



PERSONA FOR SALE: AI DIGITAL REPLICAS AND THE COMMERCIAL APPROPRIATION OF IDENTITY IN INDIA

Ms. Tanya Sharma & Dr. Monica Yadav¹

Received: 20/07/2026

Accepted: 01/09/2026

Published: 13/10/2026

Abstract

Generative AI has made it possible to manufacture a person's face, voice and manner, and to attach that replica to any product without the person ever being involved. The trust an audience places in a familiar face can now be copied at almost no cost and spent on someone else's product. Indian law protects parts of that asset through personality rights, trademark and passing off, consumer protection, data protection and the intermediary rules. This Article argues that these regimes remain fragmented because each depends on a condition that AI-generated replicas can avoid—consumer confusion, a real endorser, a non-public dataset, or a platform with actual knowledge. Drawing on the United States and the European Union, it proposes a statutory framework for commercial digital replicas that defines what is protected, requires consent and regulates licensing, allocates responsibility between creators, advertisers, AI developers and platforms, provides a limited post-mortem right, and protects parody, news, criticism and art more clearly than the present case-by-case injunctions do.

Keywords: AI-generated digital replicas; personality rights; right of publicity; false endorsement; consumer protection; India

I. INTRODUCTION

The celebrity has always lived at an awkward meeting point of image, identity and commerce. A film star's face sells jewellery, a cricketer's name sells insurance, and a singer's voice sells a mobile network. What is different now is the extent to which that image can be manufactured, replicated and circulated without the awareness or consent of the person it claims to stand for. Generative artificial intelligence (AI) has made identity exploitation cheap and scalable.

¹Tanya Sharma Research Scholar, IILM Law School, IILM University Gurgaon and Teaching Associate, Symbiosis Law School, Noida. Symbiosis International (Deemed University), Pune India (tanya.sharma@symlaw.edu.in; ORCID 0009-0003-1914-3327). Monica Yadav, Professor at IILM Law School, IILM University, Gurugram, India (monica.yadav@iilm.edu; ORCID 0000-0002-8600-404X).

In India, the commercial uses of this capability arrived quickly. In April 2024, the National Stock Exchange warned investors that videos showing its chief executive recommending stocks were deepfakes, and the Bombay Stock Exchange issued a similar warning soon after.² In July 2024, the Bombay High Court restrained platforms offering AI tools that reproduced the voice of the playback singer Arijit Singh.³ Over the same period, the Delhi High Court issued a run of orders protecting the names, images, voices and mannerisms of actors and other public figures, many of them aimed at AI-generated content.⁴

These cases are usually discussed as privacy or dignity problems, and they are both. But they are also commercial problems, and the commercial side is where the law is least settled. A deepfake endorsement takes the most valuable thing a celebrity owns—the trust an audience places in their recommendation—and spends it on someone else’s product. The celebrity loses the licence fee and perhaps future endorsements; the consumer who relied on the familiar face loses money; and the market for genuine endorsements is flooded with fakes. The harm is individual, but it is also systemic.⁵

Unauthorised use of a celebrity’s image is not new. Why, then, does AI need separate attention? There are five reasons.

First, cost. An AI replica can be built from material that is already public and reused indefinitely. Second, generation rather than copying. When a jeweller in *Titan Industries* copied an advertisement featuring Amitabh and Jaya Bachchan, the image was real; only its use was unauthorised.⁶ A generative system produces new statements, so that the celebrity appears to endorse a product they have never seen. Third, persistence: AI avatars and chatbots modelled on real people can interact with audiences continuously. Fourth, volume and anonymity: a single

² *Beware of Deepfake of CEO Recommending Stocks, Says National Stock Exchange*, BUS. STANDARD (Apr. 10, 2024), https://www.business-standard.com/markets/news/beware-of-deepfake-of-ceo-recommending-stocks-says-national-stock-exchange-124041000420_1.html; *Will File Police Complaint to Stop Spread of Deepfake Videos of CEO: BSE*, BUS. STANDARD (Apr. 22, 2024), https://www.business-standard.com/markets/news/will-file-police-complaint-to-stop-spread-of-deepfake-videos-of-ceo-bse-124042201166_1.html.

³ *Arijit Singh v. Codible Ventures LLP*, Com. IPR Suit (L) No. 23443 of 2024 (Bom. HC July 26, 2024) (India) (ad interim order).

⁴ *See, e.g., Amitabh Bachchan v. Rajat Nagi*, CS (COMM) 819/2022, 2022 SCC OnLine Del 4110 (Del. HC Nov. 25, 2022) (India) (ex parte ad interim order); *Anil Kapoor v. Simply Life India*, CS (COMM) 652/2023, 2023 SCC OnLine Del 6914 (Del. HC Sept. 20, 2023) (India) (ex parte ad interim order); *Aishwarya Rai Bachchan v. Aishwaryaworld.com* (Del. HC Sept. 2025) (India) (ex parte ad interim order). These orders are discussed in Part IV.A.

⁵ *Cf. Irene Khan* (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Disinformation and Freedom of Opinion and Expression*, ¶ 52, U.N. Doc. A/HRC/47/25 (Apr. 13, 2021).

⁶ *Titan Indus. Ltd. v. Ramkumar Jewellers*, (2012) 50 PTC 486 (Del. HC) (India).



campaign can produce thousands of variants, distributed by anonymous or offshore actors, faster than any takedown process can follow. Fifth, and most often missed, the same technology creates a legitimate market in licensed replicas. The law therefore has to govern a market, not only suppress a wrong.

Indian law has no statute on personality or publicity rights. Instead, courts have built personality rights from privacy under Article 21 and the tort of passing off, while the Trade Marks Act, 1999, the Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023 and the intermediary rules under the Information Technology Act, 2000 (amended in 2026 to address synthetic content) each protect a part of the asset.

The difficulty is that each regime depends on a condition that AI-generated replicas can avoid. Trademark infringement and passing off turn on consumer confusion, but an AI avatar acting as a brand's face may make no endorsement claim at all. The endorsement rules assume a real endorser who chose to speak; a deepfake has none. The data-protection statute excludes data made public by the person it concerns. And platform liability depends on actual knowledge, which in India ordinarily means a court order. The same deepfake advertisement may therefore be a passing-off claim, a misleading advertisement, a data-protection question and a takedown request at once, without giving the person whose identity was taken a clear right, a clear defendant or an adequate remedy.

Other legal systems offer no ready-made answer. The United States has mature law on commercial appropriation of identity, and several states now have digital-replica statutes, but protection varies by state and the federal bills have not been enacted.⁷ The European Union has an ambitious regime of data protection, AI transparency and platform due diligence, but no harmonised right against commercial appropriation; labelling a deepfake as artificial does not make it consensual.⁸

This Article argues that India needs a statutory framework for commercial AI-generated digital replicas, and it tries to say what that framework should contain. It makes three contributions. First, it reads the Indian personality-rights decisions as commercial-law decisions and shows that the courts are divided on precisely the point that AI exploits: whether liability requires proof of confusion. Second, it identifies a structural gap in consumer law, which treats the endorser as a regulated party but has no category for a person whose identity is used as an endorsement without consent. Third, it proposes a framework for what should be protected, whom the law should regulate, when liability should arise, and how these rights should be balanced against free

⁷ See *infra* Part VI.A.

⁸ See *infra* Part VI.B.



expression. Many of the Indian decisions discussed are interim orders; they show where the courts are heading, but they are not settled law.

Part II explains why identity has become a commercial asset and what AI changes about it. Part III sets out the harms that commercial replicas cause. Part IV examines the Indian framework, and Part V asks who should be responsible along the chain that produces and distributes a replica. Part VI draws comparative lessons from the United States and the European Union. Part VII makes the case for legislation, Part VIII sets out the proposed framework, and Part IX concludes.

II. IDENTITY AS A COMMERCIAL ASSET IN THE AGE OF AI

A. From Private Person to Commercial Persona

Personality rights protect the qualities that make a person recognisable: their name, appearance, voice, image and the broader public persona built around them. For celebrities and public figures these attributes are also a commercially valuable asset. The law long framed these interests mainly as protection against intrusion into private life. The question now is less often whether a person can keep their image out of public view, and more often whether they can control how their identity is presented, replicated and monetised.

