EVIDENTIARY STANDARDS IN THE ERA OF AI: IS THE BHARATIYA SAKSHYA ADHINIYAM EQUIPPED ENOUGH?

Aditi Shelke, University of Mumbai Law Academy

Chaitanya Adepu, Adv. Balasaheb Apte College of Law

ABSTRACT

This article explores how deepfakes create a huge issue for proving evidence in Indian courts under the new Bharatiya Sakshya Adhiniyam, 2023. It further proves that BSA's rules for checking electronic evidence like making sure devices worked right, tracking who controlled them, matching original data and using hash codes to prove nothing changed are not strong enough now. Contemporary deepfakes are created with such sophistication and disseminated so rapidly across electoral campaigns, misinformation networks, and non-consensual intimate imagery that existing provisions cannot detect fabrication occurring at the point of content creation itself. While examining current laws, our analysis reveals that digital signatures and hash values can verify that files remain unaltered during transmission and storage, but they cannot establish whether the original content depicts actual events or was synthetically generated. Forensic investigators also tend to assume evidence was created by humans, missing the possibility that AI produced it from the start. Our legal system and investigative methods are still catching up to a world where AI can create convincing fake evidence, and our current tools can verify technical authenticity but not whether something was artificially generated. Inspired from around the world, courts being cautious about digitally enhanced images and outright bans on AI edited legal submissions show how different systems are adapting. New laws should require upfront verification that evidence is authentic, using technology neutral forensic tools to detect and filter out fake content which would balance the need to keep up with technological changes while maintaining the justice system's core goal of finding the truth.

Keywords: Artificial Intelligence (AI), Electronic Evidence, Authenticity of Evidence, Bharatiya Sakshya Adhiniyam

INTRODUCTION

The past three decades have witnessed rapid development of technology and digital transformation in every sector due to globalisation. The legislative shift from the Indian Evidence Act, 1872 (IEA) to the Bharatiya Sakshya Adhiniyam, 2023 (BSA) meant inclusion of provisions for electronic evidence, all while retaining the core of the IEA.

It was realised that traditional evidence assessment requires specialized technical expertise when dealing with electronic data. The Examiner of Electronic Evidence is an expert under Section 79A of the Information Technology Act responsible for providing expert opinions on digital records presented in court. Their opinion becomes a relevant fact in court that can significantly influence judicial decisions on admissibility and weight.[1]

The examiner's approval process prescribed under Section 63 of the BSA requires that these conditions must be satisfied before electronic evidence can be deemed reliable:

i. The examiner must verify that the computer resource was functioning properly during the material period. Alternatively, they must show that any malfunction did not compromise the accuracy of the record produced. This acknowledges the vulnerability of digital systems while providing a practical pathway for admissibility when minor technical issues can be shown to be immaterial.

ii. The electronic evidence must have originated from a device under the lawful control of the person tendering it. The device must have been regularly used to store or process information as part of their ordinary activities. This requirement establishes a chain of custody which is a documented and continuous record showing the possession, control, transfer, and handling of evidence from the moment it is created or seized until it is produced in court.

iii. The information must constitute an accurate reproduction or derivation of data that was regularly fed into the computer system. Original input and the evidence presented to the court must be in harmony.

iv. All electronic records tendered as evidence must be accompanied by a certificate in

[1] Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023) s 45.

the form specified in The Schedule of the BSA. This certificate operates as a twopart mechanism. Part A must be completed by the person in charge of the device. Part B requires the signature of an expert. The certificate must include verification of the unique HASH value, typically generated using algorithms such as SHA256 or MD5. This is like the digital footprint proving that the data has remained unaltered since its initial collection and documentation.

On one hand, the law must ensure that electronic evidence meets threshold standards of reliability before influencing judicial decisions. On the other hand, overly stringent requirements could render valuable evidence inadmissible merely due to technical deficiencies unrelated to actual trustworthiness.

