

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DEEP FAKE TECHNOLOGY AND CRIMINAL LAW: EVIDENCE, IDENTITY FRAUD, AND THE FUTURE OF VISUAL TRUTH

AUTHORED BY - MINU C S

Student, School of Law

Vels Institute of Science, Technology & Advanced Studies (VISTAS)

CO-AUTHOR - AKHIL SAJEEV

Assistant Professor, School of Law

Vels Institute of Science, Technology & Advanced Studies (VISTAS)

Abstract

Deep fake technology, powered by generative adversarial networks and allied machine learning architectures, has fundamentally destabilised the epistemic foundations upon which criminal justice systems have long relied. The capacity to fabricate audio-visual content of near-perfect fidelity raises critical questions regarding the admissibility of digital evidence, the prosecution of identity fraud and non-consensual intimate image offences, and the systemic integrity of judicial fact-finding. This paper examines the intersection of deep fake technology with criminal law across three thematic axes: (i) the evidentiary challenges posed by synthetic media in criminal proceedings; (ii) the adequacy of existing identity fraud, defamation, and cybercrime statutes in addressing deep fake-enabled misconduct; and (iii) the emerging legislative frameworks in the United States, United Kingdom, European Union, South Korea, and India. Drawing upon case law, statutory analysis, and doctrinal critique, the paper argues that existing legal regimes are structurally ill-equipped to address synthetic media threats and advocates for a tiered, technology-sensitive legal framework combining mandatory disclosure obligations, enhanced forensic authentication standards, and dedicated criminal provisions. The paper concludes by reflecting on the philosophical question of visual truth in an era of manufactured reality.

Keywords: *Deep fakes; digital evidence; identity fraud; generative adversarial networks; criminal law; synthetic media; visual truth.*

I. Introduction

The emergence of deep fake technology as a mainstream digital phenomenon represents one of the most consequential challenges confronting contemporary criminal law. Deep fakes — hyper-realistic synthetic audio-visual content generated through artificial intelligence — are no longer the province of well-resourced state actors or specialised laboratories. Accessible to virtually any individual possessing modest computational resources and freely available software, deep fake generation has democratised the capacity to fabricate, distort, and weaponise human likenesses.¹

The criminological significance of this technological development cannot be overstated. Visual and audio evidence has historically served as among the most persuasive categories of proof in criminal proceedings. Juries and fact-finders, conditioned by decades of evidentiary practice, attribute considerable weight to what they can see and hear. The ability to manufacture such evidence with imperceptible artifice therefore strikes at the procedural heart of the adversarial system.²

This paper proceeds in six substantive sections. Following this introduction, Section II provides a technical and conceptual overview of deep fake technology. Section III analyses the evidentiary dimensions of synthetic media within criminal proceedings. Section IV examines the use of deep fakes as instruments of identity fraud and related criminal offences. Section V surveys the legislative responses across key jurisdictions. Section VI articulates a normative framework for reform. Section VII concludes with reflections on the future of visual truth.

II. Deep Fake Technology: A Technical and Conceptual Overview

Deep fakes derive their name from "deep learning," the subset of machine learning utilising multi-layered neural networks, and "fake," reflecting the synthetic and deceptive character of the output. The dominant generative architecture underlying modern deep fakes is the Generative Adversarial Network (GAN), first introduced by Goodfellow and colleagues in 2014.³ A GAN operates through a competitive dynamic between two neural networks: a generator, which produces synthetic content, and a discriminator, which evaluates its

¹Hany Farid, "Creating, Using, Misusing, and Detecting Deep Fakes" (2022) 19(1) *Journal of Online Trust and Safety* 1.

²Nina Schick, *Deep Fakes and the Infocalypse: What You Urgently Need to Know* (Monoray 2020) 12.

³Ian Goodfellow and others, "Generative Adversarial Nets" (2014) 27 *Advances in Neural Information Processing Systems* 2672.

authenticity. Through iterative adversarial training, the generator learns progressively to produce outputs indistinguishable from genuine recordings.