The commercial value of a persona comes from what an endorsement does. Marketing scholarship describes endorsement as a transfer of meaning: the qualities an audience associates with the celebrity are carried over to the product, and from the product to the consumer.⁹ That recognition took years of work to build. Unauthorised use is therefore a form of unjust enrichment: the wrongdoer draws value out of the celebrity's identity without doing the work that created it, and without paying for it.¹⁰

Indian courts have accepted this commercial character of identity. The Delhi High Court in *Anil Kapoor* treated the actor's endorsement work as a significant source of livelihood that unauthorised uses could destroy.¹¹ *Titan Industries* was itself a dispute about an endorsement campaign: the defendant reproduced, on its own hoardings, the campaign the Bachchans had done

⁹ Grant McCracken, *Who Is the Celebrity Endorser? Cultural Foundations of the Endorsement Process*, 16 J. CONSUMER RSCH. 310 (1989).

¹⁰ See Stacey L. Dogan & Mark A. Lemley, *What the Right of Publicity Can Learn from Trademark Law*, 58 STAN. L. REV. 1161 (2006) (examining the unjust-enrichment and other justifications for the right of publicity).

¹¹ Anil Kapoor, 2023 SCC OnLine Del 6914; see also *Delhi HC Protects Aishwarya Rai Personality Rights*, SUPREMETODAY (Sept. 9, 2025), <https://supremetoday.ai/delhi-hc-protects-aishwarya-rai-personality-rights-20260803027> (reporting reliance on *Anil Kapoor* for the proposition that endorsement rights are a major source of a celebrity's livelihood).

for the plaintiff.¹² The asset in question was not privacy in the ordinary sense. It was the market value of a famous couple's association with a brand.

B. The Layers of a Digital Identity

A digital identity has several layers: the *nominal* (name and handle), the *representational* (images, video and voice), the *behavioural* (how someone speaks and responds) and the *relational* (the brands, causes and people a person is linked with). AI content attacks the representational layer first, but the damage spreads: a deepfake puts forward statements the person never made and associations they never chose. Indian courts, in recognising the “persona” as the protectable unit, have in effect accepted that identity is layered in this way.¹³ The legislature has not.

C. What AI Changes: From Copying to Generation

What a decade ago required a film studio's visual-effects budget is now available to anyone with consumer hardware and open-source software. When the cost of producing a convincing likeness falls close to zero, so does the cost of misappropriating it.

The technologies need little description here. Face-swapping and video-synthesis models can place one person's face onto another's body or animate a still image; voice-cloning systems can reproduce a person's voice from recordings of their speech. What matters for the law is the change in the kind of misuse that is possible. Older forms of misappropriation reused something real: a photograph, a recording, an advertisement. Generative systems produce something new. A cloned voice can be made to read any script; a synthetic video can show a celebrity in a setting they never entered.

The newest form is the persistent AI avatar or chatbot modelled on a real person. Used commercially without consent, it can promote products while the person has little or no awareness of it; used for a deceased celebrity, it keeps the commercial machine running after death, raising the post-mortem question considered in Parts IV.A and VIII.H.

The same technology also has legitimate uses. Performers license their voices for dubbing and translation; athletes license their likeness for games; estates license the image of deceased artists. A framework that treats every digital replica as a wrong would shut down a market that performers themselves want to participate in. The real question is whether the replica was made and used with the person's informed consent, on terms the law will respect.

¹² Titan Indus., (2012) 50 PTC 486.

¹³ See, e.g., Anil Kapoor, 2023 SCC OnLine Del 6914 (protecting name, image, voice, likeness, mannerisms and the catchphrase “jhakaas”); Shivaji Rao Gaikwad v. Varsha Prods., 2015 SCC OnLine Mad 158 (Mad. HC) (India) (Rajinikanth).



D. Trust as the Asset

One more feature connects the commercial picture to the harms in Part III. An endorsement works because the audience feels it knows the person endorsing. Communication researchers call this a “parasocial” relationship: a one-sided emotional bond that functions, for the audience, much like a genuine social connection.¹⁴ In India, where film stars and cricketers command an unusual depth of public attachment, these bonds are a cultural institution in their own right.

Parasocial trust is the economic substance of endorsement value. It is what the brand pays the celebrity for, and it is what a deepfake endorsement steals. Ryan Calo has shown how digital firms can exploit consumers’ predictable vulnerabilities at scale;¹⁵ AI-generated endorsements are a sharp version of the same problem.

The harm to the celebrity and the harm to the consumer are therefore two sides of one transaction: the replica takes the celebrity’s trust and converts it into the consumer’s loss. A framework that protects only one side will leave the other unprotected.

III. WHAT COMMERCIAL REPLICAS DO: THREE KINDS OF HARM

AI-generated replicas cause harm in three places: to the person whose identity is taken, to the consumers who are deceived, and to the market for endorsements itself. The existing Indian regimes each respond to some of these harms. None responds to all of them, and the dignitary and psychological harms fall outside the commercial frameworks entirely.

A. Harm to the Person

The most visible harm is commercial. When a celebrity’s likeness is used to promote a product without permission, the celebrity loses the fee a licence would have earned and loses control over which brands they are associated with. These are the losses that passing off and publicity claims were designed to address.

The reputational harm is often larger and lasts longer. Research on the “continued influence” of misinformation shows that people keep relying on false information even after it has been retracted.¹⁶ For a celebrity shown endorsing a fraudulent investment scheme or an illegal betting application, the association may stay with them after the video is taken down, reducing the value of their brand and closing off future endorsements.

Then there is the harm that the commercial frameworks do not measure at all: being confronted with a convincing synthetic version of oneself, making declarations one never made. When a deepfake video of the actor Rashmika Mandanna circulated in November 2023, she

¹⁴ Donald Horton & R. Richard Wohl, *Mass Communication and Para-Social Interaction: Observations on Intimacy at a Distance*, 19 PSYCHIATRY 215 (1956).

¹⁵ Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

¹⁶ Stephan Lewandowsky et al., *Misinformation and Its Correction: Continued Influence and Successful Debiasing*, 13 PSYCH. SCI. PUB. INT. 106 (2012).



described it as “extremely scary.”¹⁷ The Supreme Court’s recognition in *Puttaswamy* that privacy includes control over information about oneself captures what is lost: the person’s ability to remain the main author of how their own identity is presented.¹⁸ These harms are also gendered. Non-consensual intimate imagery falls overwhelmingly on women, which is a reason to design remedies with gender in mind.

B. Harm to Consumers

The second set of harms falls on the audience. A consumer who invests in a scheme because a trusted figure appeared to recommend it suffers a direct financial loss; the stock-exchange deepfakes mentioned in Part I were circulated precisely because investors trust those officials.¹⁹ The harm is not only financial. A consumer who believes they are hearing directly from a person they admire is being manipulated through the relationship itself, particularly where AI chatbots modelled on celebrities simulate personal engagement.

C. Harm to the Market for Endorsements

The third harm is systemic. If consumers cannot tell genuine endorsements from fabricated ones, the value of all endorsements falls. This is the commercial version of what Robert Chesney and Danielle Citron call the “liar’s dividend”: once convincing fakes are common, it becomes easier to dismiss real evidence as fabricated.²⁰ A celebrity who genuinely endorsed a product that later failed could claim the endorsement was a deepfake.

D. Why the Harms Must Be Considered Together

It would be convenient to treat these harms separately: commercial loss under intellectual property law, consumer loss under consumer law, and dignitary harm under privacy law. But the harms arise from one act and depend on one another. The deepfake endorsement damages the consumer because the celebrity is trusted, and damages the celebrity because consumers are deceived. Part IV shows that Indian law does split the harms in exactly this way, and that the split leaves gaps.

IV. THE FRAGMENTED INDIAN FRAMEWORK

India’s response to AI-generated identity appropriation draws on constitutional, tortious, intellectual property, consumer and data-protection sources, each built for a different problem. This Part asks the same question of each: which parts of the harm does it reach, and what condition must be satisfied before it applies?

¹⁷ *Rashmika Mandanna Calls for Action Against “Scary” Deepfake Video*, BBC NEWS (Nov. 7, 2023), <https://www.bbc.com/news/world-asia-india-67305557>.

¹⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

¹⁹ *See supra* note 1.

²⁰ Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019).

A. Personality Rights in the Courts

1. Two Roots

Indian personality rights have grown from two roots that the courts have never fully separated. The first is privacy. In *R. Rajagopal*, the Supreme Court held that publishing a person's life story without consent could violate their privacy.²¹ In *Puttaswamy*, Justice Kaul, concurring, said that every individual should have a right to control their own life and image as portrayed to the world, and to control the commercial use of their identity.²² That observation is now cited in almost every personality-rights order.