Section 79A of the Information Technology Act, 2000 empowers the Central Government to notify specific departments, bodies, or agencies as an "Examiner of Electronic Evidence". Examiners notified under Section 79A provide critical support to Law Enforcement Agencies (LEAs) by investigating serious cybercrime cases and analysing hard disks or mobile devices. Their role is to assist the court in forming an opinion on any matter relating to information transmitted or stored in a computer resource or any other digital form. For instance, the Cyber Forensics Laboratory at CERT-In was notified under Section 79A with an evolving scope that originally covered mobile and disk forensics but was expanded in November 2024 to include Cloud, DVR, and Drone forensics.[2]

The traditional focus was on ensuring the reliability of computer systems, transmission channels, and storage media. It was assumed that digital content originates from actual realworld events and might later be modified or tampered with. However, the emergence of generative AI and deepfake technologies challenges this exact assumption. Fabrication can now happen at the moment of creation itself and produce highly realistic yet completely synthetic images, audio, or video that bear no connection to any actual event.

JUDICIAL TESTS OF AUTHENTICITY

In *Shafhi Mohammad v State of Himachal Pradesh*[3], the Supreme Court recognized the

[2] Standing Committee on Communications and Information Technology, *Action Taken on Fourth Report (Demands for Grants 2024–25)*, Fourteenth Report (Lok Sabha Secretariat, New Delhi 2024–25).
[3] *Shafhi Mohammad v State of Himachal Pradesh* (2018) SCC OnLine SC 56

growing importance of electronic evidence and held that such evidence should not be excluded merely due to the possibility of tampering. The Court emphasized that law must adapt to new technologies and that the key consideration is whether the accuracy of the electronic record can be established through appropriate safeguards.

In *Anvar P.V. v P.K. Basheer and Others*[4], the Supreme Court laid down a strict statutory framework for the admissibility of electronic evidence. The Court held that electronic records, referred to as "computer output," are admissible only if the conditions under Section 65B of the Indian Evidence Act are satisfied. These conditions are the (i) computer was regularly used for the relevant activity, that (ii) information was fed into it in the ordinary course of business, that (iii) the computer was functioning properly during the relevant period, and (iv) the record produced is a faithful reproduction or derivation of the original data. The Court further mandated that a certificate under Section 65B(4), now reflected in Section 63(4) of the BSA, must accompany the electronic record.

The Supreme Court's decision in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[5] distinguished between original electronic records and secondary copies, holding that compliance with Section 65B(4) is mandatory where secondary electronic evidence is relied upon. As deepfakes typically reach courts as circulated, downloaded, or extracted copies rather than originating systems, this precedent significantly raises the evidentiary threshold for their admissibility. This distinction becomes particularly problematic with deepfakes. The very concept of 'original' loses meaning when content is synthetically generated. A deepfake video has no original event to authenticate against. The 'original' itself is fabricated, rendering the secondary evidence framework inadequate. The court noted in *State of Kerala v Balachandran*[6] that expert reports must establish the validity of the methods used for authenticating digital content, which increasingly includes the advanced forensic checks.

These precendents collectively establish that electronic evidence must satisfy both procedural compliance and reliability standards. However, the judicial tests developed thus far assume that digital evidence, once authenticated through proper procedures, reflects actual events rather than AI-generated fabrications.

[4] *Anvar P.V. v P.K. Basheer & Ors.* (2014) SCC OnLine SC 732
[5] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) SCC OnLine SC 571
[6] *State of Kerala v Balachandran* (2025) SCC OnLine Ker 2721

RISE OF SYNTHETIC MEDIA

AI refers to systems that simulate human intelligence by recognizing patterns and drawing conclusions from datasets using machine learning techniques.[7] The number of deepfakes online increased tenfold from 2022 to 2023 alone.[8]

From a gradual deep learning phase in the 2010s to an era of intense acceleration in the 2020s, AI has gone from a niche academic field to a global force that now subtly and virtually influences every sector of society. Generative AI is currently growing at a rate that frequently outpaces modern detection tools.[9]

