DEEPFAKES, MISINFORMATION & THE INDIAN LEGAL VACUUM: THE URGENT NEED FOR A DEDICATED DEEPFAKE LAW

Priyanshu Bisht, B.A.LL.B. (Hons.), Graphic Era Hill University, Dehradun

ABSTRACT

This paper conducts a doctrinal and comparative analysis of the 'legal vacuum' in Indian law concerning the regulation of generative artificial intelligence and deepfake technology. It argues that existing statutory frameworks, primarily the Indian Penal Code, 1860 (and its successor, the Bharatiya Nyaya Sanhita, 2023) and the Information Technology (IT) Act, 2000, are conceptually inadequate to address the unique harms of synthetic media. The core thesis is that deepfake technology severs the traditional criminal law nexus of *mens rea* (guilty mind) and *actus reus* (guilty act), particularly in cases involving autonomous generation from "low-intent prompts".

The analysis demonstrates the specific failures of the IT Act: Sections 67 and 67A create an "obscenity trap," rendering them useless against the significant, non-obscene harms of political misinformation and financial fraud ; Section 66D (cheating by impersonation) is too narrowly focused on financial inducement ; and Section 66E (privacy) is textually inapplicable to the act of *synthesis* as opposed to the *capture* of an image. This paper posits that this legal vacuum creates an unavoidable constitutional collision between the fundamental right to privacy and informational autonomy under Article 21 (as articulated in *K.S. Puttaswamy v. Union of India*) and the right to free expression under Article 19(1)(a) (as protected in *Shreya Singhal v. Union of India*).

The paper critiques the Ministry of Electronics and Information Technology's (MeitY) recent attempts to regulate deepfakes via subordinate amendments to the IT Rules, 2021, arguing these moves are constitutionally suspect. The mandate for "proactive detection" is a *prima facie* violation of the *Shreya Singhal* precedent, which affirmed Section 79 safe harbours and rejected general monitoring obligations. Furthermore, the paper addresses the acute evidentiary crisis, arguing that Section 65B of the Indian Evidence Act, 1872 (now Section 63, Bharatiya Sakshya Adhiniyam, 2023) contains an "authentication fallacy," as it validates the integrity of the *medium* but not the *authenticity of the content*, rendering "pristine" deepfakes admissible.

Drawing on a comparative analysis of international models, including the transparency-led EU AI Act , the specific criminalisation approach of the UK's Online Safety Act , and the failures of overbroad US state laws, this paper rejects mere amendments. It concludes by proposing a *sui generis* Act as the only constitutionally viable path forward. This proposed framework includes precise definitions, a "trident" of graded liabilities (specific criminal offences, a civil right of action for dignity harms, and mandatory transparency obligations), technical watermarking standards , and a reformed evidentiary burden.

I. Introduction: The Crisis of Synthetic Reality

In late 2023, India's digital public square was shaken by a "synthetic tsunami." A viral video appearing to show actress Rashmika Mandanna entering an elevator was rapidly exposed as a deepfake, her face convincingly grafted onto the body of another woman.[1] This incident was not merely another instance of celebrity 'morphing'; it was a national flashpoint, dragging the obscure technological threat of deepfakes into the centre of public and political discourse. This single video served as a harbinger of a new era of misinformation, one that escalated dramatically during the 2024 general elections, where political parties were reported to be exploiting generative artificial intelligence (AI) for propaganda.[2] With reports suggesting over 75% of Indians were exposed to political deepfakes during this period, the threat to democratic integrity became undeniable.[2]

India's unique digital ecosystem creates a perfect storm for such a crisis. With over 850 million internet users, it is the world's largest connected democracy.[4] However, this high internet penetration, driven primarily by mobile platforms like WhatsApp [5], is coupled with relatively low levels of widespread digital media literacy.[6] This environment makes the populace uniquely susceptible to emotionally resonant and divisive synthetic media.[7] The World Economic Forum, recognising this vulnerability, has identified misinformation and disinformation as the highest-ranked risk for India.[5]

This paper moves beyond the vernacular term "deepfake" to address the underlying technology: a paradigm shift in AI. Unlike traditional digital alteration, modern synthetic media is created using sophisticated deep learning architectures, primarily Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and, more recently, diffusion models.[6] These models do not merely *edit* existing data; they *generate* entirely new, hyper-realistic audio-

visual content.[10] This fundamental shift from *alteration* to *synthesis* is the lynchpin of the legal challenge.

The harms precipitated by this technology are multi-pronged and severe. They range from the deeply personal and gendered weaponisation of non-consensual sexual imagery (NCII) [1] and financial fraud through voice-cloning [14]; to the systemic erosion of democratic discourse through political misinformation [7]; and finally, to the epistemic crisis in the judicial system, where digital evidence is no longer presumptively trustworthy.[15]

This paper argues that India's current legal framework constitutes a "legal vacuum" when confronted with deepfake technology.[16] This vacuum is not a simple *absence* of law, but a *doctrinal failure* of existing statutes. Laws designed for an analogue world (the Indian Penal Code, 1860) and a simpler internet era (the Information Technology Act, 2000) are conceptually incapable of addressing harms predicated on *synthesis* rather than *action*, and *autonomous generation* rather than discernible *human intent*. The public debate, sparked by the celebrity NCII case, has largely focused on obscenity [20], ignoring the equally pernicious, non-obscene threats to political and financial stability. This paper will conduct a doctrinal analysis of this legal vacuum, demonstrate the inadequacy of the state's recent regulatory responses, and propose a *sui generis* legislative framework as the only constitutionally viable path forward.