The second root is commercial. Here the courts drew on passing off and on the American right of publicity, and treated a celebrity's persona as something closer to property: a source of goodwill that others should not exploit without paying for it.²³ The two roots lead to different questions. A privacy claim asks whether the person consented. A passing-off claim asks whether the public was deceived. Indian courts have not settled which question governs, and commentators have criticised the resulting inconsistency.²⁴

2. Building the Right: From ICC to Rajinikanth

The commercial line begins with *ICC Development v. Arvee Enterprises*, where the Delhi High Court rejected a claim to a right of publicity in the 2003 Cricket World Cup, holding that the right could belong only to an individual, or to the indicia of an individual's personality such as name, personality traits, signature or voice.²⁵ In *DM Entertainment v. Baby Gift House*, the court restrained the sale of dolls modelled on the singer Daler Mehndi, requiring that the plaintiff be identifiable from the defendant's use and noting that parody, caricature and satire would ordinarily be protected.²⁶

Titan Industries v. Ramkumar Jewellers is the most important early decision. A jeweller had reproduced an advertising campaign that Amitabh and Jaya Bachchan had done for the plaintiff's Tanishq brand.²⁷ The court identified two elements of liability: *validity*, meaning that the plaintiff owns an enforceable right in the persona of a human being; and *identifiability*, meaning that the celebrity is recognisable from the defendant's use. It held that infringement "requires no

²¹ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).

²² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 625 (India) (Kaul, J., concurring).

²³ *See DM Ent. Pvt. Ltd. v. Baby Gift House*, CS (OS) 893/2002 (Del. HC Apr. 29, 2010) (India).

²⁴ *See The Many Faces of Personality Rights: How Courts Are Deepening the Confusion*, SPICYIP (Nov. 2025), <https://spicyip.com/2025/11/the-many-faces-of-personality-rights-how-courts-are-deepening-the-confusion.html>.

²⁵ *ICC Dev. (Int'l) Ltd. v. Arvee Enters.*, (2003) 26 PTC 245 (Del. HC) (India).

²⁶ *DM Ent.*, CS (OS) 893/2002.

²⁷ *Titan Indus. Ltd. v. Ramkumar Jewellers*, (2012) 50 PTC 486 (Del. HC) (India).

proof of falsity, confusion, or deception.”²⁸ This is the decisive point for this Article. *Titan* separated the publicity claim from passing off: a celebrity could restrain commercial use of their identity even where no consumer was misled.

The Madras High Court followed this approach in *Shivaji Rao Gaikwad v. Varsha Productions*, enjoining the release of a film titled *Main Hoon Rajinikanth* because the actor’s name was so closely identified with him that its use in the title was enough; confusion did not have to be shown.²⁹ Step by step, the courts moved from the photographic image to name, voice, manner of speaking and signature phrases, and finally to the “persona” as a single, culturally formed identity.

3. The Pull Back Towards Passing Off

Later decisions have not followed *Titan* consistently. In *Gautam Gambhir v. D.A.P. & Co.*, the Delhi High Court refused to restrain a restaurant chain using the cricketer’s name, finding no evidence of confusion or harm to reputation.³⁰ The absence of confusion, which *Titan* had said was irrelevant, was here a reason to refuse relief.

The clearest statement of the narrower view came in *Digital Collectibles v. Galactus Funware*, where platforms used cricketers’ names and images in online fantasy games. A single judge held that using celebrity information already in the public domain did not infringe the right of publicity; that, absent a statutory basis, the right should be assessed through the lens of passing off; and that it was subordinate to freedom of speech under Article 19(1)(a), including commercial speech.³¹ On this reading, the right of publicity is close to a law against false endorsement.

In *Krishna Kishore Singh v. Sarla A. Saraogi*, the father of the late actor Sushant Singh Rajput sought to restrain a film based on his son’s life. The court refused, holding that the rights of privacy, publicity and personality were not heritable and ended with the actor’s death, following the Madras High Court in *Deepa Jayakumar v. A.L. Vijay*.³² It also rejected a separate category of “celebrity rights” and gave considerable weight to the filmmakers’ freedom of expression.

²⁸ *Id.*; see also *Right of Publicity in India – An Unfinished Story*, SPICYIP (Jan. 2016), <https://spicyip.com/2016/01/right-of-publicity-in-india-an-unfinished-story.html>.

²⁹ *Shivaji Rao Gaikwad v. Varsha Prods.*, 2015 SCC OnLine Mad 158 (Mad. HC) (India).

³⁰ *Gautam Gambhir v. D.A.P. & Co.*, 2017 SCC OnLine Del 12167 (Del. HC) (India).

³¹ *Digital Collectibles Pte. Ltd. v. Galactus Funware Tech. Pvt. Ltd.*, 2023 SCC OnLine Del 2306 (Del. HC) (India); see *World of Possibilities: Single Judge Bench of Delhi High Court Allows Use of Celebrity Information Available in Public Domain*, SPICYIP (May 11, 2023), <https://spicyip.com/2023/05/world-of-possibilities-single-judge-bench-of-delhi-high-court-allows-use-of-celebrity-information-available-in-public-domain.html>.

³² *Krishna Kishore Singh v. Sarla A. Saraogi*, CS (COMM) 187/2021 (Del. HC July 11, 2023) (India); *Deepa Jayakumar v. A.L. Vijay* (Mad. HC 2021) (India).

4. The AI Cases

Against this background, the AI-era decisions extended protection rapidly, though almost entirely through interim orders. *Amitabh Bachchan v. Rajat Nagi* (2022) was not about AI, but it set the form of relief: a broad ex parte injunction protecting the actor's "personality" as a whole, against known and unknown defendants, with directions to government agencies and telecom providers to block infringing websites.³³

Anil Kapoor v. Simply Life India (2023) applied that model to AI expressly, restraining the use of the actor's name, likeness, voice and the catchphrase "jhakaas," including through AI tools, face morphing and deepfakes, for commercial purposes.³⁴ It accepted that satire, parody and genuine criticism are protected, but held that the protection ends where the use becomes commercial exploitation or tarnishes the person's image.³⁵

In *Arijit Singh v. Codible Ventures* (2024), the Bombay High Court dealt directly with voice cloning. It held, prima facie, that AI tools enabling unauthorised replication of a celebrity's voice violate personality rights, and that freedom of speech "does not grant the license to exploit a celebrity's persona for commercial gain."³⁶ The order identified three requirements: celebrity status, identifiability, and use for commercial gain.

Jaikishan Kakubhai Saraf v. Peppy Store (2024), involving the actor Jackie Shroff, showed the other side: the Delhi High Court declined to remove a meme-style video, warning that indiscriminate takedowns could stifle free expression.³⁷ In 2025, the same court issued a series of ex parte orders for public figures. In the order for Aishwarya Rai Bachchan, involving AI-generated sexualised content and chatbots, it restrained the use of her persona "in any manner," including through AI, and directed takedowns within seventy-two hours and the blocking of listed websites.³⁸

5. What the Case Law Leaves Unsettled

The courts have done a great deal with very little statutory material. But the case law leaves at least six questions open, and each matters for a commercial actor trying to know what is lawful.

³³ *Amitabh Bachchan v. Rajat Nagi*, CS (COMM) 819/2022, 2022 SCC OnLine Del 4110 (Del. HC Nov. 25, 2022) (India) (ex parte ad interim order).

³⁴ *Anil Kapoor v. Simply Life India*, CS (COMM) 652/2023, 2023 SCC OnLine Del 6914 (Del. HC Sept. 20, 2023) (India) (ex parte ad interim order).

³⁵ *Id.*

³⁶ *Arijit Singh v. Codible Ventures LLP*, Com. IPR Suit (L) No. 23443 of 2024 (Bom. HC July 26, 2024) (India) (ad interim order); see *Singh v. Codible Ventures*, COLUM. GLOB. FREEDOM OF EXPRESSION, <https://globalfreedomofexpression.columbia.edu/cases/singh-v-codible-ventures/> (last visited Oct. 8, 2026).

³⁷ *Jaikishan Kakubhai Saraf v. Peppy Store*, CS (COMM) 389/2024 (Del. HC May 15, 2024) (India).

³⁸ *Aishwarya Rai Bachchan v. Aishwaryaworld.com* (Del. HC Sept. 2025) (India) (ex parte ad interim order); see *Delhi HC Protects Aishwarya Rai Personality Rights*, *supra* note 10.