Deepfakes create incredibly lifelike synthetic media, such as audio, images, and videos, by utilizing AI and deep learning advancements.[10]

In March 2022, a Ukrainian news agency's website was hacked to publish a deepfake video of Ukrainian president Zelensky urging Ukrainians to surrender.[11] Conversely, despite the video being authentic, widespread suspicion emerged online that it was a deepfake when footage of President Bongo of Gabon surfaced in 2019 following his protracted absence due to poor health. This suspicion of fabrication even led to an attempted military coup.[12]

Once deepfakes have been created and published, erasing them in all their versions is virtually impossible when the content spreads across decentralized networks online. In January 2024, an audio recording went viral on social media that showed a US High School Principal making racist and antisemitic remarks including comments that black students were ungrateful and unable to test their way out of a paper bag. He was temporarily removed from school. The investigators determined the recording was fake, a forensic analyst and university professor

[7] Henry A Kissinger and others, The Age of AI (1st edn, Little, Brown and Company 2021) 57–58.
[8] *'Synthetic Media & Deepfakes'* (Center for News, Truth and Integrity, 6 October 2025) https://cnti.org/issueprimers/synthetic-media-deepfakes/ accessed 1 January 2026.
[9] Drexel University, "*On the Trail of Deepfakes, Drexel Researchers Identify 'Fingerprints' of AI-Generated Video"* (24 April 2024) Drexel University News <https://drexel.edu/news/archive/2024/April/machine-learninggenerative-ai-video-detection> accessed 3 January 2026
[10] Sonam Singh and Amol Dhumane, 'Unmasking Digital Deceptions An Integrative Review of Deepfake Detection, Multimedia Forensics, and Cybersecurity Challenges' (2025) *MethodsX* vol. 15 103632 <https://doi.org/10.1016/j.mex.2025.103632>accessed 4 January 2026
[11] Maria Pawelec, 'Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions' (2022) 1(2) *Digital Society* 19 <https://pmc.ncbi.nlm.nih.gov/articles/PMC9453721/>accessed 4 January 2026.
[12] Sonam Singh and Amol Dhumane, 'Unmasking Digital Deceptions: An Integrative Review of Deepfake Detection, Multimedia Forensics, and Cybersecurity Challenges' (2025) MethodsX 103632 <https://pmc.ncbi.nlm.nih.gov/articles/PMC12508882/> accessed 27 December 2025.

contracted by the FBI found the recording contained AI generated content.[13]

Just before the 2020 Delhi Legislative Assembly elections, two videos of BJP leader Manoj Tiwari circulated widely showed him criticising the Arvind Kejriwal government in English and in the Haryanvi dialect. Although they appeared to be ordinary campaign messages, the videos were later revealed to be deepfakes created using lip-sync technology, with scripted audio dubbed onto an original video of Tiwari. The BJP's IT Cell, in collaboration with a political communications firm, used these AI-generated videos to target specific linguistic voter groups and distributed them across thousands of WhatsApp groups and reaching millions of viewers. This was the first known use of deepfakes in an Indian election campaign[14]. In the same vein, the case of *League of Women Voters of New Hampshire v Kramer*[15] addressed the use of AI deepfake robocalls mimicking President Biden's voice to suppress voter turnout.

Non-consensual intimate images (NCII) are the most despicable misuse of deepfake technology, which disproportionately victimizes women and causes maximum psychological harm.[16] The currently existing law under Section 66E of the Information Technology Act, dealing with privacy violations, is not sufficient for cases of advanced high-tech deepfake NCII. The section in question refers to "capturing" or "transmitting" images, and thus, it might be excluding computer-generated images that do not show the recording of any actual intimate images. It is necessary to change the law to be able to effectively deal with AI-generated sexual content that does not fall under the usual definitions of invasion of privacy.