II. Doctrinal Foundations: Indian Law on Impersonation, Truth, and Obscenity

Indian criminal jurisprudence, inherited from the common law tradition and codified in the Indian Penal Code (IPC), 1860, is built upon the foundational joinder of a guilty act (*actus reus*) and a guilty mind (*mens rea*).[21] Our laws are designed to ascertain human intent and punish corresponding human actions. This framework traditionally addresses harms analogous to those from deepfakes through provisions like:

- **Forgery:** Section 463 of the IPC defines forgery as the making of a false document or electronic record with the *intent* to cause damage, commit fraud, or support a false claim.[23]
- **Cheating:** Section 415 of the IPC criminalises deceitfully inducing a person to deliver property or consent to retaining it.
- **Defamation:** Section 499 of the IPC (now Section 356 of the Bharatiya Nyaya Sanhita,

2023 or BNS) targets any imputation made with the *knowledge* or *intent* to harm another's reputation.[4]

- **Obscenity:** Section 292 of the IPC and, more pointedly for the digital realm, Sections 67 and 67A of the Information Technology (IT) Act, 2000, regulate content that is "lascivious or appeals to the prurient interest".[24]

This established legal doctrine, however, suffers a fundamental rupture when confronted with generative AI. Deepfakes sever the causal link between the human operator and the criminal act, challenging the very applicability of *mens rea* and *actus reus*.[15]

The *actus reus* is obscured. The "guilty act" of creating a hyper-realistic forgery is not performed by the human, but by the autonomous AI model, a "black box" [9], which is often pre-trained on vast datasets.[15] The human's physical "act" is often reduced to merely entering a text prompt.

More critically, the *mens rea* is strained to breaking point. Criminal intent becomes difficult to attribute when a user enters a "low-intent prompt" [15], an innocuous or vague command, and the AI autonomously generates deeply harmful, defamatory, or fraudulent content.[15] Can a user claim they lacked the specific *intent* to forge or defame, arguing they could not foresee the AI's hyper-realistic output? This "autonomously generated misinformation" [15] lacks the clear human authorship and wilful intent upon which our entire criminal jurisprudence rests.[22] This doctrinal impasse is not a minor flaw to be patched; it is a conceptual chasm, rendering traditional criminal provisions effectively sterile against this new form of harm.

III. The Unique Pathologies of Deepfake Harms in India

The deepfake threat is not monolithic; it manifests as a spectrum of harms, each with a unique character and devastating potential in the Indian context.

A. Political and Social Misinformation

The most diffuse, yet democratically corrosive, application of deepfakes is in the political arena. The 2024 general elections served as a potent testing ground, with 75% of Indian voters reporting exposure to AI-generated political deepfakes.[2] This technology is no longer a futuristic threat but a present-day tool for destabilising democratic trust.[3] Synthetic media is

used to create false narratives, impersonate political leaders, and target journalists [28] in an effort to exploit India's sensitive social and religious fault-lines.[6] The harm extends beyond "fake news"; it creates a "liar's dividend," an epistemic fog where the public loses the ability to distinguish truth from fabrication, and even authentic media can be dismissed as fake.

B. The Gendered Weapon: Non-Consensual Sexual Imagery (NCII)

The most acute, personal, and violent manifestation of deepfake technology is its use as a tool of technology-facilitated gender-based violence (TFGBV).[13] Estimates suggest that as much as 98% of all deepfake content online is non-consensual pornography, and 99% of that material targets women.[31] In India, this has manifested in "nudify" apps [12] and deepfake pornography used for public shaming, harassment, and extortion.[1]

The harms are intersectional, yet the law treats them in isolated silos. A case study from a report by the Rati Foundation provides a chilling illustration: a woman's photograph, submitted for a *loan application*, was stolen. An extortionist used a "nudify" app to create an explicit image of her.[12] When she refused to pay, the synthetic image, *along with her phone number*, was circulated on WhatsApp, resulting in a barrage of sexual harassment.[12] This single event constitutes data theft, financial extortion, sexual harassment, and a profound violation of dignity. Our legal framework, however, would force the victim to navigate a disjointed system: an FIR for obscenity under the IT Act would miss the extortion, while a complaint for cheating under the IPC would ignore the sexual violation. This siloing proves that laws targeting discrete *harms* are insufficient; we must target the *misuse of the technology itself*, the act of non-consensual synthesis.

Furthermore, the harm is not limited to the existence of an image. It is the *fear* of its possibility, which creates a "chilling effect" that silences women and forces their withdrawal from digital public life.[12]

C. Financial Deception and Identity Fraud

The economic harms are tangible and growing. They range from simple voice-cloning scams, where elderly individuals are tricked into believing a loved one is in distress [14], to sophisticated impersonations of business leaders. Deepfakes of prominent figures like N.R. Narayana Murthy have been used to promote fraudulent financial schemes.[28] The sophistication of this

threat was demonstrated in the Hong Kong-based Arup case, where an employee was duped into transferring over $25 million after attending a deepfake *video conference* call featuring a synthetic recreation of the company's CFO.[34] This signals a move from pre-recorded clips to real-time, interactive deception, a threat for which Indian commerce is unprepared.

D. The Evidentiary Conundrum

Perhaps the most systemic threat is the one posed to the integrity of the judicial system. Deepfakes fundamentally challenge the maxim of "seeing is believing," poisoning the well of digital evidence.[35] The widespread availability of this technology means that any audio-visual recording submitted in court, in cases ranging from criminal matters to divorce proceedings, can be plausibly challenged as a fabrication. This problem is compounded by a significant lack of technical expertise and forensic tools among law enforcement agencies and the judiciary [23], creating an evidentiary crisis where the law is unprepared for content that is "born fake".[15]

IV. The Indian Legal Framework: A Patchwork of Inadequacy

India's response to the deepfake threat has been to stretch existing, ill-fitting laws. A doctrinal analysis reveals that this patchwork is not merely outdated, but constitutionally and conceptually inadequate.

A. The Information Technology Act, 2000: A Misfit Tool

The IT Act, 2000, is the primary statute governing digital harms, yet its key provisions are doctrinally impotent against deepfakes.

- **The Obscenity Trap (Sections 67, 67A):** These are the most-cited provisions, punishing the publication of "obscene" or "sexually explicit" material.[23] While applicable to deepfake pornography, they create a dangerous "obscenity trap." They are *completely useless* against the vast majority of deepfake harms, including political misinformation, election propaganda, financial fraud, and reputational defamation, which are by definition *not* obscene.[27] Regulating deepfakes only through the lens of obscenity ignores the grave threats to democracy and security.

