

Legal Admissibility of Deepfakes in Film and Broadcast Media

TOMILOLA AYENI

Business Administration, University of Northampton

Abstract - This paper examines the legal admissibility of deepfakes within professional film and broadcast media, arguing that synthetic media technologies do not exist outside the law but instead test the limits of existing legal doctrines. While public discourse often frames deepfakes primarily as tools of deception and harm, their growing use in authorised film production, visual effects, historical reconstruction, and performance continuity raises more nuanced legal questions. The paper analyses how doctrines relating to consent, personality rights, privacy, defamation, copyright, and audience protection apply to deepfakes across different jurisdictions. Drawing on case law from the United States, the United Kingdom, and selected African jurisdictions, the paper demonstrates that legality turns less on the technology itself and more on the context of use, the presence of informed consent, contractual clarity, and audience transparency. The paper also considers broadcast regulation, highlighting how audience perception and regulatory standards shape admissibility beyond traditional intellectual property law.

Keywords: *Deepfakes, Legal admissibility, Media regulation, Personality rights*

I. INTRODUCTION

If there is one development that has marked a shift in audiovisual production since the transition from analog to digital filmmaking, it is the emergence of deepfakes. Deepfakes, broadly defined as synthetic media generated through machine learning techniques that convincingly replicate a real person's likeness, voice, or mannerisms, have generated intense public concern (Westerlund, 2019; Romero-Moreno, 2025). Much of this concern centers on deception, misinformation, and abuse.

Yet, deepfakes are not only tools of potential harm. In professional film and broadcast settings, they are increasingly used for legitimate purposes—authorized recreations of actors, visual effects, or even historical reenactments. The same technology that can mislead can also help tell stories that were once impossible. For example, studios can now digitally recreate a deceased performer in a respectful way, or alter a scene to preserve continuity without

endangering actors. These controlled, consent-based uses raise an important legal question: when and how can deepfakes be considered legally permissible under existing laws governing media, privacy, and personality rights?

At first glance, this may seem like an entirely new problem. But a closer look reveals that deepfakes mostly test existing legal frameworks rather than break them entirely. Doctrines around image rights, consent, copyright, defamation, and audience protection already exist; deepfakes just push these rules into new territory. The legal admissibility of synthetic media doesn't hinge on the technology itself; it hinges on the context of its use, whether consent has been obtained, and how viewers are informed. In other words, deepfakes are asking the law to stretch a little to fit a new kind of storytelling. These uses raise a fundamental legal question: under what conditions can deepfakes be considered legally admissible within existing media law frameworks?

One of the most significant legal issues surrounding deepfakes is the right of publicity, which protects individuals from unauthorized commercial exploitation of their identity (Cornell Law School, 2020). U.S. courts have consistently interpreted identity broadly to include name, image, likeness, and voice, as seen in cases such as *Midler v. Ford Motor Co.*, where the Ninth Circuit held that imitating a distinctive voice for commercial purposes could violate publicity rights even without using the person's name or image (*Midler v. Ford Motor Co.*, 849 F.2d 460 (9th Cir. 1988), [1988]). Deepfake technology does not alter this principle. If a synthetic depiction evokes a recognizable individual and is used commercially, liability may arise regardless of the technological process used to create the likeness (Kattwinkel, 2024). If a depiction evokes a recognizable individual and is used for commercial purposes, the method of creation does not negate liability.

This principle was clearly articulated in litigation involving AI-generated likeness applications, where plaintiffs argued that their faces were replicated without consent for profit-driven platforms. In *Young v. NeoCortex, Inc.*, involving the Reface app, plaintiffs alleged that their faces were used without consent in monetized deepfake content. Courts rejected defenses based on technological novelty and reaffirmed that the unauthorized exploitation of identity remains actionable regardless of whether the likeness was captured by a camera or generated by an algorithm *Kyland young v. neocortex, inc., [2024]*). EU GDPR provisions and Article 8 of the Charter of Fundamental Rights emphasize the protection of personal data and the right to privacy, including with respect to the protection of likenesses (European Union Agency for Fundamental Rights, 2015). For filmmakers and broadcasters, this reinforces a crucial point: deepfakes do not bypass consent requirements. Without explicit authorization, their use is legally vulnerable.

