REGULATING SYNTHETIC MEDIA: DIGITAL IDENTITY, PRIVACY, AND THE LAW IN INDIA AND THE UNITED STATES

Dr. Razit Sharma
Assistant Professor
ICFAI Law School, The ICFAI University Dehradun.

ABSTRACT
The creation of AI-generated content raises urgent issues of digital identity and privacy. Instances of AI-generated videos and audio recordings have been employed to impersonate individuals, resulting in cases of identity theft, fraud, and even extortion. This situation poses serious challenges for law enforcement agencies and legal systems, especially in jurisdictions where regulatory schemes are still in the process of development. The Indian legal system does not have a comprehensive approach to address the challenges of synthetic media, creating a wide gap in legal protection for individuals and organizations. This research paper delves into these challenges in more detail, keeping in mind privacy dangers, Indian and American legal contexts as well as regulatory hurdles. Through an evaluation of significant case studies and judicial tendencies, this research paper hopes to shed light on the intricacies of controlling synthetic media amidst unprecedented technological change.

Keywords: AI-generated, Deepfakes, Digital Media, Identity theft, Synthetic media

Introduction

The swift development of artificial intelligence (AI) has given rise to the use of synthetic media, such as deepfakes, AI-created content, and fabricated voices.[1] They have revolutionized digital communication and created opportunities along with challenges. Synthetic media adds creativity and innovation but also raises severe threats to privacy, trust, and security. The continually evolving nature of AI-generated content renders the distinction between original and manipulated media challenging, which is a major source of ethics and law-related issues.[2]

Among the most pressing issues around synthetic media is privacy. Manipulation of content using AI has been used to cause identity theft, unauthorized impersonation, and cyber fraud.[3] Deepfakes, for example, make it possible for cybercriminals to produce highly convincing but fully synthetic videos and voice messages that can be leveraged for monetary scams, reputational damage, and political propaganda. The victims of such manipulations tend to suffer greatly from reputational damage and emotional trauma, which means that there is a critical need for legal protections.[4]

[1] Karen Hao, 'Deepfakes and AI Ethics: Emerging Threats', MIT Technology Review (2021).
[2] Bobby Chesney & Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', 107 Cal. L. Rev. 1753 (2019).
[3] Federal Trade Commission, 'AI and Consumer Protection', FTC Report (2022).
[4] Financial Times, 'Fraudsters Use Deepfake AI to Impersonate CEO', Financial Times (2020).

Loss of public faith in online communication is another imperative matter. Deepfakes or fake news being disseminated on social media, causing people to become more distrusting of information that appears on the internet. On the political front, deepfakes are now being utilised to share manipulated narratives, alter elections, and fuel unrest among the general populace.[5] This trust deficiency not just undermines individuals but democratic institutions, media, as well as civic engagement.

Legally, current frameworks are unable to keep up with the fast pace at which synthetic media is evolving. Cybercrime laws, data protection, and digital ethics differ by jurisdiction, and this creates challenges in enforcement.[6] The Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, offer some protection from digital fraud and identity abuse, but no direct legislation against deepfakes exists in India.[7] By contrast, state-level regulations exist in the United States, with California's AB 730 (2019) and Texas' SB 751 (2019), which sought to limit the use of deepfake technology during elections and revenge porn.[8] At the federal level, however, overall laws on synthetic media are in the proposal stage.

The moral implications of synthetic media also complicate attempts at regulation. Content generated by AI creates issues regarding consent, responsibility, and the right to be in control of one's digital image.[9] Who should be liable for the abuse of synthetic media: AI creators, content producers, or platform operators? It is challenging to allocate responsibility in instances of deepfake misuse due to the absence of definitive legal requirements on AI ethics and responsibility. Furthermore, the balance of free speech freedoms and the regulation of harmful content created by AI is a debated topic, especially in the United States, since the First Amendment restricts how much the government can curtail online expression.[10]

With growing developments in synthetic media, international cooperation in regulation is necessary to confront cross-border legal issues.[11] The European Union's Artificial Intelligence Act, for instance, suggests strict requirements of transparency on AI-created content, such as watermarking and disclosure duties.[12] International standards with the same line of thinking can serve to lower the risks inherent in synthetic media while maintaining its proper applications in entertainment, education, and accessibility.