Status. Most AI-era decisions are ex parte ad interim injunctions, granted after hearing only the plaintiff, with little analysis of defences and limited value as precedent. Shwetaree Majumder has argued that they blur the difference between a right existing and its being enforceable in a particular case.³⁹

The test. *Titan*, *Rajinikanth* and the AI orders suggest that identifiability and unauthorised commercial use are enough; *Gambhir* and *Digital Collectibles* suggest that something like confusion is needed. A replica clearly labelled as AI-generated would succeed under the first line and might fail under the second.

Who is protected. *Arijit Singh* treats celebrity status as a threshold; *Krishna Kishore Singh* rejected distinct celebrity rights. If personality rights rest on Article 21, it is hard to see why an ordinary person whose face is used in a fraudulent advertisement should have less protection than a film star.

Death. Personality rights are not heritable. Yet AI makes posthumous commercial use of a famous person's identity both easy and valuable. The estate of a deceased singer may have no claim against a company that releases new songs in the singer's cloned voice.

Remedies. The case law consists almost entirely of injunctions and blocking orders. Damages are rarely assessed, and there is no method for valuing the unauthorised use of a persona.

Free expression. The orders say that parody, satire, criticism and news are protected, but rarely apply the distinction to particular content, and orders protecting a "persona" in any manner risk giving celebrities control over legitimate commentary.⁴⁰

B. Trademark and Passing Off

1. Trademark Infringement

The Trade Marks Act, 1999 offers partial grounds against the commercial exploitation of identity. A "mark" includes a name and a signature, and Indian celebrities do register their names.⁴¹ Section 29 bars use of an identical or similar mark in the course of trade where confusion is likely, and section 29(4) dispenses with confusion for marks with a reputation in India where the use takes unfair advantage of, or is detrimental to, the mark's distinctive character or repute.⁴²

The limits for AI replicas are obvious. These provisions protect *registered marks*, and most of what an AI replica copies—a face, a voice, a manner of speaking—is not registered and often

³⁹ Shwetaree Majumder, *Fame, Commerce and Free Speech: Rethinking Personality Rights in India*, BAR & BENCH, <https://www.barandbench.com/columns/fame-commerce-and-free-speech-rethinking-personality-rights-in-india>.

⁴⁰ *Id.*; see also *The Many Faces of Personality Rights*, *supra* note 23.

⁴¹ The Trade Marks Act, 1999, § 2(1)(m), No. 47, Acts of Parliament, 1999 (India).

⁴² *Id.* § 29(1)–(4).

could not be. They apply to use as a mark, which a deepfake video may not involve. And outside section 29(4), they turn on confusion.

2. *Passing Off*

Where the persona is not registered, the claim is ordinarily passing off, which the Act preserves.⁴³ It requires goodwill, a misrepresentation likely to deceive the public, and damage.⁴⁴ A false suggestion of endorsement can be a misrepresentation. In *Irvine v. Talksport*, a radio station altered a photograph of a Formula One driver so that he appeared to be holding a radio bearing its name; that case is, in effect, an early deepfake.⁴⁵ But passing off is not an image right. In *Fenty v. Arcadia*, selling T-shirts bearing Rihanna's photograph was passing off only because buyers were likely to think she had endorsed them; English law has no general right to control the use of one's image.⁴⁶

Passing off works well when a deepfake clearly communicates that the celebrity recommends a product, and less well for an AI avatar that acts as a brand's face without any endorsement statement. A newer problem has also arisen. The 2026 amendments to the intermediary rules require synthetic content to be labelled.⁴⁷ A label saying that an advertisement uses an AI-generated likeness of a named actor may remove the misrepresentation on which passing off depends, while leaving the appropriation untouched. The more honestly an advertiser labels an unauthorised replica, the weaker the passing-off claim becomes.

3. *Copyright and Performers' Rights*

Copyright offers less than might be expected. The Copyright Act gives performers rights in their performances, including moral rights, and the plaintiff in *Arijit Singh* relied on them.⁴⁸ But these rights protect a recorded performance, not the voice as such, and a cloned voice singing a new song reproduces no particular performance. Training a model on existing recordings may involve copying sound recordings, but that copyright ordinarily belongs to the producer, not the singer. Copyright may therefore give the label a claim that the singer does not have.

4. *What Trademark Law Cannot Do*

Stacey Dogan and Mark Lemley have argued that the right of publicity should learn from trademark law's focus on consumer confusion, to keep it from becoming an open-ended property right.⁴⁹ That argument has force, and Part VIII adopts some of its discipline. But for AI replicas, a

⁴³ *Id.* § 27(2).

⁴⁴ *Reckitt & Colman Prods. Ltd. v. Borden Inc.* [1990] 1 WLR 491 (HL) 499 (appeal taken from Eng.).

⁴⁵ *Irvine v. Talksport Ltd.* [2002] EWHC (Ch) 367 (Eng.).

⁴⁶ *Fenty v. Arcadia Grp. Brands Ltd.* [2015] EWCA (Civ) 3 (Eng.).

⁴⁷ *See supra* note 10.

⁴⁸ The Copyright Act, 1957, §§ 38, 38A, 38B, No. 14, Acts of Parliament, 1957 (India).

⁴⁹ Dogan & Lemley, *supra* note 9.

regime that protects only against confusion leaves the core harm unaddressed. What India needs is a right that protects the commercial value of identity without proof of confusion, while containing its own limits for expression.

C. Consumer Protection and False Endorsement

The Consumer Protection Act, 2019 is the most directly applicable statute for AI-generated false endorsements, and it is also where the structural gap is clearest.

1. *What the Act Provides*

The Act defines an “endorsement” broadly enough to cover an AI replica: any message or depiction of the name, likeness or other identifiable characteristics of an individual that makes consumers believe it reflects that individual’s opinion or experience.⁵⁰ A “misleading advertisement” includes one that conveys a representation amounting to an unfair trade practice,⁵¹ which includes falsely representing that goods have a sponsorship or approval they do not have.⁵²

The Central Consumer Protection Authority (CCPA) can direct that misleading advertisements be discontinued, penalise a manufacturer or endorser up to ten lakh rupees (fifty lakh for subsequent contraventions), and bar an endorser from endorsing for up to one year (three for a repeat).⁵³ An endorser who exercised due diligence is not liable.⁵⁴ The CCPA’s 2022 Guidelines add that an endorsement must reflect the genuine, reasonably current opinion of the person making it.⁵⁵ The Advertising Standards Council of India’s guidelines require virtual influencers to disclose that they are not human,⁵⁶ but say nothing about whether a real person whose likeness was used consented.

On these terms, an AI-generated endorsement that a celebrity never authorised is plainly a misleading advertisement, and the CCPA can act against the advertiser. So far, the framework works.

2. *The Endorser-Shaped Hole*

The gap lies in who the Act protects. It treats the endorser as a *regulated party*: someone who can be penalised, barred from endorsing, or required to show due diligence. It has no category for a person whose identity has been used as an endorsement without consent. Read literally, the

⁵⁰ The Consumer Protection Act, 2019, § 2(18), No. 35, Acts of Parliament, 2019 (India).

⁵¹ *Id.* § 2(28).

⁵² *Id.* § 2(47).

⁵³ *Id.* §§ 10, 21(1)–(3); Ministry of Consumer Affairs, Food & Public Distribution, Notification S.O. 2421(E) (July 24, 2020) (India) (establishing the Central Consumer Protection Authority).

⁵⁴ Consumer Protection Act § 21(5).

⁵⁵ Central Consumer Protection Authority, Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, cl. 13 (June 9, 2022) (India).

⁵⁶ ADVERT. STANDARDS COUNCIL OF INDIA, Guidelines for Influencer Advertising in Digital Media (2021).

definition could make the celebrity in a deepfake the “endorser,” since it is their likeness that conveys the opinion. The due-diligence defence would protect them from a penalty, but the Act gives them no standing as the injured party, no compensation and no control over future use. The regime can punish the person it cannot protect.

This is not only a drafting curiosity. The framework sees the celebrity’s identity as a source of risk to consumers, which it is, but not as an asset that has been taken. It protects the audience side of the transaction described in Part II.D and leaves the other side unprotected.

3. Enforcement in the AI Context

Even within its own field, the framework struggles with AI. The guidelines predate generative AI and say nothing about identifying or attributing synthetic endorsements. The most harmful ones—promoting fraudulent investments, unlicensed supplements and illegal gambling—are often distributed by anonymous or offshore actors beyond the CCPA’s practical reach. And penalties and cease-and-desist directions do not compensate the celebrity.

There is a further question. If a celebrity *licenses* a digital replica, can an AI-generated endorsement made under that licence reflect the “genuine, reasonably current opinion” the guidelines require, when the celebrity may never have seen the advertisement? Part VIII.D proposes an answer.