The legal framework in Africa aligns closely with these principles. The South African Protection of Personal Information Act (POPIA) (2019) enshrines data privacy and informed consent. Although it has not yet been directly applied to synthetic media, its principles would strongly counsel against the unauthorized use of personal images in broadcast or film. South Africa has already witnessed high-profile incidents that illustrate how deepfakes move with broadcast credibility, personality rights, and consumer protection. In 2024, Leanne Manas, a prominent South African broadcast anchor, was the subject of deepfake advertisements circulating on Facebook and TikTok that falsely portrayed her endorsing weight-loss products and online trading schemes (Erasmus, 2024). The content exploited her recognisable on-air persona and professional credibility, raising clear issues under personality rights, false endorsement, and consumer deception. Similar concerns arose when a deepfake video featuring South African-born entrepreneur Elon Musk circulated widely, inducing South African viewers to invest in a fraudulent financial scheme promising high returns (Kruger, 2024). Although Musk is a global public figure, the deception relied on local audience trust and media familiarity, showing exactly how deepfakes can distort audience perception even outside traditional broadcast channels. In 2025, Professor Salim Abdool Karim, director of the Centre for the AIDS Programme of

Research in South Africa, appeared in a fabricated video making anti-vaccination statements while endorsing counterfeit heart medication (Tamsin Metelerkamp, 2025). Given his public role in health communication, the deepfake posed a heightened risk of reputational harm and public misinformation. While these incidents did not arise from authorised film or broadcast productions, they show the same legal fault lines relevant to professional media: lack of consent, implied endorsement, reputational damage, and audience deception. They also show why disclosure, provenance, and authorization are central to determining the legal admissibility of deepfakes in regulated media environments.

In Kenya, the Data Protection Act of 2019 also requires explicit consent for processing personal data, including images and biometric identifiers. Broadcasters using deepfakes without consent could face claims for unlawful processing alongside privacy or personality rights violations. The Kenyan Communications Authority enforces broadcast standards emphasizing accuracy and non-deception, meaning undisclosed deepfake content in news or public programming could trigger regulatory scrutiny. More broadly, the African Charter on Human and Peoples' Rights, through its guarantees of human dignity and privacy, provides a framework for evaluating potential harms from deepfakes. Across the continent, these statutes and principles demonstrate that unauthorized or misleading synthetic content is treated seriously, highlighting why consent, disclosure, and provenance are central to determining legal admissibility in professional media.

In contrast, when consent is present, deepfakes become far less controversial from a legal standpoint. Professional film productions routinely secure extensive rights through performance contracts that allow for image manipulation, editing, and post-production alteration. In recent years, these agreements have expanded to address artificial intelligence explicitly (Oberting IV, 2024). Studios now negotiate clauses governing digital replicas, posthumous performances, and future reuse of an actor's likeness. Such contracts transform deepfakes from a legal risk into a licensed production tool. SAG-AFTRA and the UK union Equity have both issued guidelines emphasizing informed consent for AI-generated performances to ensure that contractual clarity mitigates legal risk (SAG-AFTRA, 2024).

The legal uncertainty surrounding posthumous digital performances is illustrated by the ongoing litigation over the recreation of Peter Cushing's likeness in *Star Wars: Rogue One*. Although Lucasfilm reportedly obtained authorization from Cushing's estate and compensated it for the use of his image, a subsequent lawsuit brought by film producer Kevin Francis alleges that a prior agreement with the actor prohibited any reproduction of his likeness without Francis's consent. In refusing to strike out the claim at an early stage, the English High Court acknowledged that the legal boundaries of digital likeness rights remain unsettled and fact-dependent in an evolving area of law (Brown, 2024). The case demonstrates that even where estate consent exists, competing contractual claims and historical agreements can complicate the legal admissibility of deepfake performances.