This research paper delves into these challenges in more detail, keeping in mind privacy dangers, Indian and American legal contexts, moral factors, as well as regulatory hurdles. Through an evaluation of significant case studies and judicial tendencies, this research paper hopes to shed light on the intricacies of controlling synthetic media amidst unprecedented technological change.

Risks to Privacy in Digital Communication

Concerns regarding privacy in digital communications have increased with the emergence of synthetic media. Data misuse, impersonation, and identity theft are some of the most relevant risks of AI-generated content. While AI solutions are bringing forth revolutionary innovations in diverse sectors, their abuse creates

[5] National Institute of Standards and Technology, 'AI-Generated Misinformation and Digital Trust', NIST Research Report (2021).
[6] European Commission, 'Artificial Intelligence Act Proposal', EUR-Lex (2021).
[7] Information Technology Act, 2000 (India); Digital Personal Data Protection Act, 2023 (India).
[8] California Assembly Bill No. 730 (2019); Texas Senate Bill No. 751 (2019).
[9] United Nations, 'AI Ethics and Digital Rights', UN Report (2022).
[10] United States v. Alvarez, 567 U.S. 709 (2012).
[11] Harvard Journal of Law & Technology, 'Global AI Regulation Challenges', 35 Harv. J.L. & Tech. 1 (2022).
[12] European Commission, 'AI Regulation and Synthetic Media Accountability', EUR-Lex (2023).

grave ethical and legal challenges requiring immediate regulatory responses.[13]

Identity Theft and AI-Generated Impersonation

Synthetic media has opened up new methods of identity theft, with attackers using deepfake technology for illegal purposes. Deepfake videos and voice clones created by AI have been utilized to impersonate company executives, celebrities, and politicians. In a 2020 fraud case in the UK, attackers employed AI-generated voice manipulation to impersonate a CEO and convince an employee to transfer $243,000 into a fake account.[14] These instances reflect the advanced methods that cybercriminals use to deceive others using AI.

Furthermore, the ease of access to deepfake tools has led to an increase in AI-assisted social engineering attacks. Cybercriminals exploit synthetic media to gain unauthorized access to financial institutions, manipulate authentication systems, and bypass biometric security checks.[15] Traditional legal frameworks on identity fraud struggle to address the complexities of AI-driven impersonation, necessitating enhanced legal protections and AI detection mechanisms.[16]

Data Misuse and Privacy Violations

AI content is based on large datasets for training purposes, which frequently scrape publicly accessible images, voice samples, and text data without direct consent.[17] This is a major privacy issue for personal data protection and ethical usage of AI. In jurisdictions like the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023, unlawful data harvesting and processing have legal limitations placed on them.[18] It is still lacking in enforcing those laws, though, especially concerning AI-generated deepfakes taken from publicly available sources.

Another hot-button issue surrounded Clearview AI, an American facial recognition startup that aggregated billions of images across social media sites without users' knowledge. Those images were applied for law enforcement purposes, raising privacy-related court battles.[19] The example showed how technology-enabled tools abuse personal information and requires more restrictive regulation to protect against abuse.

Non-Consensual Impersonation and Synthetic Media

One of the most damaging uses of synthetic media is the production of non-consensual deepfake porn. In 2019, an AI-based app called "DeepNude" was launched, which enabled users to create nude pictures of women using publicly accessible photos.[20] The app was rapidly removed after global criticism, but other such tools are still being created, subjecting not only top celebrities but also ordinary civilians to both public and private humiliation.