- **The Impersonation Failure (Section 66D):** This provision penalises "cheating by impersonation" using a computer resource.[23] The failure lies in its linkage to "cheating,"

which, as defined in the IPC, requires a fraudulent or dishonest inducement, typically for property. The section does not squarely apply to impersonation for the purpose of non-financial reputational harm, public mischief, or political satire.[23]

- **The Privacy Gap (Section 66E):** This provision, which punishes the violation of privacy, is textually inapplicable. Its *actus reus* is specific: "intentionally or knowingly *captures, publishes or transmits* the image of a *private area* of any person without his or her consent".[26] A deepfake does not "capture" an image of a "private area." It *synthesizes* an image of a *public* face, or voice, and grafts it onto other content.[41] The act is one of fabrication, not voyeurism, and thus falls outside the statute's plain language.

B. Criminal Law (IPC, 1860 and BNS, 2023): An Analogue Fix

The traditional criminal code offers little recourse. Provisions for defamation (Section 499 IPC / Section 356 BNS) [4] are notoriously slow, post-facto remedies, utterly insufficient for a harm that becomes global and irreversible in minutes.

The most damning critique of this framework comes from the National Commission for Women (NCW). The NCW has formally stated that existing laws on defamation and obscenity are inadequate to tackle AI-generated fake content.[43] It has recommended that the new Bharatiya Nyaya Sanhita (BNS) be amended to *add* specific definitions for "modified content" and "deep fake technology," and to create a new, specific offence criminalizing their creation and distribution.[43] This formal admission from a statutory body is a clear acknowledgement of the legal vacuum. Even with the new BNS, the *mens rea* impasse remains: proving criminal intent for content generated by a "low-intent prompt" remains a doctrinal impossibility.[15]

C. The Constitutional Rubicon: Puttaswamy vs. Shreya Singhal

The deepfake dilemma forces a direct and unavoidable collision between two pillars of our post-millennial constitutional jurisprudence: the right to privacy under Article 21 and the right to free expression under Article 19(1)(a).

The non-consensual creation of a deepfake is a *prima facie* violation of the fundamental right to privacy, dignity, and, crucially, informational autonomy, as articulated by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[13] This builds on *R. Rajagopal v. State of*

Tamil Nadu, which linked privacy to an individual's control over the dissemination of their own likeness.[36]

The state, therefore, has a constitutional obligation to act. However, its *method* of action is severely constrained by Article 19(1)(a) and the precedent in *Shreya Singhal v. Union of India*.[4] That judgment struck down Section 66A of the IT Act for its "vagueness" [4] and firmly established the "safe harbour" principle under Section 79. Intermediaries are passive conduits and cannot be held liable for user-generated content unless they receive "actual knowledge" of its illegality through a court order or government notification.[45] *Shreya Singhal* explicitly protects platforms from the burden of proactive or general monitoring of content.

This is where the state's response has become constitutionally checkmated. Faced with public pressure, the Ministry of Electronics and Information Technology (MeitY) has attempted to solve the deepfake problem not through a new Act of Parliament, but through *subordinate legislation*, namely, draft amendments to the IT Rules, 2021.[46] These draft rules are constitutionally suspect. They introduce a dangerously overbroad definition of "synthetically generated information" [47] and, most critically, they mandate that intermediaries "proactively detect and label" all such content.[48]

This mandate for proactive monitoring is a direct contravention of the *Shreya Singhal* precedent.[46] It converts passive conduits into active arbiters of truth, imposing a general surveillance duty that the Supreme Court has already found to be an unreasonable restriction on free speech. These draft rules are arguably *ultra vires* the parent Act (Section 79) and would likely be struck down as unconstitutional.[46] This constitutional impasse proves that the deepfake problem *cannot* be solved by executive rule-making. The only viable path is a new, *sui generis* Act of Parliament that is "narrowly tailored" [24] to survive the twin tests of Article 19(2) and *Puttaswamy*.

D. The Evidence Act, 1872 and BSA, 2023: The Authentication Fallacy

The final gap is evidentiary. The admissibility of electronic evidence in Indian courts is governed by Section 65B of the Indian Evidence Act, 1872 (now Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 or BSA).[36] The Supreme Court, in *Anvar P.V. v. P.K. Basheer* [57] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* [36], has made the certificate under Section 65B(4) mandatory for admitting secondary electronic evidence.[36]

This framework, however, contains a critical doctrinal flaw: it authenticates the *medium*, not the *message*. The Section 65B certificate merely attests to the integrity of the computer system, the lawfulness of its use, and the process of data storage.[36] It *does not* and *cannot* attest to the *truthfulness or authenticity of the content itself*.[57] A deepfake is a "pristine" file; it can be generated on a device and stored without any subsequent tampering. It would, therefore, be *fully admissible* in court with a valid Section 65B certificate, even though it is a complete fabrication. This "authentication fallacy" renders our evidentiary law powerless, allowing the very tools of justice to be co-opted for disseminating falsehoods.

Table 1: Analysis of Existing Indian Legal Framework & Gaps

Legal Provision	**Stated Offence / Requirement**	**Required Elements (Mens Rea / Actus Reus)**	**Doctrinal Gap for Deepfakes**
S. 67, 67A IT Act	Publishing obscene / sexually explicit material.	Content must be "lascivious or appeal to the prurient interest."	**Inapplicable to non-obscene harms** (e.g., political misinformation, financial fraud).[27]
S. 66D IT Act	Cheating by impersonation using a computer resource.	*Mens Rea:* Intent to "cheat" (i.e., fraudulent inducement for property).	**Narrow Scope.** Does not cover impersonation for non-financial reputational harm, harassment, or political propaganda.[23]
S. 66E IT Act	Violation of privacy.	*Actus Reus:* "Captures, publishes or transmits... image of a private area."	**Textually Inapplicable.** A deepfake *synthesizes* a *public* face; it does not "capture" a "private area".[26]
S. 463 IPC / BNS	Forgery.	*Mens Rea:* "Intent to cause damage or	**Mens Rea Impasse.** Hard to prove

		injury... or to commit fraud."	specific intent when a user enters a "low-intent prompt" and the AI generates the forgery.[15]
S. 499 IPC / BNS	Defamation.	Making an imputation with intent/knowledge of harm.	**Ineffective Remedy.** A slow, post-facto civil/criminal process. Insufficient for instantaneous, viral harm.
S. 65B Evidence Act / S. 63 BSA	Admissibility of electronic evidence.	Requires certificate authenticating the *device* and *process*.	**Authenticates the Medium, Not the Message.** A "pristine" deepfake file is perfectly admissible, defeating the rule's purpose.[36]

V. Comparative International Approaches: A Menu of Model

India is not alone in this regulatory struggle. As it contemplates a new law, it can draw from a global "menu" of regulatory models, each with distinct lessons.