Elon Musk's Grok AI on X was observed generating sexualized images of women and minors by digitally undressing them upon user requests, prompting investigations by France and India after experts warned xAI ignored concerns about this predictable misuse.[17] In the USA, The TAKE IT DOWN Act mandates that non-consensual sexually explicit image be prohibited, and this is extended even to those generated by AI. According to the bill, platforms will be held

[13] Associated Press, 'AI-generated voice recording leads to arrest after Maryland principal is framed' (AP News, 2024) <https://apnews.com/article/ai-maryland-principal-voice-recording-663d5bc0714a3af221392cc6f1af985e>

[14] VICE News, 'The First Use of Deepfakes in an Indian Election Was by the BJP' (VICE, 2024) <https://www.vice.com/en/article/the-first-use-of-deepfakes-in-indian-election-by-bjp/.>

[15] *League of Women Voters of New Hampshire v Kramer* (D NH, 26 March 2025) No 24-cv-73, 2025 WL 919897

[16] Harmanjeet Singh and Ritu Panta, 'Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law' (2024) International Journal for Multidisciplinary Research.

[17] A J Vicens and Raphael Satter, 'Elon Musk's Grok AI floods X with sexualized photos of women and minors' (Reuters, 4 January 2026) <https://www.reuters.com/legal/litigation/grok-says-safeguard-lapses-led-imagesminors-minimal-clothing-x-2026-01-02/> accessed 7 January 2026.

accountable and, if they fail to remove such content within 48 hours from the time of their being notified, they will be subjected to a prison term of up to three years.[18]

The Delhi High Court's intervention in the *Anjana Om Kashyap* case[19] ordered immediate content removal and mandating user identification. The same High Court also acknowledged the deceptive nature of deepfakes and the need for rigorous verification in *Ankur Warikoo v John Doe*[20] Industry thought leaders and experts predict that up to 90% of online content will be synthetic by 2027[21] An AI-generated "actress" named Tilly Norwood created by Eline Van der Velden sparked widespread backlash for mimicking real human performers and being marketed as a potential replacement for actors.[22] Generative AI is currently growing at a rate that frequently outpaces modern detection tools.[23]

ADEQUACY OF THE BHARATIYA SAKSHYA ADHINIYAM

While deepfake technology opens new doors for digital evidence investigation and exhibition, its use in legal cases poses significant legal and ethical issues. These problems are based on the deceptive nature of artificial intelligence, the lack of legal protection, procedural uncertainty, and the inability of individuals to recognize falsehood.

A significant challenge posed by AI-generated deepfakes lies in their ease of creation and the corresponding difficulty in reliable detection[24] The *Parliament attack case*[25] revolved around the 2001 terrorist attack on the Indian parliament. When the prosecution wanted to present call records as evidence, the defence objected on the ground that the records didn't have the required certificate as per section 65B(4) of IEA. It was held that the electronic records could be accepted as evidence even without the certificate in section 65B(4) of the IEA. The court

[18] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act Pub L No 119–12 (US, 2025)
[19] T.V. Today Network Ltd. v Google LLC & Ors.(2025) SCC OnLine Del 4587
[20] *Ankur Warikoo v John Doe* (2025) SCC OnLine Del 3727
[21] *Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era* (US Department of Defence, January 2025)
[22] Dani Di Placido, *'The Backlash Against AI-Generated "Actress" Tilly Norwood, Explained'* (Forbes, 30 September 2025) https://www.forbes.com/sites/danidiplacido/2025/09/30/the-backlash-against-ai-generatedactress-tilly-norwood-explained/ accessed 5 January 2026.
[23] *On the Trail of Deepfakes, Drexel Researchers Identify 'Fingerprints' of AI-Generated Video* (Drexel University, 24 April 2024) https://drexel.edu/news/archive/2024/April/machine-learning-generative-ai-video-detection accessed 1 January 2026.
[24] Jack Karp, 'AI Deepens "Quicksand" Landscape for Evidentiary Measures' (Law360 Pulse, 16 April 2025) https://www.law360.com/pulse/articles/2320591
[25] *State N.C.T of Delhi v Navjot Sandhu* (2003) SCC OnLine SC 654

further held that the admissibility of electronic record as evidence depends on the details of each case and facts like reliability of evidence, where it came from and how it was presented have to be considered. However, the same view is opposed in *Ravinder Singh Alias Kaku v State of Punjab*[26] wherein the court held that the electronic evidence produced before the court should have been in accordance with the statute and should have compiled with the certification requirement, for it to be admissible in the court of law. Additionally, the court stated that oral evidence, in the absence of such certificate cannot possibly suffice as section 65B(4) of the Evidence Act, 1872 is a mandatory requirement of the law.