By contrast, When Paul Walker died in 2013, *Furious 7* was only partly finished. In an earlier era, the film would have been rewritten, recast, or abandoned. Instead, the studio chose to finish Walker's remaining scenes using digital reconstruction. His brothers, Caleb and Cody Walker, acted as body doubles, while visual effects teams used existing footage to recreate Walker's face and expressions. Some scenes also relied on unused material shot before his death. The result was not a fully artificial performance, but a carefully assembled one built from consented material and human stand-ins (Giardina, 2015).

What matters legally is not how advanced the technology was, but how the decision was made. The studio worked with Walker's family and estate and stayed within the boundaries of his existing contracts. There was no claim that his image had been misused or exploited, even though the film made billions worldwide. That silence is telling. It suggests that the real legal issue with digital likenesses is not whether a person is recreated on screen, but whether the use respects prior agreements and the wishes of those who control the rights after death. Walker's likeness was used to complete a story the audience already expected, not to place words in his mouth or reinvent him for a new purpose. Viewers were told what had been done, and why. That transparency, combined with consent, is likely why the film avoided controversy. As synthetic media becomes easier to produce, this case shows that the line between acceptable use and legal trouble is less about

technology and more about trust, permission, and intent.

Broadcast media introduces additional legal sensitivities due to its regulatory environment and audience expectations. Unlike fictional cinema, broadcast content often carries an implicit claim to authenticity, particularly in news, documentary, and public affairs programming. Deepfakes used in these contexts may raise concerns under misrepresentation and regulatory standards enforced by bodies such as the Federal Communications Commission in the United States, Ofcom in the United Kingdom, and the Canadian Radio-television and Telecommunications Commission (CRTC).

This tension became visible in early 2025 following backlash against a Channel 4 documentary directed and produced by Vicky Pattison, which used deepfake pornographic imagery to demonstrate how non-consensual sexual content circulates online. Although the stated intention was to raise awareness and explain takedown processes, survivor organisations and image-abuse advocates strongly criticised the programme. They argued that recreating explicit deepfake material, even for documentary purposes, risked retraumatising victims and normalising the very harm the programme sought to expose. The controversy highlighted a central issue in broadcast deepfake use: lawful intent does not automatically neutralise audience harm or ethical failure (Morris, 2025).

From a legal perspective, the Channel 4 case illustrates how deepfakes intersect with broadcast regulation rather than traditional copyright or publicity doctrines alone. UK broadcast standards place heavy emphasis on audience protection, proportionality, and contextual clarity. Even where consent exists or no specific individual is legally harmed, regulators may still question whether the use of realistic synthetic imagery misleads viewers or causes unnecessary distress. Survivor groups pointed out that they had advised producers against using such footage and that this guidance was ignored, reinforcing how disclosure and editorial judgment matter as much as legality. In broadcast environments, admissibility is shaped not only by whether content is lawful, but by how it is perceived, understood, and emotionally processed by viewers. While no definitive court ruling emerged from the incident, regulatory discussions emphasized the

importance of disclosure and contextual clarity. This aligns with broader legal principles holding that audience perception, rather than producer intent, often determines liability in broadcast regulation.

Defamation law further constrains deepfake use when depictions suggest false statements or actions attributed to real individuals. Even in fictional narratives, if a deepfake portrayal implies damaging conduct that audiences could reasonably believe to be true, liability may arise. This is particularly relevant in docudramas and hybrid formats that blur the line between fiction and reality. Courts in the U.S., including in *Hustler Magazine v. Falwell* (1988), have emphasized context in determining whether reputational harm occurs.

The interaction between deepfakes and copyright law adds another layer of complexity. While a person's likeness itself is not subject to copyright protection, the underlying materials used to generate deepfakes often are. Training data may include copyrighted films, television episodes, or sound recordings. If these materials are used without authorization, deepfake outputs may constitute infringing derivative works under statutes such as Section 106 of the U.S. Copyright Act or the EU DSM Directive (Cornell Law School, n.d.). Conversely, when training datasets rely on licensed content or original recordings created for the production, copyright concerns diminish significantly.