A. The European Union: The Transparency Model

The EU's comprehensive AI Act employs a risk-based approach.[61] It classifies deepfakes as a "limited-risk" technology.[62] The core regulatory obligation is not prohibition but *transparency*.[64] Deployers of AI systems that generate or manipulate audio-visual content must *disclose* that the content is artificial.[35] This includes an obligation to inform users when they are interacting with an AI system.[66]

- **Lesson for India:** A mandatory disclosure and labeling regime is a powerful, proportionate, and speech-respecting tool that can be adopted to balance Article 19 and Article 21.

B. The United Kingdom: The Specific Criminalization Model

The UK has taken a precise, surgical approach to the most acute harm: NCII. The Online Safety Act 2023 inserts new offences into the Sexual Offences Act 2003.[69] Section 66B criminalises the *sharing* of intimate images, real or synthetic, without consent.[69] Critically, this base offence *removes the traditional mens rea requirement* of "intent to cause distress," which had been a barrier to prosecution.[71] Furthermore, new government proposals aim to go further by criminalising the mere *creation* and *requesting* of non-consensual intimate deepfakes.[69]

- **Lesson for India:** This is a doctrinally precise solution. By isolating the worst harm (NCII) and creating a specific offence that bypasses the "intent" impasse, the UK has provided a template for solving the *mens rea* problem.

C. The United States: A Cautionary Tale

The US provides a critical "cautionary tale." Its fragmented, state-level approach is failing.[3] Several California laws targeting election-related deepfakes have been struck down by a Federal Judge.[76] AB 2655, which required platforms to block or label such content, was invalidated for violating **Section 230** (platform immunity).[76] AB 2839, which created a civil cause of action, was struck down as a violation of the **First Amendment** (free speech), with the judge calling it a "blunt tool" that unconstitutionally hindered satire.[76]

- **Lesson for India:** This is a stark warning. Any Indian law that is overbroad (like MeitY's draft rules) and fails to provide explicit, robust safe harbours for parody, satire, and art *will* be struck down as a violation of Article 19(1)(a).

D. The State-Control Models: China and Singapore

China and Singapore offer models of efficiency based on state control. China's "Deep Synthesis Regulation" is a top-down regime [17] that mandates *explicit user consent* for biometric use [79] and requires *strict, non-removable watermarking* for all synthetic content.[77] Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) empowers government ministers with *direct, pre-emptive authority* to issue correction or takedown orders without prior judicial review.[81]

- **Lesson for India:** These models offer viable technical (watermarking) and rapid-response

(takedown) mechanisms. However, their executive-heavy, pre-censorship nature is constitutionally incompatible with India's jurisprudence, particularly the *Shreya Singhal* precedent and the doctrine of separation of powers.

Table 2: Comparative International Regulatory Models

Jurisdiction	**Primary Law**	**Core Regulatory Approach**	**Key Provisions**	**Applicability / Lessons for India**
European Union	EU AI Act	**Transparency (Risk-Based)**	Mandates *disclosure* for all "limited-risk" deepfakes. Users must be informed they are interacting with AI.[62]	**Adopt.** A mandatory labeling/disclosure regime is a constitutionally sound, proportionate measure.
United Kingdom	Online Safety Act 2023	**Specific Criminalization**	Criminalizes *sharing* (S. 66B) and (proposes to) *creating* intimate deepfakes, *without* requiring "intent to cause distress".[69]	**Adopt.** This is the *precise surgical tool* to tackle NCII, solving the *mens rea* problem for the most grievous harm.
United States	State Laws (e.g., CA, TX)	**Fragmented / Unconstitutional**	State laws targeting election deepfakes have been struck down on S. 230 (platform) and First Amendment (speech) grounds.[74]	**Learn From Failure.** Proves that any Indian law *must* have robust safe harbours for satire/parody to survive an Art 19(1)(a) challenge.

China	Deep Synthesis Regulation	**State Control (Technical)**	Mandates *non-removable watermarking* and explicit consent for biometrics.[77]	**Adapt.** A mandatory *technical standard* for watermarking/ provenance is a viable, preventative solution.
Singapore	POFMA 2019	**State Control (Executive)**	Grants government ministers *direct power* to issue takedown/correction orders without prior judicial review.[81]	**Caution.** While rapid takedowns are needed, this executive-led model would likely fail India's *Shreya Singhal* and basic structure tests.

VI. Analysis & Proposed Framework: A Dedicated Indian Deepfake Act

A. The Case for a Sui Generis Act over Amendments

The analysis in Section IV demonstrates that amending existing laws is a constitutionally and doctrinally doomed exercise. Amending the IT Rules is constitutionally untenable post-*Shreya Singhal*.[46] Amending the IPC/BNS is doctrinally insufficient to address the *mens rea* impasse and the speed of viral harm.[15] The *only* constitutionally viable path forward is a new, *sui generis* Act of Parliament [16] that is "narrowly tailored" [24] to balance the competing rights at play.

This new framework should adopt the perspective advanced by legal scholars Mohan & Wadhwa, reframing the issue not as a "platform-regulation problem" but as a "communication-governance problem".[84] The law's focus must be on the *actors* and the *content*, not on deputising platforms as state censors.

B. Core Components of a Dedicated Deepfake Law

A balanced and effective Act must incorporate a multi-pronged "trident" approach, supplemented by technical and evidentiary reforms.

1. **Clear Definitions:** The Act must begin by rejecting the overbroad "synthetically generated information" definition from MeitY's draft rules.[46] It must create a precise legal distinction between:

    - **Benign Synthetic Media:** Content created for parody, satire, art, research, education, or entertainment.