The "liar's dividend" is a political and social phenomenon where the mere existence of deepfake technology allows bad actors to escape accountability by claiming that authentic evidence is a machine-generated fake. As photos, videos, and audio become easier to fabricate, the public loses faith in all digital media. Bad actors take advantage of this cynicism trap to discredit legitimate, incriminating evidence used against them.[27] In legal contexts, this is often called the "deepfake defense". Defence counsel may attempt to dismiss genuine video evidence by painting it as a deepfake, leading juries to accord little or no weight to authentic footage they should be considering.[28] The liar's dividend allows individuals to dismiss authentic evidence by claiming it is AI-generated, forcing courts into expensive authenticity disputes.[29] The BSA provides no framework for navigating this problem, offering no guidance on when such challenges should be entertained or dismissed as frivolous.

The Examiner of Electronic Evidence focuses on identifying the computer source, verifying whether the electronic record was produced by a regularly used device, ensuring integrity through hash values, examining metadata consistency, and confirming that the evidence has remained untampered during the chain of custody but he does not determine whether the content itself is fabricated. It must be noted that hash values prove no alteration after hashing,

[26] *Ravinder Singh Alias Kaku v State of Punjab* (2022) 7 SCC 581
[27] James Bickford, 'AI Is Coming, But the Rules Aren't Ready' (Georgetown Law Technology Review, January 2025) <https://georgetownlawtechreview.org/ai-is-coming-but-the-rules-arent-ready/GLTR-01-2025/> accessed 3 January 2026.
[28] Lisa Marshall, 'Deepfakes and AI in the Courtroom: Report Calls for Legal Reforms to Address a Troubling Trend' (CU Boulder Today, 17 November 2025) <https://www.colorado.edu/today/2025/11/17/deepfakes-and-aicourtroom-report-calls-legal-reforms-address-troubling-trend>accessed 7 January 2026.
[29] Helen Robinson and Andrew Spencer, 'When the Evidence Thinks for Itself: How Will the Courts Keep AIGenerated Evidence in Check?' (Taylor Wessing, 12 December 2025) <https://www.taylorwessing.com/en/insights-and-events/insights/2025/12/how-will-the-courts-keep-aigenerated-evidence-in-check> accessed 5 January 2026.

not that the content was originally genuine.

This entire process of examining electronic evidence works under the assumption that the digital content of electronic record is generated by a human and then can be subjected to subsequent manipulation. But this assumption must be challenged in this era of AI-generated content, where fabrication of evidence can occur at the point of creation itself. The BSA's provisions are equipped to answer the question "has this record been tampered with?" but not the fundamentally different question "was this record ever real?"

Expecting an Examiner of Electronic Evidence to decide whether digital content reflects a realworld event would stretch their role beyond forensic verification. The examiner's statutory function is limited to validating system integrity, data consistency, and chain of custody. Determining whether content is genuine or fabricated involves factual assessment is traditionally the court's role and requires judicial scrutiny. Legislative reform should potentially therefore support courts in this context rather than expanding the examiner's mandate beyond its forensic limits.

Courts relying on Section 63 compliance may admit deepfake evidence that satisfies all technical requirements while being entirely fabricated. A certificate under Section 63(4) confirming device functionality, lawful control, accurate reproduction, and hash value integrity provides false assurance of authenticity. The certificate attests to procedural compliance, not substantive genuineness.