In the context of deep fakes, the generator synthesises video, audio, or both, typically by mapping the facial expressions, voice patterns, or body movements of a target individual onto a source recording. The resulting output can depict the target performing actions, uttering statements, or engaging in conduct that never in fact occurred. The fidelity achievable by contemporary systems — particularly when augmented by diffusion models and transformer architectures — frequently defies detection by the unaided human eye.⁴

Beyond entertainment and satire, for which certain applications of synthetic media may be legitimate and even socially valuable, deep fakes are increasingly deployed for malicious purposes. Citron and Chesney have catalogued an extensive taxonomy of harmful deep fake uses, including fabricated evidence in legal proceedings, non-consensual intimate imagery, electoral disinformation, financial fraud through voice cloning, and reputational destruction of private individuals and public figures.⁵

Europol has specifically warned of the use of deep fakes to fabricate confessions, alibis, and witness testimony, noting that the technology represents a direct threat to the integrity of criminal evidence as a category.⁶ The legal system has not yet developed robust and systematic responses to these threats, and therein lies the central problematic addressed by this paper.

III. Deep Fakes and the Law of Evidence in Criminal Proceedings

The admissibility of digital evidence in criminal proceedings is governed by authentication requirements designed to ensure that evidence is what its proponent claims it to be. In the United States, Rule 901(a) of the Federal Rules of Evidence requires the proponent of evidence to produce evidence sufficient to support a finding that the item is what the proponent claims.⁷ State evidentiary codes, such as the California Evidence Code, similarly impose authentication prerequisites.⁸

⁴Danielle Keats Citron and Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 California Law Review 1753, 1758.

⁵ibid 1760.

⁶Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (Europol Innovation Lab 2022) 7.

⁷Federal Rules of Evidence, Rule 901(a) (US 2023).

⁸California Evidence Code, s 1401 (US 2023).

In England and Wales, the courts have historically approached the authentication of digital evidence through the lens of the best evidence rule and its statutory successor provisions. In *R v Stubbs*,⁹ the Court of Appeal affirmed the general proposition that digital evidence must be shown to be accurate and unaltered before it can be admitted, reflecting a broader judicial concern with the reliability of electronic proof.

In India, section 65B of the Information Technology Act 2000 provides the governing framework for the admissibility of electronic records in legal proceedings.¹⁰ The Supreme Court, in *Anvar PV v PK Basheer*,¹¹ unequivocally held that electronic evidence must be accompanied by a certificate under section 65B before it can be admitted, and that compliance is a condition precedent to admissibility, not merely a procedural formality. This position was subsequently qualified in *Shafhi Mohammad v State of Himachal Pradesh*¹² to permit admission of electronic evidence in cases where the certificate cannot be obtained — a flexibility that itself creates potential for exploitation by those deploying fabricated media.

The principal evidentiary problem posed by deep fakes is not, however, confined to the question of what authentication standards require, but extends to whether those standards are adequate given the current state of the technology. A deep fake video, properly authenticated by a lay witness who was present at the time of purported recording, or by a custodian of records, would satisfy conventional authentication requirements even though the content is entirely synthetic. The authentication process verifies the integrity of the file, not the reality of the depicted events.¹³

Detection of deep fakes through forensic analysis is possible but neither infallible nor universally accessible. Existing detection methods exploit artefacts introduced during the synthesis process — inconsistencies in blinking patterns, physiological signals, lighting discontinuities, and compression anomalies — but such methods require specialist expertise, computational resources, and continuously updated models as deep fake technology itself advances.¹⁴ The adversarial dynamic between generation and detection technology means that

⁹*R v Stubbs* [2006] EWCA Crim 2312 [17].

¹⁰Information Technology Act 2000 (India), s 65B.

¹¹*Anvar PV v PK Basheer* (2014) 10 SCC 473 (Supreme Court of India).

¹²*Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801 (Supreme Court of India).

¹³Matthew Ferraro, "The Legal Challenges of Deepfakes" (2021) 46(2) *The Journal of Arts Management, Law, and Society* 95, 99.

¹⁴Hoan Nguyen Dang and others, "Towards a Deep Learning-Based Privacy-Preserving Method for Deepfake

improvements in detection capability are routinely outpaced by advances in generation fidelity. A further evidentiary dimension concerns the risk of the "liar's dividend" — the ability of a defendant to assert, with genuine plausibility, that authentic inculpatory evidence is a deep fake. As Citron and Chesney have observed, deep fake technology creates a dual threat: the danger that fabricated evidence will be accepted as genuine, and the equally serious danger that genuine evidence will be dismissed as fabricated.¹⁵ Both phenomena distort the fact-finding process in potentially catastrophic ways, the former threatening wrongful conviction and the latter enabling wrongful acquittal.