The legality of non-consensual deepfake materials differs between jurisdictions. Some countries in the United States, for instance, California and Virginia, have criminalized deepfake pornography.[21] Victims of deepfake impersonation in India take legal action based on the Information Technology Act, 2000, but

[13] Karen Hao, 'How AI Deepfakes are Changing Digital Crime', MIT Technology Review (2021).
[14] Financial Times, 'Fraudsters Use AI-Generated Deepfake Voices to Steal $243,000', Financial Times (2020).
[15] Federal Bureau of Investigation, 'Deepfake Technology and Emerging Cybersecurity Threats', FBI Public Announcement (2021).
[16] World Economic Forum, 'AI and Identity Theft: The Future of Cybercrime', WEF Report (2022).
[17] European Parliament, 'AI and Data Privacy: Regulatory Gaps and Solutions', EU Policy Paper (2022).
[18] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 (2016).
[19] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It', The New York Times (2020).
[20] BBC News, 'DeepNude App Sparks Outrage Over AI-Generated Explicit Content', BBC Report (2019).
[21] California Penal Code § 647(j)(4) (2019) (criminalizing deepfake pornography).

deepfake pornography itself is not defined by any particular law as an offense.[22] The absence of a solid legal framework to handle deepfake pornography makes victims find it difficult to delete negative content and identify and prosecute criminals.

The Need for Stricter Rules and AI Detection Tools

With the shocking surge of AI-fabricated fraud, privacy intrusions, and non-consensual deepfakes, legal safeguards and technical countermeasures need to be enhanced. Governments and technology firms are working on AI detectors that can pinpoint synthetic media, yet their performance is still limited as deepfake technology improves.[23] Regulatory action needs to be directed towards compulsory watermarking of AI-created content, more stringent consent for data gathering, and better cybersecurity measures to prevent deepfake fraud.

The subsequent sections will also discuss in greater detail how legal frameworks in India and the United States are responding to these privacy threats and what challenges lie ahead in implementing digital media regulations effectively.

Legal Analysis: India vs. USA

India and the USA have developed their legal frameworks that regulate synthetic media based on increased privacy and security concerns. Despite this, the two jurisdictions also struggle to efficiently regulate AI-produced content. India has mostly depended on sweeping cyber laws like the Information Technology Act, 2000[24], and the Digital Personal Data Protection Act, 2023[25], whereas the United States has followed a more disjointed strategy with state-level legislation and pending federal bills. All this notwithstanding, enforcement issues, jurisdictional questions, and free speech concerns remain important hurdles in both nations.

In India, the Information Technology Act, 2000, is the main enactment dealing with cybercrimes and cyber offenses. Although it was initially intended to deal with old-fashioned cyber fraud and data leakages, provisions of the Act have been so expanded as to include identity fraud and impersonation online.[26] Fraudulent online behaviour under Section 66D of the Act has been criminalized, including identity fraud, and could be so interpreted as deepfake-based impersonation. Additionally, Section 67 prohibits the transmission of obscene material online, which could be applicable in cases involving deepfake pornography.[27] However, these provisions were not specifically drafted to address synthetic media, making their enforcement in deepfake-related cases legally complex. The lack of clear definitions and specific legal guidelines leaves a gap in effectively prosecuting cases of AI-generated media misuse.

Besides the IT Act 2000, the Digital Personal Data Protection Act, 2023, brings more stringent data protection provisions, giving individuals more control over their personal data. This Act follows international privacy legislations like the European Union's General Data Protection Regulation (GDPR).[28]But it has no direct mention of the implications of AI-generated content. The Act deals mainly with personal data protection and data processing laws but does not have direct provisions for synthetic media and deepfakes. The legal lacuna hinders the responsibilities of AI developers and platforms to provide accountability for misuse of AI-generated media impacting people's right to privacy. Judicial precedents have also influenced India's position

[22] Information Technology Act, 2000, S. 67 (India).
[23] Google AI Research, 'Developing Advanced Deepfake Detection Tools', Google Research Blog (2022).
[24] Information Technology Act, 2000 (India).
[25] Digital Personal Data Protection Act, 2023 (India).
[26] Information Technology Act, 2000, § 66D (India).
[27] Information Technology Act, 2000, Sec. 67 (India).
[28] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 (2016).

regarding digital privacy. The pathfinder case of Justice K.S. Puttaswamy v. Union of India, identified the right to privacy as a constitutionally guaranteed right under Article 21 of the Indian Constitution.[29] Though this judgement has played an important role in shaping privacy-specific policies, whether this will also be applicable for synthetic media cannot be determined clearly since deepfakes and artificially created content have still been mostly in an unregulated arena within India.