D. Data Protection

The Digital Personal Data Protection Act, 2023 might seem the natural instrument for controlling the use of a person’s face and voice to train AI systems. As of October 2026, its substantive processing provisions have not all commenced, and its eventual reach is limited by its exclusions and structure.

The Act does not apply to personal data made publicly available by the data principal.⁵⁷ Most of a celebrity’s images, interviews and performances are made public by the celebrity or with their participation, so an AI developer training on them may fall outside the Act altogether. Material made public by someone else—a newspaper photograph, say—may remain within it, which makes protection depend on who posted the image rather than on what is done with it.⁵⁸

Nor does the Act create a special category for biometric data or a right to compensation for misuse of identity. It treats identity as information to be processed lawfully, not as a commercial asset whose value can be taken.

The criminal law fills some of the space. The IT Act punishes identity theft, cheating by personation using a computer resource, and the publication of obscene or sexually explicit

⁵⁷ The Digital Personal Data Protection Act, 2023, § 3(c)(ii), No. 22, Acts of Parliament, 2023 (India).

⁵⁸ See *Five Ways in Which the DPDP Act Could Shape the Development of AI in India*, FUTURE OF PRIVACY F. (Sept. 2024), <https://fpf.org/blog/five-ways-in-which-the-dpdp-act-could-shape-the-development-of-ai-in-india/>.

material,⁵⁹ and the Bharatiya Nyaya Sanhita, 2023 punishes cheating by personation and defamation.⁶⁰ These provisions deal with deception and obscenity, not appropriation, and give the person whose identity was used no commercial remedy.

E. What Falls Between the Regimes

A single example shows how these regimes interact. Suppose a well-known actor discovers a paid social-media advertisement in which an AI-generated version of the actor recommends an online betting application. It was produced by an unknown person using a commercial voice-cloning service and a free face-animation tool. A small caption describes it as “AI-generated.”

The actor can bring a personality-rights suit and is likely to obtain an ex parte injunction. That is the strongest remedy available, but it requires a commercial suit in a High Court and rests on a doctrine whose test is unsettled. A passing-off claim is weakened by the caption. A trademark claim needs a registered name used as a mark. Copyright offers nothing. The CCPA can act against the advertiser, if it can be found, but the actor is not a complainant whom the Act compensates and is, on a literal reading, the “endorser.” The data-protection statute may not reach training on interviews the actor made public. And the platform must label the video and remove it once it receives a court order, but was never required to check whether the actor consented before selling the advertising slot.

No regime asked the question that matters most: did this person agree to be used to sell this product? The table below summarises the analysis.

Regime	What it protects	Condition AI replicas can avoid	Remedy for the person depicted
Personality rights (courts)	Persona against unauthorised commercial use	Unsettled test; celebrity threshold; ends at death	Mainly interim injunctions
Trademark (s. 29)	Registered marks	Registration; use as a mark; confusion	Injunction, damages (registered marks only)
Passing off	Goodwill against misrepresentation	Confusion (may be removed by labelling)	Injunction, damages or account of profits
Copyright performers' rights	Works, recordings, performances	Replica generates a new performance; label owns recordings	Limited

⁵⁹ Information Technology Act §§ 66C, 66D, 66E, 67, 67A.

⁶⁰ The Bharatiya Nyaya Sanhita, 2023, §§ 319, 356, No. 45, Acts of Parliament, 2023 (India).

Regime	What it protects	Condition AI replicas can avoid	Remedy for the person depicted
Consumer protection	Consumers against misleading ads	Treats depicted person as endorser, not victim	None for the depicted person
Data protection	Personal data processing	Data made public by the person; no special biometric category	None (penalties only)
Criminal law	Fraud, obscenity, personation	Requires criminal elements; offshore actors	None commercial

Read across the rows, the pattern is plain. The person depicted has a strong claim only where a court will grant an injunction on an unsettled personality-rights theory. Every other regime either protects someone else (the consumer, the trademark owner, the record label) or depends on a condition that the replica can avoid.

V. WHO IS RESPONSIBLE? LIABILITY ALONG THE REPLICA SUPPLY CHAIN

The rules on deceptive advertising assume that false claims have human authors who can be found. A single deepfake endorsement may instead involve a model developer, a voice-cloning application, the individual who generated the video, the advertiser who paid for it, and the platform that distributed it and earned revenue from the placement. Indian law has no settled answer to how responsibility should be shared among them.

A. Creators and Advertisers

The person who generates a replica and the advertiser who uses it are the obvious primary wrongdoers. The problem is practical rather than doctrinal: the creators of fraudulent endorsements are frequently anonymous, offshore or both, and in many fraud cases the “advertiser” is the fraudster.

Indian courts have adapted their remedies. Personality-rights suits are routinely brought against “John Doe” defendants, so that an injunction can bind persons not yet identified,⁶¹ and courts have directed platforms and domain registrars to disclose subscriber information.⁶² These are effective tools. But they are available only after a suit has been filed in a High Court, and they place the cost of finding the wrongdoer on the person whose identity was taken.

The present law also treats one category of advertiser too lightly: the legitimate business that accepts AI-generated content featuring a recognisable person without checking whether

⁶¹ See, e.g., Amitabh Bachchan v. Rajat Nagi, CS (COMM) 819/2022, 2022 SCC OnLine Del 4110 (Del. HC Nov. 25, 2022) (India).

⁶² See, e.g., Arijit Singh v. Codible Ventures LLP, Com. IPR Suit (L) No. 23443 of 2024 (Bom. HC July 26, 2024) (India); Aishwarya Rai Bachchan v. Aishwaryaworld.com (Del. HC Sept. 2025) (India).

consent was given. The consumer-protection rules require advertisers to substantiate their claims, but not to confirm that a person depicted agreed to appear. That duty should fall on the advertiser, the party best placed to perform it.

B. AI Developers and Tool Providers

A harder question is whether the companies that build AI systems should bear responsibility for what users make with them. A distinction is useful. A general-purpose image or voice model can produce a replica of anyone, but is not designed for that purpose. A dedicated tool that offers to reproduce a named celebrity's voice is designed for exactly that purpose.

The 2026 amendments to the intermediary rules strengthen labelling and provenance obligations for synthetic content, but they do not create a right to control the commercial use of a person's identity. And whether training a model on a person's images or recordings requires their consent is not addressed by any Indian statute: as Part IV.D explained, the data-protection statute does not apply to data the person has made public, and copyright in recordings belongs to producers rather than performers.

C. Platforms

1. Section 79 and Actual Knowledge

Platforms are protected by the safe harbour in section 79 of the IT Act, which applies where an intermediary does not initiate the transmission or select or modify the information, observes due diligence, and expeditiously removes unlawful material on receiving actual knowledge.⁶³ In *Shreya Singhal v. Union of India*, the Supreme Court read "actual knowledge" to mean a court order or government notification, not a private complaint, because private notices would force intermediaries to judge the lawfulness of millions of requests.⁶⁴

That reasoning remains sound for most content. But it means that, for a celebrity whose deepfake is circulating, the ordinary route to removal is a court order. Indian courts have held that a platform taking an active role in the transaction may lose the protection of section 79.⁶⁵ Paid advertising is a strong candidate for this reasoning: a platform that sells, targets and earns revenue from a deepfake endorsement is not a passive conduit. The point has not yet been tested in the AI context.

⁶³ Information Technology Act § 79.

⁶⁴ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

⁶⁵ See *Christian Louboutin SAS v. Nakul Bajaj*, 2018 SCC OnLine Del 12215 (Del. HC) (India); cf. *MySpace Inc. v. Super Cassettes Indus. Ltd.*, 2016 SCC OnLine Del 6382 (Del. HC) (India) (division bench).



2. *The Intermediary Rules*

The 2021 intermediary rules require platforms to tell users not to host content that impersonates another person,⁶⁶ and to remove, within twenty-four hours of a complaint by the affected individual, content in the nature of impersonation, including artificially morphed images.⁶⁷ This is one of the few routes to removal without going to court, and it already covers many deepfakes.

The 2026 amendments go further. They require permitted synthetic content to be prominently labelled and to carry permanent metadata or provenance markers, and reduce the time for acting on government and court orders to three hours. Significant social media intermediaries must require users to declare whether content is synthetic, verify those declarations, and label confirmed synthetic content; one that knowingly permits non-compliant synthetic content fails its due-diligence obligations.⁶⁸

These are significant changes. But they are transparency and speed measures. They do not decide whether a particular use of a person's identity is unlawful, they do not require consent, and they give the person depicted no compensation. As Part IV.B noted, a labelling duty may even weaken a passing-off claim. The rules regulate the *form* of synthetic content; *appropriation* is left to the courts.