To identify deepfakes, there are a number of technical options available, such as the following:

i. Software for AI Output Detection: This kind of software examines digital traces left by artificial intelligence-generated material to ascertain whether a picture, video, or audio file has been altered.

ii. AI-Powered Watermarking: This method entails tagging an image or text with a special code that indicates where it came from. This facilitates the process of tracking and tracing the origin of media content, thereby aiding in the assessment of its legitimacy. iii. Content Provenance: This tactic seeks to identify the sources of digital media, both synthetic and natural. Keeping track of a piece of media's history and sources makes it

easier to identify instances of manipulation.[30]

FOREIGN APPROACHES TO AI

In the *Kyle Rittenhouse* trial[31], the prosecution tried to rely on a zoomed in drone video to show the defendant raising his rifle, but the defence objected that Apple's pinch to zoom feature might algorithmically create new pixels and alter the image. Uncertain about how technology worked the judge refused to admit the video without immediate expert testimony.

The Canadian Judicial Council acknowledges the growing difficulties judges face in dealing with digitally enhanced and AI-generated evidence, particularly with respect to authentication and reliability. Their Guidelines recognize that the emergence of deepfakes and similar technologies complicates traditional evidentiary assessment and caution that existing rules of evidence may not always be adequate to address these challenges. They advise courts to consider the necessity of expert testimony to authenticate disputed AI-generated or digitally enhanced material and encourage a re-examination of evidence.[32]

In the case of *State v Puloka*[33] the court had an AI enhanced cellphone video processed using the Topaz Video Enhance AI and evaluated it under multiple standards such as Frye[34], FRE (Federal Rules of Evidence) 702, 401 and 403. But the defence failed to prove that the enhancement method was generally accepted in the forensic video community or if it was reliable. The court also found the video irrelevant because it showed what the AI 'thought' happened instead of the actual events. This case demonstrates the difficulty of applying traditional evidence rules to AI-enhanced content. The court's concern was that the video showed what AI 'thought' happened rather than actual events. AI interpolation creates new visual information that has no direct correspondence to reality. Yet it may appear seamlessly integrated and authentic to the untrained observer.

In *USA v Khalilian*[35], the defense claimed that voice recordings might have been created using

[30] Yash Dahiya, *'The Rise of Deepfake Technology: A Threat to Evidence in Arbitration?'* (LiveLaw, 22 November 2023) <https://www.livelaw.in/articles/the-rise-of-deepfake-technology-a-threat-to-evidence-in-arbitration242718#_ftn10> accessed 2 January 2026

[31] *State v Rittenhouse* (Wis. Cir. Ct. Crim., 2021).

[32] Canadian Judicial Council, Guidelines for the Use of Artificial Intelligence in Canadian Courts (adopted 1 September 2024).

[33] *State v Puloka* (Wash. Super. Ct., 2024).

[34] Judicial test of determining the authenticity of evidence as laid down in *Frye v United States* (DC Cir, 1923) 293 F 1013.

[35] *United States v Khalilian* (C.D. Cal, Case No 2:23-cr-00331)

AI. The prosecutors proved the recordings were real by having witnesses say they recognized the defendant's voice. The court accepted this as 'probably enough' evidence, but this low standard of proof may not be good enough anymore since AI deepfake technology can now create very convincing fake voice recordings that sound exactly like someone.

The Superior Court of California, County of Alameda identified suspicious exhibits, including video testimonials, images, and message screenshots displaying characteristics of deepfakes and digital manipulation. It also found numerous instances of fabrication. Video exhibits were deepfakes showing robotic speech patterns and mismatched facial movements. Photographs were digitally altered, message screenshots were inconsistent with their purported platforms, and metadata was unreliable and suggested manipulation. Given the deliberate submission of fabricated evidence and the resulting harm to judicial integrity, the Court imposed terminating sanctions and dismissed the action with prejudice.[36] In *Project Veritas v Schmidt*[37], the Court recognised that the rise of deepfake technology has intensified the risks associated with cases involving improper audio recordings, given how easily such recordings can now be altered or repurposed. It was also observed that technological advances are steadily eroding the assumption that audio recordings are inherently self-authenticating.