Conversely, the United States has taken a mixed approach to regulating synthetic media at both the state and federal levels. Perhaps the most important privacy legislation in the U.S. is the California Consumer Privacy Act (CCPA), which provides individuals with the right to know what personal information is gathered about them and how it is utilized.[30] The CCPA, though, does not directly regulate deepfake technology and thus is hindered in enforcing synthetic media privacy. Due to the decentralized system of lawmaking in the United States, other states have moved to enact laws that counteract the abuse of synthetic media. California's California Assembly Bill 730,[31] criminalizes the use of deepfake videos meant to manipulate an election, and Texas' Texas Senate Bill 751,[32] prohibits the use of deepfake content meant to mislead voters. Virginia has also legislated against non-consensual deepfake pornography under, criminalizing the dissemination of AI-created explicit content without permission.[33]

In the federal sphere, the U.S. Congress has tabled numerous bills to control synthetic media, such as the DEEPFAKES Accountability Act in the U.S. Congress.[34] This Act aims to require labeling for AI-created content and create criminal offenses for malicious deepfake usage. Another important proposal is the Honest Ads Act that seeks to regulate AI-created political ads and block election-related disinformation.[35] Yet, even with these legislative proposals, enforcement is a major challenge. The First Amendment to the U.S. Constitution guarantees free speech, and it is challenging to place broad limits on AI-created content without risking constitutional challenges. US courts have already decided on cases involving false speech, for example, United States v. Alvarez, where the Supreme Court held that false statements are normally protected by the First Amendment except when they cause particular harm.[36] This precedent puts into question the degree to which deepfake laws can be enforced without violating free speech rights.

In comparison between India and the United States, both nations have similar enforcement issues regardless of their different legal responses. India does not have a specific deepfake legislation and depends on general cybercrime laws, which might not be adequate to cover the intricacies involved in AI-generated content. The United States has more specific laws at the state level, but it does not have a general federal regulation and therefore has enforcement discrepancies across the various states. The other significant challenge is cross-border jurisdictional challenges, since the AI-based fraud and disinformation are usually from foreign sources, making it tough for prosecution. Moreover, both nations face challenges in balancing privacy protection and free speech concerns, especially when AI-generated material is used for purposes deemed to be satire, parody, or journalism.

[29] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[30] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018).
[31] California Assembly Bill No. 730, Cal. Elec. Code § 20010 (2019).
[32] Texas Senate Bill No. 751, Tex. Elec. Code § 255.004 (2019).
[33] Virginia Code Ann. § 18.2-386.2 (2019).
[34] DEEPFAKES Accountability Act, H.R. 3230, 116th Cong. (2019).
[35] Honest Ads Act, S. 1356, 117th Cong. (2021).
[36] United States v. Alvarez, 567 U.S. 709 (2012).

In response to these legal challenges, policymakers in India and the United States need to strive to create more effective and enforceable laws. India can use a specialized deepfake law that clearly delineates and criminalizes the abuse of synthetic media while making sure that current privacy legislation is adapted to include AI-generated content. The United States, however, requires a more cohesive federal policy on synthetic media regulation to promote consistency across various states. International cooperation will also be important in addressing cross-border AI-generated deception and disinformation. As the synthetic media are global in scope, regulatory authorities have to cooperate with each other to create unified legal standards and enforcement procedures.

With developing AI-generated content, legal instruments have to evolve to cover new threats to privacy while ensuring a balance between technological advancement and human rights. India and the United States have initiated measures to govern synthetic media, but major gaps exist. Legal protection must be enhanced, detection tools for AI must be developed, and ethical AI research should be fostered in order to counteract the threats posed by synthetic media to online communications.