Consumer protection and false endorsement laws further shape the boundaries of admissibility. Deepfakes that imply endorsement, sponsorship, or participation by individuals who did not consent may violate unfair competition statutes. This risk is particularly acute in advertising and promotional content, where audience assumptions about authenticity are stronger. Courts have repeatedly emphasized that even non-explicit suggestions of endorsement can be actionable if they exploit consumer trust.

By contrast, parody and satire occupy a more protected legal space. Deepfake content used in clearly satirical contexts benefits from free expression protections, provided it does not cross into commercial exploitation or deceptive endorsement. Satirical productions that exaggerate, distort, or openly mock public figures are less likely to be construed as factual claims. However, this protection

is highly context-dependent and does not immunize all uses.

Recent legislative developments have begun to address the most harmful applications of deepfakes, particularly non-consensual intimate imagery and election interference. While these statutes are not aimed at professional film and broadcast production, they establish clear prohibitions that indirectly shape industry practices. Any deepfake that depicts a real person in an intimate or degrading context without consent is increasingly subject to criminal and civil liability, regardless of artistic justification. U.S. laws such as the Take It Down Act (Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act), along with draft regulations in China under the Cybersecurity Law, exemplify global trends toward targeted restrictions rather than blanket bans (Congressional Research Service, 2025; China Briefing, 2025).

From an evidentiary perspective, deepfakes also raise questions about admissibility in legal proceedings and regulatory review. Courts evaluating disputes involving deepfakes often focus on provenance, disclosure, and intent. Documentation demonstrating consent, licensing, and production context can be decisive in determining legality. This has encouraged studios and broadcasters to adopt internal governance practices, including audit trails and ethical review processes for synthetic media use.

Taken together, these legal developments indicate that deepfakes are neither categorically banned nor unregulated in film and broadcast media. Instead, they are governed by an interlocking set of doctrines that prioritize consent, transparency, and accountability. The law treats deepfakes as a method of representation rather than a fundamentally new category of speech. This approach mirrors how earlier technologies such as digital compositing and motion capture were absorbed into existing legal frameworks.

The legal admissibility of deepfakes therefore depends not on technological sophistication but on compliance with established principles. When used with informed consent, contractual clarity, lawful sourcing, and audience transparency, deepfakes function as legitimate creative tools. When used deceptively or exploitatively, they trigger the same

liabilities that have long governed media production. This continuity suggests that the law is less unprepared for deepfakes than popular discourse often assumes.

As film and broadcast industries continue to experiment with synthetic media, legal norms will likely evolve incrementally rather than through radical reform. Courts and regulators appear inclined to refine disclosure standards and consent requirements rather than prohibit deepfake use outright. For creators, the challenge lies not in avoiding deepfakes altogether but in integrating them responsibly within the legal and ethical boundaries that already shape media practice.