    - **Malicious Deceptive Deepfake:** Content that (a) is created without the explicit consent of the person depicted, and (b) is intended to cause harm, defraud, defame, incite violence, or constitutes NCII. This aligns with the NCW's call for a clear legal definition.[43]

2. **A Graded Liability Framework (The "Trident" Approach):**

    - **Tier 1: Criminal Offences (High-Tier):** Borrowing from the UK model [69], the Act must create *new, specific offences* for the *creation, possession, or distribution* of non-consensual sexual deepfakes. This offence should remove the traditional *mens rea* of "intent" and focus on the *act* of non-consensual creation. Specific offences must also target deepfakes used for financial fraud, extortion, and incitement to violence.[88]

    - **Tier 2: Civil Remedies (Mid-Tier):** The Act must create a new, *sui generis* civil "right of action" for victims of *all* "Malicious Deceptive Deepfakes" [42], including those for purely reputational and dignity-based harm. This would ground the right squarely in Article 21 and the *Puttaswamy* jurisprudence, providing victims (especially non-celebrities who cannot claim "personality rights" [42]) with a statutory path to seek rapid *injunctions* (takedowns) and *monetary damages*.

    - **Tier 3: Transparency (Low-Tier):** Borrowing from the EU AI Act [64], the Act should mandate *mandatory, clear, and conspicuous labeling* for all *Benign Synthetic Media* used in the public domain, especially in political advertising and news media.[20] This allows satire and art to exist, protecting Article 19, while simultaneously informing the public.

3. **Mandatory Technical Standards (Watermarking):** Adapting the principle from China's regulation [79], the Act should empower MeitY to set mandatory technical standards requiring generative AI service providers to embed *permanent, machine-readable*

metadata or watermarks [24] in all synthetic content. This provides a durable mechanism for provenance and traceability without resorting to content-based scanning.

4. **Platform Liability (A Shreya Singhal-Compliant Model):** This is the constitutional lynchpin.
    - **No Proactive Monitoring:** The Act must explicitly uphold the *Shreya Singhal* principle. Platforms retain their Section 79 "safe harbour" and must *not* be required to proactively monitor content.[46]
    - **Specific, Reactive Takedown Obligations:** The Act would create a new, *specific takedown mechanism* for content defined as *criminally illegal* (e.g., NCII). This would mandate rapid removal (e.g., within 24 hours) *upon receipt of a complaint from a victim* or a specific, *bona fide* court order.[24] This differs from MeitY's draft rules [90] as it is *reactive* to a specific, high-harm complaint, not *proactive* about all synthetic content.
5. **Evidentiary Reforms (The Burden Shift):** To fix the "authentication fallacy," the Act must amend the Bharatiya Sakshya Adhiniyam. It should state that when a party in a judicial proceeding challenges a piece of electronic evidence as a "Malicious Deceptive Deepfake," a *rebuttable presumption of inauthenticity* shall arise. The burden of proof would then *shift* to the party *submitting* the evidence to prove its authenticity through forensic means, rather than the burden being on the *victim* to prove its falsity.

VII. Conclusion: Rebuilding Truth in the Synthetic Era

This paper has demonstrated that India's existing legal framework is doctrinally flawed and practically incapable of addressing the multi-faceted deepfake threat.[16] The current reliance on outdated IPC provisions and constitutionally-suspect executive rule-making [46] leaves a dangerous legal vacuum. This is not merely a technical lacuna; it is an existential threat to the very concepts of privacy, dignity, and democratic integrity.

The philosophical challenge of deepfakes is not just the harm they cause to individuals, but their power to erode the shared, verifiable reality, the "death of truth" [50], upon which both democratic discourse and the judicial system depend.[3] The unchecked proliferation of synthetic media creates an epistemic crisis where trust, the bedrock of society, dissolves.

A dedicated, *sui generis* Deepfake Act is therefore not a policy choice, but a *constitutional necessity*. It is the only mechanism to resolve the intense friction between the Article 21 right to dignity and privacy under *Puttaswamy* and the Article 19(1)(a) right to free expression guarded by *Shreya Singhal*. By adopting a "trident" approach, specific criminalization for the worst harms (the UK model), a civil right of action for dignity harms (the *Puttaswamy* model), and mandatory transparency for all other synthetic media (the EU model), India can craft a law that is both effective and "narrowly tailored."

Such a law, buttressed by robust safe harbours for art and satire (the US lesson) and a reformed evidentiary standard, is the only way to defend the integrity of truth and the autonomy of the individual. The legislature must act with urgency, before the line between the real and the synthetic is irrevocably blurred.

Works cited

1. Full article: Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India, accessed on November 17, 2025, https://www.tandfonline.com/doi/full/10.1080/13600834.2024.2408914

2. Indian Voters Inundated with Deepfakes During the Largest Democratic Exercise in the World | Blackbird.AI, accessed on November 17, 2025, https://blackbird.ai/blog/india-election-deepfakes/

3. Regulating Deepfakes: Global Approaches to Combatting AI-Driven Manipulation - GLOBSEC, accessed on November 17, 2025, https://www.globsec.org/sites/default/files/2024-12/Regulating%20Deepfakes%20-%20Global%20Approaches%20to%20Combatting%20AI-Driven%20Manipulation%20policy%20paper%20ver4%20web.pdf

4. Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement - NeGD - National e-Governance Division, accessed on November 17, 2025, https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/

5. Elections and Misinformation – India Case Study | Al Jazeera Media Institute, accessed on November 17, 2025, https://institute.aljazeera.net/en/ajr/article/2645

6. Artificial Intelligence and the Escalation of Political Manipulation in South Asia, accessed on November 17, 2025, https://www.csohate.org/2025/11/14/ai-political-manipulation-in-south-asia/

7. Deepfakes, cloned voices, and digital media literacy: AI's role in the misinformation crisis in India - WACC Global, accessed on November 17, 2025, https://waccglobal.org/deepfakes-cloned-voices-and-digital-media-literacy-ais-role-in-the-misinformation-crisis-in-india/