Case Studies in Privacy Infringements: India

The growing maturity of synthetic media has resulted in a number of high-profile cases that demonstrate the privacy threats presented by AI-created content. Ranging from financial scams to election tampering and unwanted deepfake pornography, these case studies give a real-world insight into the challenges presented by synthetic media and the legal nuances involved in solving them.

Deepfake Political Manipulation in the 2019 Delhi Assembly Elections (India)

Another highly publicized case involved the application of deepfake technology in politics. During the 2019 Delhi Assembly election, deepfakes of a high-profile politician were shared in the form of videos, purportedly speaking various languages.[37] Though the original address had been doctored to widen reach across various linguistic sections, the experience did generate ethics-based questions over the manipulation of voters and genuineness of political communication via digital media. The Election Commission of India replied by releasing guidelines against the utilization of deepfake content during campaigns, but the absence of enforceable legal provisions enabled similar practices to continue in future elections.[38]

Indian Politics Deepfake Scandal(2023)

In a more recent example, deepfake technology was applied during India's 2023 state elections, with political leaders' videos being doctored to disseminate misinformation.[39] In some videos, candidates were shown uttering inflammatory remarks they had never made, and this created a lot of confusion among voters. This instance further proved the necessity for strict regulations to prevent AI-based political misinformation in India.[40]

RashmikaMandanna Deepfake (2023)

In November 2023, a deepfake video of Bollywood actressRashmikaMandanna went viral across social media platforms. The video was originally a clip of British-Indian influencer Zara Patel entering an elevator, but her face had been digitally replaced with Mandanna’s using AI-powered deepfake technology. The manipulated video falsely depicted Mandanna in a compromising situation, leading to widespread

[37] Election Commission of India, 'Guidelines on AI and Political Campaigns', ECI Report (2020).
[38] The Indian Express, 'Deepfake Manipulation in 2019 Elections', The Indian Express (2019).
[39] The Times of India, '2023 Elections and AI-Generated Misinformation', TOI Report (2023).
[40] Ministry of Electronics & IT, 'Need for AI Regulation in Digital Elections', Government of India White Paper (2023).

harassment, slut-shaming, and reputational damage.

The video spread rapidly on platforms like Instagram, Twitter (now X), and Telegram, amassing millions of views before being flagged. Mandanna publicly condemned the video, calling it "extremely scary" and highlighting how such misuse of technology could harm anyone. The incident sparked a national debate in India about the dangers of deepfakes and the urgent need for legal safeguards.[41]

Legal and Societal Impact: India

India's legal framework was ill-equipped to handle such cases at the time. While the **Information Technology Act, 2000** had provisions related to cybercrimes, none explicitly addressed deepfake-generated content:

- **Section 66E**: Punished "violation of privacy," but only if the content was captured without consent—not applicable to AI-generated forgeries.
- **Section 67**: Criminalized transmitting obscene material, but deepfake pornography was not explicitly covered.
- **Section 66D**: Addressed identity fraud, but enforcement was weak due to jurisdictional delays and lack of specialized cybercrime expertise.[42]

The case forced policymakers to take notice. India's **Ministry of Electronics and IT (MeitY)** issued an advisory in December 2023, mandating social media platforms to remove deepfake content within **36 hours** of reporting or face penalties under **IT Rules, 2021**. However, critics argued that this was reactive rather than preventive.[43]

Outcome and Reforms

- **No Arrests**: Despite investigations, the original creator of the deepfake remained unidentified, showcasing law enforcement's struggle with digital anonymity.
- **Public Outcry**: The incident led to demands for a dedicated **anti-deepfake law**, with discussions in Parliament about amending the **Digital Personal Data Protection Act (2023)** to include synthetic media.[44]
- **Tech Accountability**: Platforms like Meta and X were criticized for slow takedowns, prompting calls for stricter **AI content moderation policies** in India.