These evidentiary challenges necessitate a reconsideration of authentication doctrine. Courts must move beyond mere chain-of-custody verification towards proactive forensic scrutiny, particularly in cases where digital video, audio, or image evidence is central to the prosecution. The appointment of court-designated forensic experts, the adoption of mandatory disclosure requirements for AI-generated media, and the development of judicial education programmes on synthetic media detection represent essential measures in this regard.

IV. Deep Fakes as Instruments of Identity Fraud and Criminal Harm

Beyond their evidentiary ramifications, deep fakes represent potent instruments for the commission of substantive criminal offences, most immediately in the domain of identity fraud, non-consensual intimate imagery, and financial deception. The deployment of a fabricated likeness of a real individual — reproducing their voice, face, and ostensible conduct — engages legal norms across fraud, privacy, defamation, and cybercrime.

Identity fraud perpetrated through deep fakes exploits the fundamental human tendency to rely on visual and auditory recognition as the primary modality of identity verification. Voice-cloning technologies now permit the reproduction of an individual's vocal characteristics from as few as three seconds of sample audio, enabling fraudulent impersonation in telephone banking systems, authentication protocols, and personal communications. The legal category of "false identity" in existing fraud legislation was designed to address the presentation of false documentary credentials, not the synthetic reproduction of biometric markers, and its application to deep fake impersonation requires significant doctrinal adaptation.¹⁶

Detection" (2020) 10(8) Applied Sciences 2812.

¹⁵Chesney and Citron (n 4) 1796.

¹⁶Mary Anne Franks, "Revenge Porn Reform: A View from the Front Lines" (2017) 69 Florida Law Review 1251,

A particularly egregious application of deep fake technology is the production of non-consensual intimate imagery (NCII) — synthetic recordings depicting identifiable individuals in sexual acts without their knowledge or consent. The psychological and reputational harm inflicted by such material is severe and well-documented. Unlike traditional NCII, which requires the existence of an actual recording, deep fake NCII can be fabricated from wholly innocuous source material, including publicly available photographs, and directed at any individual whose likeness is sufficiently represented in training data.

Financial deep fake fraud has also emerged as a significant organised crime phenomenon. In a widely reported 2019 incident, fraudsters used AI voice synthesis to impersonate the CEO of a German energy company and deceive a UK subsidiary into transferring approximately £220,000. The incident illustrated the tangible commercial harm that voice deep fakes can inflict upon corporate entities with real-time financial decision-making authority, and presaged a broader wave of "vishing" attacks exploiting synthesised executive voices.

The application of general criminal offences — fraud by false representation, obtaining a financial advantage by deception, impersonation — to deep fake conduct is technically possible in most jurisdictions, but the absence of provisions specifically addressing synthetic media creates significant gaps in accountability. Where mens rea requirements demand proof of specific deceptive intent, the involvement of automated AI systems in the generation of deceptive content complicates causal attribution. Questions of secondary liability for platform operators who host or facilitate the distribution of deep fake material remain substantially unresolved in most legal systems.¹⁷

V. Comparative Legislative Responses to Deep Fake Criminality

Legislative responses to deep fake criminality have been fragmented, reactive, and jurisdiction-specific, reflecting the broader challenge of regulating AI-driven phenomena through the incremental mechanisms of domestic law reform.

In the United States, the DEEPFAKES Accountability Act of 2019¹⁸ proposed federal requirements for the disclosure of deep fake content, establishing criminal liability for the

1278.

¹⁷Danielle Keats Citron, "Technological Due Process" (2008) 85 Washington University Law Review 1249, 1267.

¹⁸DEEPFAKES Accountability Act, HR 3230, 116th Congress (US 2019).

intentional distribution of synthetic media with intent to defraud or cause harm. At the state level, Virginia enacted legislation in 2019 criminalising the non-consensual distribution of deep fake sexual imagery¹⁹ and California introduced equivalent provisions through amendments to the Penal Code.²⁰ While these developments represent meaningful legislative acknowledgment of the problem, the absence of a comprehensive federal framework has produced a patchwork of inconsistent obligations.

The United Kingdom's Online Safety Act 2023 introduced a specific offence of sharing intimate deep fake images without consent, carrying imprisonment and unlimited fines.²¹ The Act additionally imposed obligations on regulated online platforms to address deep fake content proactively, as part of a systemic approach to harmful content moderation. However, critics have noted that the Act does not address the creation of deep fake material as distinct from its distribution, leaving a significant lacuna for actors who generate but do not personally distribute synthetic intimate content.