8. Deepfake - Wikipedia, accessed on November 17, 2025, https://en.wikipedia.org/wiki/Deepfake

9. What is Generative AI? | IBM, accessed on November 17, 2025, https://www.ibm.com/think/topics/generative-ai

10. Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis - MDPI, accessed on November 17, 2025, https://www.mdpi.com/2224-2708/14/1/17

11. Copyright Protection in Generative AI: A Technical Perspective - arXiv, accessed on November 17, 2025, https://arxiv.org/html/2402.02333v2

12. 'The chilling effect': how fear of 'nudify' apps and AI deepfakes is ..., accessed on November 17, 2025, https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion-abuse

13. What's behind SFLC.in's award for defending digital freedoms?, accessed on November 17, 2025, https://www.apc.org/en/news/whats-behind-sflcins-award-defending-digital-freedoms

14. Deepfakes In India: Scammers Cloned My Nephew's Voice With AI | Cyber Scammed - Part 3/3 - YouTube, accessed on November 17, 2025, https://www.youtube.com/watch?v=SoxSHlsxkMQ

15. NAVIGATING DEEPFAKES IN INDIAN CRIMINAL LAW ..., accessed on November 17, 2025, https://ijirl.com/wp-content/uploads/2025/06/NAVIGATING-DEEPFAKES-IN-INDIAN-CRIMINAL-LAW-NAVIGATING-EVIDENTIARY-AND-LEGAL-REFORMS-UNDER-THE-BSA-AND-BNS-2023.pdf

16. Regulating Deepfakes: An Indian perspective - Digital Commons @ USF - University of South Florida, accessed on November 17, 2025, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2245&context=jss

17. Regulating Deepfakes In India: A Legal And Ethical Analysis Of Misinformation In The Age Of AI, accessed on November 17, 2025, https://www.ijllr.com/post/regulating-deepfakes-in-india-a-legal-and-ethical-analysis-of-misinformation-in-the-age-of-ai

18. Deepfake Laws In India: A Critical Analysis - IJFMR, accessed on November 17, 2025, https://www.ijfmr.com/papers/2025/1/34563.pdf

19. Deepfakes And The Law: A Comprehensive Comparative Analysis Of Indian And International Legal Frameworks, accessed on November 17, 2025, https://www.ijllr.com/post/deepfakes-and-the-law-a-comprehensive-comparative-analysis-of-indian-and-international-legal-framew

20. Regulating deepfakes and generative AI in India | Explained - The Hindu, accessed on November 17, 2025, https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece

21. artificial intelligence and criminal responsibility: legal challenges and implications for defamation in india by: pooja rajeep, accessed on November 17, 2025, https://www.ijlra.com/details/artificial-intelligence-and-criminal-responsibility-legal-challenges-and-implications-for-defamation-in-india-by-pooja-rajeep

22. CRIMINAL ACCOUNTABILITY FOR AI: MENS REA, ACTUS REUS, AND THE CHALLENGES OF AUTONOMOUS SYSTEMS - LIJDLR, accessed on November 17, 2025, https://lijdlr.com/2025/04/05/criminal-accountability-for-ai-mens-rea-actus-reus-and-the-challenges-of-autonomous-systems/

23. LEGAL CHALLENGES OF DEEPFAKE TECHNOLOGY AND AI ..., accessed on November 17, 2025, https://www.juscorpus.com/legal-challenges-of-deepfake-technology-and-ai-generated-content-in-india/

24. Deepfake Technology and It's Legal Regulation in India: A Doctrinal and Comparative Study, accessed on November 17, 2025, https://www.vintagelegalvl.com/post/deepfake-technology-and-it-s-legal-regulation-in-india-a-doctrinal-and-comparative-study

25. Articulating A Regulatory Approach to Deepfake Pornography in India - NLS Forum, accessed on November 17, 2025, https://forum.nls.ac.in/ijlt-blog-post/articulating-a-regulatory-approach-to-deepfake-pornography-in-india/

26. Deepfake Technology in Social Media: Social and Legal Implications in India - IJFMR, accessed on November 17, 2025, https://www.ijfmr.com/papers/2024/6/31284.pdf

27. Deepfake Technology in India and World: Foreboding and Forbidding, accessed on November 17, 2025, https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world%3A-foreboding-and-forbidding

28. Year of elections: Lessons from India's fight against AI-generated misinformation, accessed on November 17, 2025, https://www.weforum.org/stories/2024/08/deepfakes-india-tackling-ai-generated-misinformation-elections/

29. COMPARING "DEEPFAKE" REGULATORY REGIMES IN THE UNITED STATES, THE EUROPEAN UNION, AND CHINA - Georgetown Law Technology Review, accessed on November 17, 2025, https://georgetownlawtechreview.org/wp-content/uploads/2023/01/Geng-Deepfakes.pdf

30. The Question of Misinformation-Triggered Violence in Singapore: The Interplay between Misinformation, Faultlines and Violence - S. Rajaratnam School of International Studies (RSIS), accessed on November 17, 2025, https://rsis.edu.sg/ctta-newsarticle/the-question-of-misinformation-triggered-violence-in-singapore-the-interplay-between-misinformation-faultlines-and-violence/

31. Why India's Deepfake Pornography Infestation is a Concern - NUJS IPTLS - WordPress.com, accessed on November 17, 2025, https://nujsiplaw.wordpress.com/2024/04/01/why-indias-deepfake-pornography-infestation-is-a-concern/

32. Deepfakes, doxxing and digital abuse - The New Indian Express, accessed on November 17, 2025, https://www.newindianexpress.com/opinions/2025/Oct/20/deepfakes-doxxing-and-digital-abuse

33. Karnataka reports 12 deepfake-related cybercrime cases in two years - The Hindu, accessed on November 17, 2025, https://www.thehindu.com/news/national/karnataka/karnataka-reports-12-deepfake-related-cybercrime-cases-in-two-years/article69333474.ece

34. Top 5 Cases of AI Deepfake Fraud From 2024 Exposed | Blog - Incode, accessed on November 17, 2025, https://incode.com/blog/top-5-cases-of-ai-deepfake-fraud-from-2024-exposed/