Case Studies: United States of America

Landmark U.S. Case: *United States* v. *Alvarez* (2012)

While not directly related to deepfakes, the United States Supreme Court case of United States v. Alvarez dealt with the boundaries of free speech protection of false statements.[45] The decision stated that false speech is protected by the First Amendment except when it results in direct harm, making it difficult to regulate AI-generated disinformation. The case remains cited in legal arguments regarding regulation of synthetic media in the United States.[46]

U.S. Midterm Elections – Deepfake Voter Suppression(2022)

[41] Deepfake Video of Actress RashmikaMandanna Sparks Outrage, THE INDIAN EXPRESS (Nov. 6, 2023), https://indianexpress.com/article/technology/tech-news-technology/deepfake-video-actress-rashmika-mandanna-outrage-9011025/ (last visited Feb. 7, 2025).
[42] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[43] Ministry of Electronics & IT, Advisory on Deepfake Content (Dec. 26, 2023), https://www.meity.gov.in/content/advisory-deepfake-content (last visited Mar. 17, 2025).
[44] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[45] United States v. Alvarez, 567 U.S. 709 (2012).
[46] Harvard Journal of Law & Technology, 'Free Speech and the Challenges of AI Misinformation', 35 Harv. J.L. & Tech. 1 (2023).

Deepfake misinformation was a point of concern in the United States during the 2022 midterm elections. Videos created using artificial intelligence that showed election officials giving out misleading information about voting circulated on social media, causing voters to become confused.[47] A few videos falsely stated that polling centres had moved to new locations or that certain communities were no longer allowed to vote. This intentional application of artificial media to disseminate misinformation not only undermined the electoral process but also weakened public confidence in democratic institutions.[48] Even with increasing awareness of deepfake threats, implementation of legal provisions like the Honest Ads Act was inconsistent, enabling malicious actors to take advantage of loopholes in regulation.

Deepfake Pornography and DeepNude Case (2019)

One of the most alarming uses of artificial media has been the emergence of non-consensual deepfake pornography. In 2019, a DeepNude application powered by an AI was released, enabling users to generate explicit pictures of women from publicly available images. The app was later removed after mass outrage, but such technologies keep surfacing, and it becomes challenging for victims to stop the unauthorized sharing of their doctored images. Although some US jurisdictions have made deepfake pornography a criminal offense, Indian legal frameworks are still weak, and victims have few options under current cyber laws.

Zelenskyy Deepfake Incident (2022)

There was a 2022 example of deepfake abuse in a geopolitical context, when a simulated video of the President of Ukraine Volodymyr Zelenskyy appeared online with him allegedly surrendering to Russians. The deepfake went viral before it was discredited, showing the use of synthetic media as a method of propaganda and psychological warfare. The incident reiterated the need to create AI-detecting solutions and global coordination to fight malicious synthetic content diffusion.[49]

Taylor Swift AI Porn Case (USA, 2024)

In January 2024, AI-generated explicit images of global pop star Taylor Swift flooded social media, particularly X (Twitter). The images, created using text-to-image AI tools like Stable Diffusion, depicted Swift in sexually explicit scenarios without her consent. The deepfakeswere viewed over 47 million times before being removed, highlighting the viral potential of AI-generated non-consensual intimate imagery (NCII).[50] The incident triggered outrage from Swift's fanbase, women's rights groups, and lawmakers. The White House even addressed the issue, calling for legislative action.[51]

Legal and Regulatory Response: USA

Unlike India, the U.S. had **state-level laws** against deepfake pornography, but no federal legislation:

- **California Penal Code Sec. 647(j)(4)**: Criminalized non-consensual deepfake porn since 2019, but the Swift case originated from unknown jurisdictions.[52]
- **Texas SB 751 (2019)**: Banned malicious deepfakes, but enforcement was patchy.[53]

[47] U.S. Senate Committee on Intelligence, 'Deepfakes and Election Security', Senate Hearing Report (2022).
[48] Reuters, 'AI-Generated Misinformation and U.S. Elections', Reuters Investigative Report (2022).
[49] United Nations, 'AI and the Threat of Synthetic Media in Geopolitics', UN Security Council Brief (2023).
[50]Kalley Huang, AI-Generated Explicit Images of Taylor Swift Spread on social media, N.Y. TIMES (Jan. 26, 2024), https://www.nytimes.com/2024/01/26/technology/taylor-swift-ai-images.html. (last visited Feb. 27, 2025).
[51] Press Release, The White House, Statement on AI-Generated Explicit Imagery (Jan. 27, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/01/27/statement-on-ai-generated-explicit-imagery/. (last visited Apr. 01, 2025).
[52] Cal. Penal Code § 647(j)(4) (West 2019) (non-consensual deepfake pornography).
[53] Tex. Civ. Prac. & Rem. Code Ann. Sec. 143A.001 (2019) (deepfake liability).