D. The Gap in Allocation

Responsibility in India is therefore allocated by courts, one order at a time, through injunctions against unknown defendants, takedown directions, blocking orders and disclosure orders. This works well for a plaintiff who can afford a commercial suit in a High Court. It works much less well for a regional actor, a social-media creator or an ordinary person whose face is used in a fraudulent advertisement.

It also leaves the *ex ante* allocation of responsibility undefined: no one is clearly required to check consent before a replica is generated, advertised or distributed. Following Jack Balkin's argument that firms holding power over people's data should owe duties of care,⁶⁹ the platforms and advertisers who profit from a person's identity should bear a duty to verify consent, tied to their protection from liability.

⁶⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(b) (India).

⁶⁷ *Id.* r. 3(2)(b).

⁶⁸ See India Introduces Mandatory Labelling for AI and 3-Hour Takedown for Illegal Content, *supra* note 10.

⁶⁹ Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020).



VI. COMPARATIVE LESSONS: THE UNITED STATES AND THE EUROPEAN UNION

Neither the United States nor the European Union has solved the problem of commercial AI replicas. Each, however, has developed parts of the solution that India lacks, and each has made choices that India should avoid.

A. The United States

1. The Right of Publicity and False Endorsement

The United States has the most developed law on the commercial appropriation of identity. The “right of publicity” dates from *Haelan Laboratories v. Topps Chewing Gum*,⁷⁰ and the Supreme Court accepted in *Zacchini v. Scripps-Howard Broadcasting* that a state could protect a performer’s interest in the commercial value of his act.⁷¹ The right is now recognised in a majority of states, though its scope, duration and remedies vary considerably.⁷² California protects living persons against the knowing use of their name, voice, signature, photograph or likeness for advertising without consent, and protects deceased personalities for seventy years after death.⁷³ New York has, since 2020, specifically protected against digital replicas of deceased performers.⁷⁴

The federal Lanham Act adds a claim for false endorsement where a use is likely to cause confusion as to sponsorship or approval.⁷⁵ The voice cases show how far these doctrines had gone before AI. In *Midler v. Ford Motor Co.*, the Ninth Circuit held that deliberately imitating a well-known singer’s voice to sell a product appropriates her identity.⁷⁶ *White v. Samsung Electronics* allowed a claim based on a robot posed to evoke a television personality, which is close to the modern AI avatar.⁷⁷ Judge Kozinski’s dissent from the denial of rehearing remains the classic warning that publicity rights can grow broad enough to restrict legitimate expression,⁷⁸ a tension Indian courts face today.

In the first AI voice-cloning case, *Lehrman v. Lovo, Inc.*, voice actors alleged that an AI company had cloned and sold their voices. The court reportedly dismissed most of the federal trademark and copyright claims while allowing claims under New York’s publicity statute to

⁷⁰ *Haelan Lab’ys, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866, 868 (2d Cir. 1953).

⁷¹ *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977).

⁷² See generally J. THOMAS MCCARTHY & ROGER E. SCHECHTER, *THE RIGHTS OF PUBLICITY AND PRIVACY* (2d ed.); *RESTATEMENT (THIRD) OF UNFAIR COMPETITION* § 46 (AM. L. INST. 1995).

⁷³ CAL. CIV. CODE §§ 3344, 3344.1 (West).

⁷⁴ N.Y. CIV. RIGHTS LAW §§ 50, 51, 50-f (McKinney).

⁷⁵ 15 U.S.C. § 1125(a)(1)(A).

⁷⁶ *Midler v. Ford Motor Co.*, 849 F.2d 460, 463 (9th Cir. 1988).

⁷⁷ *White v. Samsung Elecs. Am., Inc.*, 971 F.2d 1395 (9th Cir. 1992).

⁷⁸ *White v. Samsung Elecs. Am., Inc.*, 989 F.2d 1512, 1512–21 (9th Cir. 1993) (Kozinski, J., dissenting from the order rejecting the suggestion for rehearing en banc).

proceed.⁷⁹ The lesson is the one drawn in Part IV.B: confusion-based and copyright-based theories miss the core wrong, and a dedicated identity right does more work.

2. Statutes on Digital Replicas

Several states have legislated specifically for AI replicas. Tennessee's ELVIS Act of 2024 protects voice and creates liability for distributing a tool whose primary purpose is producing a particular individual's voice or likeness without authorisation.⁸⁰ California in 2024 made unenforceable any contract term allowing a digital replica to replace a performer's in-person work unless the term reasonably specifically describes the intended uses and the performer had legal or union representation,⁸¹ and extended its post-mortem right to digital replicas.⁸² These statutes treat a replica as something a person may license, but only on terms the law supervises.

At the federal level, the NO FAKES Act would create a federal right against unauthorised digital replicas of voice and likeness that cannot be assigned during life but can be licensed, survives death for a limited period, provides notice-and-removal with penalties for false notices, and excludes news, commentary, satire and parody.⁸³ It has not been enacted. The TAKE IT DOWN Act, which has, criminalises non-consensual intimate imagery, including AI-generated forgeries, and requires platforms to remove it within forty-eight hours.⁸⁴

3. Platform Immunity

Section 230 of the Communications Decency Act gives platforms broad immunity for third-party content,⁸⁵ subject to an exception for "any law pertaining to intellectual property." The circuits are divided on whether that exception covers state publicity claims: the Ninth Circuit says it does not; the Third Circuit says it does.⁸⁶ Whether a platform hosting a deepfake endorsement is liable under state publicity law may therefore depend on where the suit is brought.

B. The European Union

1. No Harmonised Right Against Appropriation

The European Union has not harmonised the right to control commercial use of one's identity; protection depends on national law, such as the German statute protecting a person's

⁷⁹ *Lehrman v. Lovo, Inc.*, No. 1:24-cv-03770 (S.D.N.Y. July 10, 2025).

⁸⁰ ELVIS Act, *supra* note 80.

⁸¹ Assemb. B. 2602, 2023–2024 Reg. Sess. (Cal. 2024) (codified at CAL. LAB. CODE § 927).

⁸² Assemb. B. 1836, 2023–2024 Reg. Sess. (Cal. 2024) (amending CAL. CIV. CODE § 3344.1).

⁸³ Nurture Originals, Foster Art, and Keep Entertainment Safe (NO FAKES) Act of 2025, S. 1367, 119th Cong. (2025); *see also* NO FAKES Act of 2024, S. 4875, 118th Cong. (2024).

⁸⁴ Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act, Pub. L. No. 119-12, 139 Stat. ____ (2025).

⁸⁵ 47 U.S.C. § 230(c)(1).

⁸⁶ *Id.* § 230(e)(2); *compare* *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118–19 (9th Cir. 2007), *with* *Hepp v. Facebook*, 14 F.4th 204, 210–14 (3d Cir. 2021).

image or the French Civil Code's guarantee of respect for private life.⁸⁷ The Union has instead responded through data protection, AI regulation and platform regulation.

2. Data Protection

The GDPR treats images and recordings of identifiable persons as personal data, and biometric data as a special category, but only where processed “for the purpose of uniquely identifying a natural person,”⁸⁸ and with an exception for data the subject has manifestly made public.⁸⁹ Even so, it offers two things the Indian statute does not. Publicly available data still requires a lawful basis for processing. And individuals have a right to compensation for material and non-material damage caused by unlawful processing.⁹⁰

3. The AI Act

The AI Act addresses deepfakes through transparency duties that apply from August 2, 2026.⁹¹ It defines a deepfake as AI-generated or manipulated content that resembles existing persons, objects, places or events and would falsely appear to be authentic.⁹² Providers of generative systems must ensure that outputs are machine-readably marked as artificial, and deployers who generate deepfakes must disclose that the content is artificial, with a lighter duty for evidently artistic, satirical or fictional works.⁹³

4. The Digital Services Act

The Digital Services Act preserves a knowledge-based safe harbour for hosting services, prohibits general monitoring, and requires a notice-and-action mechanism.⁹⁴ Platforms must disclose who paid for each advertisement, and very large platforms must assess and mitigate systemic risks to fundamental rights, which may include marking deepfakes prominently.⁹⁵ The

⁸⁷ Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie [KUG] [Art Copyright Act], Jan. 9, 1907, §§ 22–23 (Ger.); CODE CIVIL [C. civ.] [Civil Code] art. 9 (Fr.).

