reversal of the burden of proof in every case. Nor should the existence of an authenticity challenge automatically make the electronic record inadmissible. Instead, the court should consider the strength of the challenge, the availability of the relevant evidence and the circumstances of the case when deciding how much additional proof is necessary. The significance of the C.A.S.E. framework therefore lies in its separation of two questions that are often treated as though they were identical. The first question is whether the electronic record is genuine as a record. The second is whether the content of that record genuinely represents the event it claims to represent.

The first question can ordinarily be addressed through Section 63. The second may require additional evidence when a credible challenge is raised. Such an approach also has the advantage of being more realistic for the Indian legal system. India's forensic infrastructure has important capacity constraints, and requiring forensic examination of every electronic record would not be an efficient use of limited resources. A trigger-based system would allow forensic expertise to be directed towards cases where the risk of manipulation is actually material. The approach may also be gradually implemented. Courts could initially apply the framework in cases involving high-risk digital evidence, such as disputed videos, audio recordings or images where the authenticity of the underlying event is central to the dispute. Over time, clearer judicial standards could develop concerning what constitutes a sufficient authenticity challenge and what types of verification should ordinarily follow.

The United Kingdom provides a useful comparative perspective in this regard. Its forensic evidence framework places considerable emphasis on standards, competence and quality management through the statutory role of the Forensic Science Regulator and the applicable Code of Practice.[9] The UK approach is not specifically designed as a deepfake rule and cannot simply be transplanted into Indian evidence law. However, it demonstrates the broader principle that forensic evidence requires institutional standards and reliable processes rather than merely the existence of technical expertise. For India, the important lesson is therefore not that every electronic record must undergo forensic testing. It is that when forensic examination becomes necessary, the examination itself should be carried out according to reliable standards and by appropriately qualified experts. The C.A.S.E. framework consequently seeks to preserve the advantages of the existing statutory system while responding to the new epistemic problem created by synthetic media. It does not reject certification; it places certification in its proper evidentiary role.

[9] FORENSIC SCIENCE REGULATOR, CODE OF PRACTICE (VERSION 2), issued pursuant to the Forensic Science Regulator Act 2021.

6 CONCLUSION

The development of Indian electronic evidence law shows a clear attempt to adapt traditional evidentiary principles to a digital environment. Section 65B of the Indian Evidence Act created a specialised mechanism for electronic records, and the Supreme Court's decisions in *Anvar P.V.* and *Arjun Panditrao* provided important guidance concerning certification and admissibility. The BSA has continued this approach through Section 63 while making the certification process more detailed, including through the Schedule's requirements concerning device information and hash values. These developments are important, but the rise of deepfakes reveals a conceptual limitation that cannot be solved merely by making the certificate more detailed. The certificate can establish important facts about the electronic record. It can help establish where the record came from, how it was produced and whether the particular file has remained unchanged. A hash value can strengthen the proof of digital integrity. However, none of these mechanisms necessarily establish that the event represented by the recording actually occurred. This distinction is increasingly significant because artificial intelligence has changed the nature of digital manipulation. Earlier, the central evidentiary concern could often be expressed as: "Has this recording been altered?" With deepfakes, the more fundamental question may be: "Was there ever a real event corresponding to this recording?"

The answer requires a shift from treating authentication as a single concept to recognising different layers of authenticity. The proposed C.A.S.E. framework attempts to provide such a distinction. Certification remains the ordinary first layer because Section 63 serves an important purpose in establishing the integrity and provenance of electronic evidence. However, where a specific and credible challenge is raised regarding the authenticity of the underlying content, the court should have the ability to move to a second layer involving substantive verification. This may involve forensic analysis as well as independent corroborative evidence. The level of scrutiny should depend upon the circumstances of the case rather than being imposed uniformly upon every electronic record. Such a model also avoids two extremes. On one side is complete reliance on certification, which risks treating a properly preserved falsehood as trustworthy merely because its digital chain of custody is intact. On the other side is universal forensic scrutiny, which would be impractical and could unnecessarily burden the judicial and forensic systems. The deeper lesson is that technological change does not always require completely new legal rules. Sometimes it requires existing legal concepts to be examined more carefully. Section 63 answers an important question about electronic evidence, but deepfakes demonstrate that it does not answer every question that a court may need to ask. Ultimately, the difference can be expressed through two simple questions: "Is this the same file?" and "Is what this file shows actually real?" Section 63 is well equipped to assist with the first question. The challenge for the future of Indian evidence law is to ensure that the second question does not disappear merely because the first one has been answered. The C.A.S.E. framework therefore proposes not a rejection of the existing law, but its development. In an environment where digital evidence can be preserved perfectly while depicting an event that never happened, custody should remain evidence of integrity, but it should not automatically become evidence of truth.

* * *