- **New York Proposed Bills**: Lawmakers pushed for "Taylor's Law" to criminalize AI-generated NCII at the federal level.[54]

Platform Accountability:

- X eventually removed the images under its non-consensual nudity policy, but critics noted the delayed response (some content remained up for 17+ hours).
- Microsoft (which invests in OpenAI) announced stricter AI content filters for tools like Bing Image Creator.

Outcome and Reforms

- **No Prosecutions**: The creators were shielded by anonymity and cross-border jurisdictional challenges.
- **Policy Shifts**: The case accelerated the **DEFIANCE Act** (federal bill proposing civil lawsuits for deepfake victims).
- **Industry Changes**: Google and Meta pledged to downrank AI-manipulated content in search/algorithms.

Concluding Remarks

These case studies capture the pervasive reach of synthetic media in various fields, ranging from finance and politics to individual privacy. Although regulatory systems exist in US and in many nations try to tackle these issues, yet legal enforcement is a key challenge. The Government of India is in the process of drafting exclusive legislation to address the challenges posed by deepfake technology. Although no statute specifically targeting deepfakes has yet been enacted, policymakers are actively moving toward a comprehensive regulatory framework.

The comprehensive legislative framework must clearly define unlawful uses. It includes the non-consensual intimate imagery, electoral interference, and financial fraud to eliminate ambiguity and facilitate enforcement.

The proposed framework must comprehensively define illegal deepfake uses such as non-consensual intimate content, election interference, and financial fraud. It must fix the clear liability of creators, platforms, and intermediaries with penalties scaled to the severity of harm. Further, the law must require the transparency through mandatory labeling of AI-generated content. To build technical capacity in law enforcement and the judiciary we require advanced forensic tools and specialized training.

However, legislation alone will not suffice. Efforts must be made to foster collaboration among government bodies, industry stakeholders, academic researchers, and civil-society organizations.

Bibliography

Aiyar, Shankkar, *Aadhaar: A Biometric History of India's 12-Digit Revolution* (Harper Collins Publishers India, 2024)

Narayan, Shivangi, *Surveillance as Governance: Aadhaar Big Data in Governance* (People's Literature Publication, 2021)

Solove, Daniel . J., *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, (2007))

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

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)

Windley, P. J., *Digital Identity* (O'Reilly Media, Inc.", 2005)

Citron, Danielle and **Chesney, Robert, "**Deep Fakes: A Looming Challenge for Privacy,

[54] DEFIANCE Act of 2024, S. 4121, 118th Cong. (2024).

Democracy, and National Security", Volume 107, *California Law Review* (December 2019)

Levine**,** Madison Julia, **"**Biometric Identification in India versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States", Vol. 73:618, *University of Miami Law Review* (2019)

Meneses, Joao Paulo, "Seeking to Define Deepfakes from U.S. State Laws", Vol. 37(3), *Communication & Society* (2024)

Pascale, Emily, **"**Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse"**,** Vol. 73:335**,** *Syracuse Law Review* (2023)

Delfino, Rebecca A., "The Deepfake Defense—Exploring the Limits of the Law and Ethical Norms in Protecting Legal Proceedings from Lying Lawyers", Vol. 84:5, *Ohio State Law Journal* (2024)

Miotti, A. and Wasil, A., "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations", (2024), DOI: https://doi.org/10.48550/arXiv.2402.09581

Emilio, Ferrara, "Charting the Landscape of Nefarious Uses of Generative Artificial Intelligence for Online Election Interference", (2024) DOI: https://doi.org/10.48550/arXiv.2406.01862