Courts of New Zealand Guidelines for judges and non-lawyers stress that GenAI can also fabricate convincing images, audio and other media, which parties could present as evidence, and that it may be appropriate to inquire whether a lay litigant has used a GenAI chatbot, and to ask what checks for accuracy they have undertaken (if any)[38] Similarly, a 2024 Chief Justice of New South Wales Practice Note prohibits the use of generative AI to generate or alter affidavits, witness statements, or expert reports, and requires that such evidence reflect a person's own knowledge, not AI-generated content. It also warns that information subject to non-publication or suppression orders etc. must not be entered into any Gen AI program and that Gen AI must not be used in generating the content of affidavits, witness statements, character references or other material that is intended to reflect the deponent or witness' evidence and/or opinion, or other material tendered in evidence or used in cross examination.[39]

[36] *Ariel Mendones & Anr. v Cushman and Wakefield Inc & Ors. (*Superior Court of California, County of Alameda, No 23CV028772, 9 September 2025).
[37] *Project Veritas v Schmidt* 72 F.4th 1043 (9th Cir 2023)
[38] Courts of New Zealand Guidelines for Judges, Judicial Officers, Tribunal Members and Judicial Support Staff on the Use of Generative Artificial Intelligence in Courts and Tribunals (2023), adopted on 7 December 2023
[39] Chief Justice of New South Wales Practice Note SC Gen 23 on the Use of Generative Artificial Intelligence (2024), adopted on 21 November 2024

NEED FOR REFORM

In the United States, a proposed 901(c) amendment to the Federal Rules of Evidence would conditionally raise burden for authenticity above the current sufficiency standard. Under this amendment, a party could object to the authenticity of evidence due to deepfake concerns. However, the opponent's objection itself would need to meet the sufficiency standard.[40]

China has enacted a law on deepfakes from the Cyberspace Administration of China (CAC) requiring labelling of content created by AI.[41] It prohibits creating illegal content through deepfakes and requires user identity authentication for services utilizing deepfakes. Criminal liability and removal of content are in store for offenders.

The Indian National Crime Records Bureau (NCRB) and Central Forensic Science Laboratories (CFSLs) is working together with the Indian Institutes of Technology (IIT) in Delhi and Hyderabad to create systems for AI detection.[42] These systems employ 'Generative Adversarial Network (GAN) signature analysis' to locate the synthetic origin, a method that is being introduced in cybercrime units for testing.[43]

We suggest that before the court even moves to the admissibility stage under Section 63, there should be a preliminary screening focused on the authenticity of the content of the electronic record itself. This would mean first examining whether the nature and substance of the digital content can be treated as genuine and credible, independent of compliance with procedural requirements like certification or mode of production. Such an authenticity filter would be broad and technology-neutral, but it would still be capable of addressing risks posed by AImanipulated evidence as part of the larger problem of unreliable digital content. For this purpose, we suggest an amendment to Section 63 by the addition of a new sub-section (1A), wherein, before the court proceeds to examine the admissibility of an electronic record under the existing requirements of Section 63, it is required to undertake a preliminary scrutiny focused on the authenticity of the content of the electronic record itself.

---

[40] Brandon L Garrett, 'Deepfaked Evidence: What Case Law Tells Us About How the Rules of Authenticity Need to Change' (6 June 2025) Berkeley Technology Law Journal <https://btlj.org/2025/06/deepfaked-evidence-whatcase-law-tells-us-about-how-the-rules-of-authenticity-needs-to-change/> accessed 1 January 2026

[41] Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services* (adopted on 25 November 2022)

[42] S Bhattacharya, 'Deepfake Evidence and Judicial Accountability in India' (2023) 16 NUJS Law Review 87.

[43] Harmanjeet Singh and Ritu Panta, 'Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law' (2024) International Journal for Multidisciplinary Research.