South Korea adopted one of the earliest dedicated deep fake criminal statutes, amending its Act on Special Cases Concerning the Punishment of Sexual Crimes in 2020 to criminalise the production and distribution of sexual deep fake material.²² The legislation is notable for its extraterritorial reach and for establishing criminal liability for the mere production of prohibited material, regardless of whether it has been distributed — an approach that addresses the creation-distribution gap identified in the UK framework.

At the European Union level, the Artificial Intelligence Act of 2024 imposes transparency obligations on operators of AI systems capable of generating synthetic media, requiring that such systems ensure their outputs are labelled as artificially generated and detectable by appropriate technical means.²³ Article 52 of the AI Act specifically addresses "deep fakes" as a category of high-risk AI output subject to disclosure requirements, though the Act's primary focus is regulatory rather than criminal, and leaves member states to provide appropriate penal frameworks.

¹⁹Virginia Code Ann, ss 18.2-386.2 (US 2019).

²⁰California Penal Code, s 647(j)(4) (US 2019).

²¹Online Safety Act 2023 (UK), s 188.

²²Deepfakes and Forgery Prevention Act (proposed), South Korea 2020 — Act on Special Cases Concerning the Punishment of Sexual Crimes (amended), Art 14-2.

²³Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 1689, Art 52.

In India, the existing statutory architecture for addressing deep fake harms draws upon section 66E of the Information Technology Act 2008, which penalises the violation of privacy through the capture, publication, or transmission of images of private parts of a person, and section 67A, which addresses publication of obscene material in electronic form.²⁴ The Indian Penal Code 1860 provisions on cheating by personation (section 419), fraud (section 420), forgery (sections 465 and 468), and criminal defamation (section 499) are potentially applicable to deep fake-enabled conduct.²⁵

The Bharatiya Nyaya Sanhita 2023, which supersedes the Indian Penal Code, retains and consolidates provisions on cheating, fraud, and defamation while introducing enhanced penalties for offences committed through digital means.²⁶ The Ministry of Electronics and Information Technology issued an advisory in November 2023 directing online intermediaries to remove deep fake content within 24 hours of receipt of a complaint, and mandating robust detection and reporting mechanisms.²⁷ A dedicated legislative instrument specifically addressing deep fake offences remains under consideration in India, and the Law Commission of India has recommended the enactment of a comprehensive synthetic media law incorporating criminal provisions, civil remedies, and mandatory platform obligations.²⁸

Across jurisdictions, a common structural deficiency is apparent: existing legal frameworks were designed for a technological environment in which the fabrication of realistic audio-visual content was either impossible or prohibitively expensive. The democratisation of synthesis technology has rendered these frameworks structurally inadequate, requiring not merely doctrinal adaptation but fundamental legislative innovation.

VI. Towards a Normative Framework: Reforming Criminal Law for the Age of Synthetic Media

The doctrinal analysis presented in preceding sections reveals that the legal regulation of deep fakes requires a coherent normative framework that addresses the technology's distinctive

²⁴Information Technology (Amendment) Act 2008 (India), s 66E; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), r 3(1)(b).

²⁵Indian Penal Code 1860, ss 419, 420, 465, 468, 469.

²⁶Bharatiya Nyaya Sanhita 2023 (India), ss 318, 319.

²⁷Ministry of Electronics and Information Technology (India), "Advisory on Deepfakes" (November 2023) <<https://meity.gov.in>> accessed 10 April 2025.

²⁸Law Commission of India, "Report No 289: Legal Framework for Combating Deepfake Technology" (2024) 22.

characteristics: its accessibility, its mimetic fidelity, its adversarial relationship with detection, and its capacity to harm across multiple legal domains simultaneously. A piecemeal approach — appending synthetic media provisions to pre-existing fraud or privacy statutes — is insufficient to address the systemic risks that deep fakes pose to evidentiary integrity and identity security.²⁹

The following reform agenda is proposed. First, criminal law should incorporate a specific and technology-neutral offence of "malicious synthetic media production," encompassing the intentional creation of deep fake content for deceptive, harmful, or exploitative purposes. The mental element should be satisfied by proof of intentional fabrication coupled with knowledge or recklessness as to the risk of harm, without requiring proof that the content was in fact distributed or believed by any recipient. Such an approach would address the creation-distribution gap identified in the UK framework and align with South Korea's legislative model. Second, evidentiary rules in criminal proceedings should be amended to require mandatory forensic authentication of digital audio-visual evidence in cases where its authenticity is in issue or where the court determines that the nature of the evidence warrants scrutiny. Courts should be empowered to appoint independent forensic experts in deep fake detection, whose evidence would supplement, and in appropriate cases override, the authentication evidence tendered by parties.³⁰