35. Bharatiya Laws Against Deepfake Cybercrime Opportunities and Challenges, accessed on November 17, 2025, https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges

36. Deepfake Evidence and the Indian Criminal Justice System ... - IJFMR, accessed on November 17, 2025, https://www.ijfmr.com/papers/2025/6/60298.pdf

37. 7 Alarming Ways Deepfake Evidence Impacts Court Cases & How to Fight Back - The Kanoon Advisors, accessed on November 17, 2025, https://thekanoonadvisors.com/7-alarming-ways-deepfake-evidence-impacts-court-cases-how-to-fight-back/

38. Summary Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation - National Conference of State Legislatures, accessed on November 17, 2025, https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation

39. Legal Dimensions of Deepfake Technology: Privacy, Consent, and Criminal Liability, accessed on November 17, 2025, https://juriscentre.com/2025/07/27/legal-dimensions-of-deepfake-technology-privacy-consent-and-criminal-liability/

40. Exploring Legal and Technical Challenges of Deep Fakes in India - IJFMR, accessed on November 17, 2025, https://www.ijfmr.com/papers/2024/4/24793.pdf

41. SYNTHETIC MEDIA AND DEEPFAKES: LEGAL CHALLENGES TO SAFEGUARDING INDIAN DEMOCRACY IN THE DIGITAL AGE - Jus Corpus, accessed on November 17, 2025, https://www.juscorpus.com/synthetic-media-and-deepfakes-legal-challenges-to-safeguarding-indian-democracy-in-the-digital-age/

42. Countering non-consensual deepfakes: proposing a legal solution, accessed on November 17, 2025, https://lawschoolpolicyreview.com/2024/08/18/countering-non-consensual-deepfakes-proposing-a-legal-solution/

43. NCW recommends legal definition, penalties under criminal law to ..., accessed on November 17, 2025, https://timesofindia.indiatimes.com/india/ncw-recommends-legal-definition-penalties-under-criminal-law-to-counter-deep-fake-abuse/articleshow/125241763.cms

44. Chasing Deepfakes Across Borders & Protecting Rights - SCC Online, accessed on November 17, 2025, https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/

45. INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES, accessed on November 17, 2025, https://ijlmh.com/wp-content/uploads/The-Role-of-Intermediaries-and-Social-Media-Platforms-in-Curbing-Deepfake-Circulation.pdf

46. India's New IT Rules on Deepfakes Threaten to Entrench Online ..., accessed on November 17, 2025, https://www.techpolicy.press/indias-new-it-rules-on-deepfakes-threaten-to-entrench-online-censorship/

47. India Finally Stands (Tentatively) Up to AI Deepfakes - Ronin Legal, accessed on November 17, 2025, https://roninlegalconsulting.com/india-finally-stands-tentatively-up-to-ai-deepfakes/

48. MeitY invites comments over India's draft rules on deepfakes | Law.asia, accessed on November 17, 2025, https://law.asia/india-deepfake-regulation-draft-rules/

49. India proposes law to label AI-generated social media content, accessed on November 17, 2025, https://coingeek.com/india-proposes-law-to-label-ai-generated-social-media-content/

50. IT Ministry proposes mandatory labelling of AI-generated content on ..., accessed on November 17, 2025, https://www.thehindu.com/news/national/it-ministry-proposes-strict-rules-for-labelling-deepfakes-amidaimisuse/article70189322.ece

51. IT (Amendment) Rules, 2025 | Current Affairs - Vision IAS, accessed on November 17, 2025, https://visionias.in/current-affairs/monthly-magazine/2025-11-12/polity-and-governance/it-amendment-rules-2025

52. India's Deepfake Laws: Where New Rules Win and Fail - Times Of AI, accessed on November 17, 2025, https://www.timesofai.com/news/indias-deepfake-laws-it-act/

53. IAMAI flags 'overreach' risk in draft AI labelling rules - The Financial Express, accessed on November 17, 2025, https://www.financialexpress.com/artificial-intelligence/iamai-

flags-overreach-risk-in-draft-ai-labelling-rulesnbsp/4042445/

54. Decoding the proposed IT Amendment Rules, 2025 - The Leaflet, accessed on November 17, 2025, https://theleaflet.in/digital-rights/law-and-technology/decoding-the-proposed-it-amendment-rules-2025

55. IGAP flags overreach in MeitY's draft deepfake regulations, warns of pre-emptive censorship, accessed on November 17, 2025, https://www.storyboard18.com/digital/igap-flags-overreach-in-meitys-draft-deepfake-regulations-warns-of-pre-emptive-censorship-84182.htm

56. Digital Evidence and Deepfake: A Challenge to Criminal Justice System in India - JETIR.org, accessed on November 17, 2025, https://www.jetir.org/papers/JETIR2508273.pdf

57. Criminal Law in the Age of Deepfakes: A Looming Evidentiary Crisis - Jus Corpus, accessed on November 17, 2025, https://www.juscorpus.com/wp-content/uploads/2025/09/54.-Vibha-Rana.pdf

58. AI-Generated Evidence in IndianCourts: Admissibility and Legal Challenges - law Jurist, accessed on November 17, 2025, https://lawjurist.com/index.php/2025/07/02/ai-generated-evidence-in-indiancourts-admissibility-and-legal-challenges/

59. AI-GENERATED EVIDENCE IN INDIAN COURTS: ADMISSIBILITY, RELIABILITY AND THE CHAIN OF CUSTODY CHALLENGE, accessed on November 17, 2025, https://ijirl.com/wp-content/uploads/2025/09/AI-GENERATED-EVIDENCE-IN-INDIAN-COURTS-ADMISSIBILITY-RELIABILITY-AND-THE-CHAIN-OF-CUSTODY-CHALLENGE.pdf

60. The Authenticity Challenge: Addressing the Concern of Producing Deepfake Generated Media as Evidence in Courts - The Criminal Law Blog, accessed on November 17, 2025, https://criminallawstudiesnluj.wordpress.com/2025/04/05/the-authenticity-challenge-addressing-the-concern-of-producing-deepfake-generated-media-as-evidence-in-courts/