⁸⁸ GDPR, *supra* note 72, arts. 4(14), 9(1).

⁸⁹ *Id.* art. 9(2)(e).

⁹⁰ *Id.* arts. 6, 82.

⁹¹ Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), art. 113, O.J. (L 2024/1689) [hereinafter AI Act].

⁹² *Id.* art. 3(60).

⁹³ *Id.* art. 50(2), (4).

⁹⁴ Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), arts. 6, 8, 16, 2022 O.J. (L 277) 1 [hereinafter DSA].

⁹⁵ *Id.* arts. 26, 34, 35(1)(k).

Unfair Commercial Practices Directive separately prohibits false claims about the sponsorship or approval of a trader or product.⁹⁶

These instruments form a comprehensive, if complex, regulatory architecture. Their limits are partly ones of enforcement, particularly against content originating outside the Union. But there is a more basic limit. The EU regime tells consumers that content is synthetic and makes platforms manage risk. It does not give the person replicated a right to refuse commercial use. A correctly labelled, unauthorised AI advertisement featuring a recognisable actor may satisfy the AI Act and still appropriate that actor's identity.

C. What India Should Borrow, and What It Should Not

Across the three jurisdictions, a common pattern appears. India has constitutional seriousness but little statutory detail. The United States has sophisticated commercial law, fragmented across states and limited by platform immunity. The European Union has regulatory reach, but leaves appropriation itself to national law. An adequate framework would combine the first two strengths while keeping the third in view.

More concretely, the comparison shows five things India lacks:

1. a statutory right against commercial appropriation of identity that does not depend on proof of confusion;
2. rules on the content of digital-replica licences that protect the person licensing their identity (California);
3. a defined post-mortem term (California and the NO FAKES Act), where Indian courts have held that the rights end at death;
4. an individual right to compensation for unlawful processing, as under the GDPR; and
5. a notice-and-takedown process that the affected person can use directly, with penalties for false notices (the NO FAKES Act).

It also shows five things India should not copy:

1. *Broad platform immunity*. India's safe harbour is already conditional on due diligence; adopting anything like section 230, particularly for paid advertising, would be a step backwards.
2. *Fragmentation*. The American state-by-state approach produces uncertainty that a single national statute in India can avoid.

⁹⁶ Directive 2005/29/EC, of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market, art. 6(1)(c), 2005 O.J. (L 149) 22.

3. *Unlimited transferability.* Jennifer Rothman has argued that freely assignable publicity rights let others own a person's identity.⁹⁷ India should permit licensing but not outright assignment, as the NO FAKES Act does.
4. *Transparency as a substitute for consent.* Labelling rules are valuable, but they do not answer whether a person agreed to be replicated.
5. *Imported speech doctrines.* American tests such as "transformative use" do not map onto Article 19(2).⁹⁸ Indian law protects commercial speech under Article 19(1)(a) while allowing restriction of deceptive advertising,⁹⁹ and needs exceptions drafted for its own constitutional framework.

VII. WHY A STATUTE, AND WHY NOT ONLY THE COURTS

If Indian courts are already protecting against AI replicas, why legislate? There are four reasons.

The first is certainty, which matters most to the legitimate market. A company licensing an actor's replica needs to know what valid consent looks like and whether the estate can enforce it after death; a developer needs to know whether training a voice model on a singer's recordings is lawful; a platform needs to know what to do with a complaint. Interim orders cannot answer these questions, and Part IV.A.5 identified six on which the case law is unsettled.

The second is access. The remedial system described in Part V.D is available to those who can bring a commercial suit in a High Court. A regional actor, a doctor whose face is used to sell a fake medicine, or an ordinary person placed in a fraudulent advertisement often cannot. If personality rights rest on Article 21, protection should not depend on the resources needed to obtain an *ex parte* injunction.

The third is remedies. Injunctions stop future harm but do not compensate for past use, and the courts have no method for valuing it. A statute can provide for damages, an account of profits and statutory damages.

The fourth concerns free expression, and it cuts in a direction that is sometimes overlooked. The strongest criticism of the recent orders is that they protect too much: orders restraining use of a person's identity "in any manner" may reach parody, memes and news.¹⁰⁰ That is an argument for legislation, not against it. Courts acting on *ex parte* applications are poorly placed to draw the line between appropriation and expression. A statute can draw it in advance, in every case.

⁹⁷ Jennifer E. Rothman, *The Inalienable Right of Publicity*, 101 GEO. L.J. 185 (2012); *see also* JENNIFER E. ROTHMAN, *THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD* (2018).

⁹⁸ *See* Comedy III Prods., Inc. v. Gary Saderup, Inc., 21 P.3d 797 (Cal. 2001).

⁹⁹ *Tata Press Ltd. v. Mahanagar Tel. Nigam Ltd.*, (1995) 5 SCC 139 (India).

¹⁰⁰ Majumder, *supra* note 38.

Two objections deserve a response. One is that regulation will discourage innovation; the opposite seems more likely, since performers will license their identity more readily when they know the terms will be enforced. The other is that existing statutes could simply be amended. Some amendments are needed, but the central right needs a single home, with one definition and one set of exceptions. The Government has so far adapted existing instruments.¹⁰¹ For commercial replicas at least, adaptation has reached its limit.

VIII. A FRAMEWORK FOR COMMERCIAL AI-GENERATED DIGITAL REPLICAS

This Part sets out the elements of a statute, which this Article calls a Personality Rights and Digital Identity Protection Act. These are normative recommendations; where they draw on existing law, that is noted.

A. What Is Protected: Defining a Digital Replica

The statute should protect two things. The first is a general right to control the commercial use of one's identity—name, likeness, voice, signature and other distinctive attributes—putting on a statutory basis what the courts have developed since *ICC* and *Titan*. The second is a specific rule for digital replicas, defined as a computer-generated or computer-altered representation of an individual's voice or visual likeness, realistic enough to be readily identified as that individual, in a performance, statement or appearance the individual did not actually make.

The definition is deliberately narrower than “persona.” Catchphrases and mannerisms are already covered by the general right where they identify a person. The digital-replica rule is reserved for what makes AI different: the realistic simulation of a person doing or saying something they did not.

B. Who Is Protected

The right should belong to every individual, not only to celebrities. Fame should affect the measure of damages, not the existence of the right. This resolves the tension between *Arijit Singh*, which treats celebrity status as a threshold, and *Krishna Kishore Singh*, which rejected a separate category of celebrity rights.

C. When Liability Arises: Commercial Use Without Consent

The core prohibition should be the use of a person's identity, or a digital replica of them, for a commercial purpose without consent. Commercial purposes include advertising, endorsement, merchandise, and use of a replica in place of a paid performance. Following *Titan*, liability should not require proof of confusion. And to correct the problem identified in Part IV.B, a label stating that content is AI-generated should not be a defence.

Non-commercial uses should remain governed by privacy, defamation and criminal law, with one exception. Creating or distributing sexually explicit digital replicas without consent

¹⁰¹ See also Ministry of Elecs. & Info. Tech., India AI Governance Guidelines (Nov. 2025) (India).



should be prohibited whether or not there is a commercial purpose, with expedited removal and protection of the victim's identity in proceedings. This responds to the gendered pattern of harm discussed in Part III.A.

D. Consent and Licensing

Consent should be informed, specific and in writing. The statute should permit a person to license the commercial use of their identity and digital replica, so that the legitimate market described in Part II.C can develop, but the right should not be assignable outright during the person's lifetime. A licence may transfer the right to use; it should not transfer ownership of the person's identity.¹⁰²

A valid licence should state the intended uses with reasonable specificity, the duration, territory and media. Following California, a term allowing a replica to replace work the person would otherwise perform should be unenforceable unless it describes the intended uses and the person had independent legal or union representation.¹⁰³ The person should be able to end a licence for future uses on defined grounds, such as use for unlawful products or in a manner seriously harmful to their reputation.

The statute should also resolve the question raised in Part IV.C.3. An advertisement using a licensed replica should disclose that it does so, and the licence should require the person's approval of the claims made in their name, individually or by category. On that basis, a licensed synthetic endorsement can reflect the "genuine, reasonably current opinion" the CCPA guidelines require.

E. Training

A rule requiring consent for every appearance of an identifiable person in a training dataset would reach almost every general-purpose model. A more workable rule distinguishes two cases.