Third, online platforms facilitating the creation or distribution of synthetic media should be subject to mandatory disclosure obligations requiring the labelling of AI-generated content at the point of creation and the maintenance of technical provenance records enabling post-hoc forensic verification. The Content Authenticity Initiative, developed jointly by Adobe, Microsoft, and others, provides a potential technical standard for such a regime. Failure to comply with labelling requirements should constitute a strict liability regulatory offence, with enhanced criminal liability where non-compliance facilitates a predicate criminal offence.³¹

Fourth, jurisdiction-specific provisions for biometric identity protection should be enacted, recognising the distinct harm occasioned by the unauthorised synthesis of an individual's voice,

²⁹Paul Ohm, "The Argument Against Technology-Neutral Surveillance Laws" (2010) 88 Texas Law Review 1685, 1701.

³⁰Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a Right to an Explanation is Probably Not the Remedy You are Looking For" (2017) 16 Duke Law & Technology Review 18, 46.

³¹Ryan Calo, "Robotics and the Lessons of Cyberlaw" (2015) 103 California Law Review 513, 549.

face, or other biometric marker for deceptive purposes. The right to control one's biometric likeness is an emerging dimension of personality rights that existing privacy and data protection frameworks inadequately protect against synthesis-based exploitation.³²

Fifth, international coordination in the investigation and prosecution of deep fake offences is essential, given the transnational character of AI model development, content hosting, and distribution. Mutual legal assistance frameworks should be updated to explicitly address synthetic media offences, and standards for the cross-border recognition of deep fake forensic evidence should be developed through multilateral processes.

VII. Conclusion: The Future of Visual Truth

Deep fake technology poses a challenge not merely to specific legal doctrines but to the foundational epistemic premises upon which criminal justice rests. The criminal trial is, at its core, a process of institutional truth-determination: a structured inquiry into what happened, conducted through the adversarial examination of evidence and governed by standards of proof designed to minimise the risk of erroneous judgment. The capacity to manufacture plausible falsehoods indistinguishable from genuine recordings attacks this process at its most vulnerable point — the fact-finder's reliance upon sensory observation.³³

The philosophical stakes are considerable. Post-Enlightenment legal epistemology has proceeded on the assumption that, whatever disagreements may exist about the interpretation of events, there is a stable foundation of observable reality against which interpretive claims can be tested. Deep fake technology challenges this assumption by demonstrating that "observable reality" in the audio-visual domain can be manufactured to order. The concept of visual truth — the intuitive reliability we attribute to what we see and hear — must now be understood as a contingent and revisable construct rather than a bedrock epistemic given.

Courts in the United States have already confronted the incipient stages of this challenge. In *United States v Batiste*,³⁴ the First Circuit addressed the admissibility of digitally altered audio and held that where tampering with evidence is demonstrated, the reliability of the altered

³²Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018) 203.

³³European Parliament, "Artificial Intelligence: Threats and Opportunities" (2020) PE 634.452, 14.

³⁴*United States v Batiste*, 868 F3d 1 (1st Cir 2017).

evidence is undermined regardless of its subsequent authentication. In *State v Leuluaiali'i*,³⁵ the Washington Court of Appeal recognised that the authenticity of digital video evidence was not self-proving and required independent corroboration. These decisions, though decided before the emergence of modern deep fake technology, provide useful precedential frameworks for addressing synthetic media in future proceedings.

The legal response to deep fake technology must ultimately be grounded in a recognition that law is not merely reactive but constitutive of the epistemic norms that govern social life. By establishing clear standards for the authentication of digital evidence, by criminalising the malicious fabrication of synthetic media, and by imposing transparency obligations upon AI systems capable of generating deceptive content, law can help to preserve the conditions under which visual truth remains a meaningful and legally cognisable concept.

In the final analysis, the regulation of deep fakes is not merely a problem of technical legal engineering. It is a question of institutional self-preservation: whether the legal system, designed for a world of imperfect but fundamentally authentic evidence, can adapt to a world in which the most persuasive categories of proof are subject to perfect fabrication. The answer depends upon the willingness of legislators, courts, and legal scholars to confront the depth of the challenge and to construct, through deliberate normative effort, a new architecture of evidentiary integrity adequate to the demands of the synthetic media age.

³⁵*State v Leuluaiali'i*, 77 P3d 1192 (Wash Ct App 2003).