REFERENCES

- [1] African Commission on Human and Peoples' Rights (2025). *PART I: RIGHTS AND DUTIES (Articles 1-26)*. [online] African Commission on Human and Peoples' Rights. Available at: <https://achpr.au.int/en/node/641>.
- [2] Brown, D. (2024). *Peter Cushing's Star Wars resurrection at centre of legal battle*. [online] *The Times*. Available at: <https://www.thetimes.com/article/peter-cushings-star-wars-resurrection-at-centre-of-legal-battle-vsp8ssjg2>.
- [3] China Briefing (2025). *China Cybersecurity Law Amendment in Effect January 1, 2026*. [online] China Briefing News. Available at: <https://www.china-briefing.com/news/china-cybersecurity-law-amendment/>.
- [4] Congressional Research Service (2025). *The TAKE IT DOWN Act: A Federal Law Prohibiting the Nonconsensual Publication of Intimate Images*. [online] Congress.gov. Available at: <https://www.congress.gov/crs-product/LSB11314>.
- [5] Cornell Law School (n.d.). *17 U.S. Code § 106 - Exclusive rights in copyrighted works*. [online] LII / Legal Information Institute. Available at: <https://www.law.cornell.edu/uscode/text/17/106>.
- [6] Cornell Law School (2020). *Publicity*. [online] LII / Legal Information Institute. Available at: <https://www.law.cornell.edu/wex/publicity>.
- [7] Erasmus, D. (2024). *Leanne Manas speaks out about battling deepfake scams and identity theft*. [online] *The Mail & Guardian*. Available at: <https://mg.co.za/news/2024-07-21-leanne-manas-speaks-out-about-battling-deepfake-scams-and-identity-theft/>.
- [8] European Union Agency for Fundamental Rights (2015). *EU Charter of Fundamental Rights: Article 8 - Protection of personal data*. [online] European Union Agency for Fundamental Rights. Available at: <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data>.
- [9] Giardina, C. (2015). *How 'Furious 7' Brought the Late Paul Walker Back to Life*. [online] *The Hollywood Reporter*. Available at: <https://www.hollywoodreporter.com/movies/movie-news/how-furious-7-brought-late-845763/>.
- [10] *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46 [1988] 86-1278 (U.S. Supreme Court) Available at: <https://supreme.justia.com/cases/federal/us/485/46/>.
- [11] Kattwinkel, L.J. (2024). *Legalities 7: Issues Regarding the Use of Someone's Likeness*. [online] Owen, Wickersham & Erickson, P.C. Available at: <https://www.owe.com/resources/legalities/7-issues-regarding-use-someones-likeness/>.
- [12] Kenya Law The National Council of Law Reporting (2022). *Data Protection Act*. [online] Kenyalaw.org. Available at: <https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31>.
- [13] Kruger, C. (2024). *Run on numbers: From Musk to Manas: South Africa's battle against deepfake fraud*. [online] *The Star*. Available at: <https://thestar.co.za/personal-finance/financial-planning/2024-10-26-run-on-numbers-from-musk-to-manas-south-africas-battle-against-deepfake-fraud/>.
- [14] *KYLAND YOUNG V. NEOCORTEXT, INC.* [2024] No. 23-55772 (9th Cir. 2024) (U.S. Courts of Appeals) Available at: <https://law.justia.com/cases/federal/appellate-courts/ca9/23-55772/23-55772-2024-12-05.html>.
- [15] *Midler v. Ford Motor Co.*, 849 F.2d 460 (9th Cir. 1988) [1988] (US Court of Appeals for the Ninth Circuit) Available at: <https://law.justia.com/cases/federal/appellate-courts/F2/849/460/37485/>.
- [16] Morris, S. (2025). *What is a deepfake? Channel 4 and Vicky Pattison's controversy*. [online] *The Standard*. Available at: <https://www.standard.co.uk/news/uk/deepfake->

channel-4-vicky-pattison-backlash-documentary-b1011065.html.

- [17] Oberting IV, V.A. (2024). Generative Artificial Intelligence and Copyright in the Film and Media Industry. *Washington and Lee Law Review Online*, 82(2), pp.124–171.
- [18] Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. *Computer Law & Security Review*, 58(106162), pp.106162–106162. doi: <https://doi.org/10.1016/j.clsr.2025.106162>.
- [19] SAG-AFTRA (2024). *Artificial Intelligence | SAG-AFTRA*. [online] [Sagaftra.org](https://www.sagaftra.org/contracts-industry-resources/member-resources/artificial-intelligence). Available at: <https://www.sagaftra.org/contracts-industry-resources/member-resources/artificial-intelligence>.
- [20] South African Protection of Personal Information Act (POPIA) (2019). *Protection of Personal Information ACT*. [online] POPIA. Available at: <https://popia.co.za/act/>.
- [21] Tamsin Metelerkamp (2025). *Deepfake of renowned SA physician used to promote bogus heart medicine*. [online] Daily Maverick. Available at: <https://www.dailymaverick.co.za/article/2025-07-01-deepfake-ai-video-of-renowned-prof-salim-abdool-karim-used-to-promote-bogus-heart-medicine/>
- [22] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, [online] 9(11), pp.39–52. Available at: <https://timreview.ca/article/1282>.