61. Full article: Generative AI and deepfakes: a human rights approach to tackling harmful content - Taylor & Francis Online, accessed on November 17, 2025,

https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2324540

62. In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse - Scholarship Repository, accessed on November 17, 2025, https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1553&context=ijlt

63. High-level summary of the AI Act | EU Artificial Intelligence Act, accessed on November 17, 2025, https://artificialintelligenceact.eu/high-level-summary/

64. Key Issue 5: Transparency Obligations - EU AI Act, accessed on November 17, 2025, https://www.euaiact.com/key-issue/5

65. EU AI Act: first regulation on artificial intelligence | Topics - European Parliament, accessed on November 17, 2025, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

66. Navigating Generative AI Under the European Union's Artificial Intelligence Act - WilmerHale, accessed on November 17, 2025, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20241002-navigating-generative-ai-under-the-european-unions-artificial-intelligence-act

67. China's proposed AI Labelling Regulations: Key points - Norton Rose Fulbright, accessed on November 17, 2025, https://www.nortonrosefulbright.com/en/knowledge/publications/c1211a61/chinas-proposed-ai-labelling-regulations-key-points

68. Article 50: Transparency Obligations for Providers and Deployers of Certain AI Systems | EU Artificial Intelligence Act, accessed on November 17, 2025, https://artificialintelligenceact.eu/article/50/

69. “Deepfakes” and the Criminal Law: Addressing the Rise of AI ..., accessed on November 17, 2025, https://corkerbinning.com/deepfakes-and-the-criminal-law/

70. Government crackdown on explicit deepfakes - GOV.UK, accessed on November 17,

2025, https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes

71. Tackling the regulation of sexually explicit deepfakes | Criminal Law Blog | Kingsley Napley, accessed on November 17, 2025, https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/tackling-the-regulation-of-sexually-explicit-deepfakes

72. Tackling non-consensual intimate image abuse - Parliament UK, accessed on November 17, 2025, https://publications.parliament.uk/pa/cm5901/cmselect/cmwomeq/336/report.html

73. Deepfakes and the Law: Why Britain needs stronger protections against technology-facilitated abuse - Queen Mary University of London, accessed on November 17, 2025, https://www.qmul.ac.uk/law/news/2025/items/deepfakes-and-the-law-why-britain-needs-stronger-protections-against-technology-facilitated-abuse.html

74. Regulating Election Deepfakes: A Comparison of State Laws | TechPolicy.Press, accessed on November 17, 2025, https://www.techpolicy.press/regulating-election-deepfakes-a-comparison-of-state-laws/

75. Tracker: State Legislation on Deepfakes in Elections - Public Citizen, accessed on November 17, 2025, https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/

76. Federal Judge Strikes Down California Deepfake Law, accessed on November 17, 2025, https://www.conference-board.org/research/CED-Newsletters-Alerts/federal-judge-strikes-down-california-deepfake-law

77. China to Regulate Deep Synthesis (Deepfake) Technology from 2023, accessed on November 17, 2025, https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/

78. China's AI Regulations and How They Get Made, accessed on November 17, 2025, https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en

79. China Deep Synthesis Regulation 2025: Essential Guide, accessed on November 17, 2025, https://www.chinalegalexperts.com/news/china-deep-synthesis-regulation

80. Should the United States or the European Union Follow China's Lead and Require Watermarks for Generative AI? - Georgetown Journal of International Affairs, accessed on November 17, 2025, https://gjia.georgetown.edu/2023/05/24/should-the-united-states-or-the-european-union-follow-chinas-lead-and-require-watermarks-for-generative-ai/

81. Singapore's POFMA 2019: Curbing Online Misleadingness and ..., accessed on November 17, 2025, https://facia.ai/knowledgebase/protection-from-online-falsehoods-and-manipulation-act-2019-pofma/

82. Singapore's Fight Against Misinformation | gov.sg, accessed on November 17, 2025, https://www.gov.sg/explainers/singapore-fight-against-misinformation/

83. How Effective is POFMA in Battling Online Falsehoods? - RSIS, accessed on November 17, 2025, https://rsis.edu.sg/rsis-publication/rsis/how-effective-is-pofma-in-battling-online-falsehoods/

84. Deepfakes and Shallow Laws: Regulating Distorted Narratives in the Political Cyberspace - Scholarship Repository, accessed on November 17, 2025, https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1458&context=ijlt

85. Digital Age: Navigating Legal Landscape vis-à-vis Addressing Deepfakes and Manipulated Media - ResearchGate, accessed on November 17, 2025, https://www.researchgate.net/publication/396428693_Digital_Age_Navigating_Legal_Landscape_vis-a-vis_Addressing_Deepfakes_and_Manipulated_Media

86. Deepfakes and Shallow Laws: Regulating Distorted Narratives in the Political Cyberspace, accessed on November 17, 2025, https://repository.nls.ac.in/ijlt/vol19/iss2/4/

87. Using IP rights to protect human rights: copyright for 'revenge porn' removal, accessed on November 17, 2025, https://www.semanticscholar.org/paper/Using-IP-rights-to-protect-human-rights%3A-copyright-O%E2%80%99Connell-

Bakina/e3baec30f479adbd13c1846d4e74c93938e3a50d

88. New laws and penalties for creators and platforms to address deepfakes - IndiaAI, accessed on November 17, 2025, https://indiaai.gov.in/news/new-laws-and-penalties-for-creators-and-platforms-to-address-deepfakes

89. Centre planning new regulations, penalties for both creators and platforms to deal with deepfakes - Deccan Herald, accessed on November 17, 2025, https://www.deccanherald.com/india/centre-planning-new-regulations-penalties-for-both-creators-and-platforms-to-deal-with-deepfakes-2782372

90. Law to regulate deepfake manipulation coming very soon, with penalties for creators and platforms: Vaishnaw - The Times of India, accessed on November 17, 2025, https://timesofindia.indiatimes.com/india/law-to-regulate-deepfake-manipulation-coming-very-soon-with-penalties-for-creators-and-platforms-vaishnaw/articleshow/105461660.cms

91. A Socio-Legal Inquiry on Deepfakes - CWSL Scholarly Commons, accessed on November 17, 2025, https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=2066&context=cwilj