Where a model, voice pack or other system is trained on an individual's images or recordings with the purpose, or reasonably foreseeable effect, of producing replicas of that particular individual, consent should be required. This is the conduct at issue in *Arijit Singh*. For general-purpose training, the statute should rely on data-protection and copyright law, but the publicly available data exclusion should be amended so that it does not extend to processing biometric features of a person's face or voice in order to build a replica of that person.

F. Generation, Distribution and Platform Responsibility

The statute should allocate responsibility along the chain described in Part V.

¹⁰² See Rothman, *The Inalienable Right of Publicity*, *supra* note 96.

¹⁰³ Assemb. B. 2602, *supra* note 80.



Creators and advertisers should be directly liable for unauthorised commercial use. An advertiser publishing an advertisement featuring a recognisable real person should hold evidence of that person's consent and produce it on request.

Tool providers that market a system for replicating particular named individuals should be liable for unauthorised replicas made with it, unless they verify consent, drawing on the ELVIS Act's treatment of tools whose primary purpose is replication.¹⁰⁴ Providers of general-purpose systems should embed provenance markers and act on notices about specific outputs, but should not be liable merely because a user misused a general tool.

Platforms should keep the section 79 safe harbour, on conditions specific to digital replicas. First, the person depicted, or their agent, should be able to notify an unauthorised commercial replica, which the platform must act on within a fixed period—extending the model already used for morphed images in rule 3(2)(b)—subject to counter-notice and penalties for knowingly false notices, as the NO FAKES Act proposes.¹⁰⁵ Second, a platform accepting a *paid* advertisement featuring a recognisable real person should require the advertiser to declare that consent has been obtained, and should lose the safe harbour for that advertisement if it does not. Third, once a replica has been found unlawful, platforms should take reasonable steps against identical reuploads. This is consistent with *Shreya Singhal*, because the finding of unlawfulness will already have been made.

G. Consent Infrastructure and Provenance

Duties to check consent are workable only if consent can be checked. The statute should establish a voluntary registry, which performers' agencies could also use, in which individuals record whether they have granted or withheld consent to commercial digital replicas. Registration should not be a condition of protection, but it should make it harder for an advertiser or platform to claim that it could not have known consent was absent.

Provenance standards are the technical counterpart. The 2026 amendments already require provenance markers for synthetic content, and the C2PA specification provides an industry standard for recording how content was made.¹⁰⁶ The statute should require licensed replicas to carry provenance information identifying the licence, so that a platform can tell a licensed synthetic endorsement from an unlicensed one.

¹⁰⁴ ELVIS Act, *supra* note 80.

¹⁰⁵ S. 1367, *supra* note 82.

¹⁰⁶ COAL. FOR CONTENT PROVENANCE & AUTHENTICITY, C2PA Technical Specification, <https://c2pa.org/specifications/>.

H. Post-Mortem Rights

Indian courts have held that personality rights are not heritable.¹⁰⁷ For commercial digital replicas, Parliament should depart from that position by creating a descendible right for a fixed term after death, exercisable by the heirs, by a representative the person designated or, failing either, by a statutory trustee. The length of the term is a policy question; California's seventy years and the shorter period in the NO FAKES Act show the range of choices.¹⁰⁸

The post-mortem right should be limited to commercial uses. Biographies, biopics, documentaries, historical works and news should be outside it. This preserves the holding in *Krishna Kishore Singh*, which concerned a film about the actor's life, while addressing the case it did not face: the use of a dead person's cloned voice or face to sell products or produce new performances.

I. Exceptions for Expression

The statute should state its exceptions expressly, so that they do not depend on a defendant appearing in an ex parte proceeding. It should exclude:

1. news reporting, documentary and biographical works, and public-affairs commentary;
2. criticism, commentary, parody, satire and pastiche, including memes;
3. fictional and artistic works, provided the replica is not used to advertise a product other than the work itself and is not presented as a genuine statement or appearance of the person;
4. incidental or fleeting uses; and
5. research, detection and authentication of synthetic media.

None of these exceptions should cover sexually explicit replicas made without consent, or replicas used to suggest that the person endorses a product. The underlying test is whether the use exploits the person's identity to sell something, and whether it is likely to be taken as genuine. This tracks the distinction drawn in *DM Entertainment* and *Jackie Shroff*, and fits the constitutional position that commercial speech is protected while deceptive advertising may be restricted.¹⁰⁹

J. Remedies

The statute should provide for:

1. interim and final injunctions, including against unidentified defendants and, where appropriate, dynamic injunctions;
2. orders requiring platforms and registrars to disclose the identity of persons responsible;

¹⁰⁷ *Krishna Kishore Singh v. Sarla A. Saraogi*, CS (COMM) 187/2021 (Del. HC July 11, 2023) (India); *Deepa Jayakumar v. A.L. Vijay* (Mad. HC 2021) (India).

¹⁰⁸ CAL. CIV. CODE § 3344.1(g) (West); S. 1367.

¹⁰⁹ *Tata Press Ltd. v. Mahanagar Tel. Nigam Ltd.*, (1995) 5 SCC 139 (India); *DM Ent. Pvt. Ltd. v. Baby Gift House*, CS (OS) 893/2002 (Del. HC Apr. 29, 2010) (India); *Jaikishan Kakubhai Saraf v. Peppy Store*, CS (COMM) 389/2024 (Del. HC May 15, 2024) (India).

3. damages for commercial loss, or an account of the defendant's profits, at the claimant's election;
4. statutory damages within a defined range, where actual loss is hard to prove;
5. additional damages for sexually explicit or seriously defamatory replicas;
6. corrective notices, published by the defendant or the platform, where a false endorsement has circulated widely.

The measure of damages needs particular attention. The natural starting point is the fee the person would reasonably have charged for a licence covering the use actually made, as in *Irvine v. Talksport*.¹¹⁰ But that understates the loss where the person would never have agreed at any price—an association with a fraudulent scheme, for example—or where reputation was damaged. There the court should be able to award more, and statutory damages should provide a floor for persons with no endorsement history.

Two consequential amendments are also needed. The Consumer Protection Act should give the person whose identity was used in a misleading advertisement standing to complain to the CCPA and to receive compensation, and should make clear that such a person is not an “endorser” under section 21 unless they consented. And victims of sexually explicit replicas should have access to expedited procedures and legal aid.

K. Cross-Border Enforcement

A deepfake may be generated anonymously in one country, distributed through a platform incorporated in a second, and viewed in a third.

The statute should give Indian courts jurisdiction over unauthorised replicas targeted at audiences in India, and require platforms serving Indian users to designate a contact for notices. The Delhi High Court has held that it may order global removal of content uploaded from India.¹¹¹ That approach is controversial, and the statute should prefer geographic restriction by default, reserving global removal for replicas clearly unlawful where they are hosted, such as non-consensual sexual imagery.

International cooperation remains necessary. India is not a party to the Budapest Convention,¹¹² though the UN Convention against Cybercrime adopted in 2024 may assist with serious offences.¹¹³ For civil identity rights, the realistic path is bilateral cooperation, mutual

¹¹⁰ *Irvine v. Talksport Ltd.* [2003] EWCA (Civ) 423 (Eng.).

¹¹¹ *Swami Ramdev v. Facebook, Inc.*, 2019 SCC OnLine Del 10701 (Del. HC) (India).

¹¹² Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

¹¹³ G.A. Res. 79/243, United Nations Convention against Cybercrime (Dec. 24, 2024).



recognition of judgments and work in WIPO on minimum standards, supported by consent and provenance built into the systems that generate content.¹¹⁴

IX. CONCLUSION

AI-generated celebrity content is an early sign of a broader change, in which anyone whose image or voice exists online can become raw material for a commercial replica. Celebrities shown endorsing fraudulent schemes are the most visible cases; ordinary people whose faces are used in fake advertisements are harmed more widely, with far fewer means of relief.

Indian law protects the commercial value of identity in fragments, each depending on a condition that AI replicas can avoid. The courts have responded with energy, but through interim orders that leave the test for liability, the scope of protection, the position after death, the remedies and the limits of free expression unsettled. The 2026 amendments bring transparency to synthetic media, but transparency is not consent.

The proposed framework treats identity as both an aspect of dignity and a commercial asset, and sees no contradiction between the two. It allows people to license their replicas on terms the law supervises, requires consent before commercial use, places duties on those best placed to check that consent, provides a limited post-mortem right, and protects news, criticism, parody and art.

The legal choices made in the next few years will decide whether generative AI becomes a tool that people can use to extend their own creative and commercial lives, or an industrial machine for taking human identity and exploiting it again and again.

¹¹⁴ WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* (2018).