Strengthening Privacy Laws to Combat Deepfakes: An Evaluation of Current Legal Protection and Future Directions

Nandni Kamal

Student at CHRIST (Deemed to be University), Bangalore

ABSTRACT

Deepfakes created through artificial intelligence can manipulate images, audio, and videos to mimic real people in fabricated contexts. The proliferation of this deepfake technology poses a tremendous threat to substantial privacy breaches; public trust; security in the digital age. The manipulations have ensued extreme violations of privacy, especially non-consensual deepfake pornography and have contributed to political disinformation and erosion of public trust. This paper critically reviews the existing legal frameworks of deepfakes in terms of privacy protection and the failures in this regard with the current law. It proposes concrete legal reforms, platform accountability, and international cooperation to deal with the threats associated with deepfakes. Finally, the detection and counter-technology also have to be the mainstay of any future legal framework dealing with deepfakes.

Keywords: deepfakes, legal frameworks, privacy

INTRODUCTION

Deepfake technology[1] has ushered in a troubling era of digital manipulation, where audio, video, and images can be seamlessly altered to mimic reality. Initially seen as a fun tool for entertainment, deepfakes have quickly revealed a darker side. People are now worried about the serious consequences they bring, from fake videos of celebrities or politicians to manipulated content that targets everyday individuals. These deceptive creations have the power to distort reality, harm reputations, and fuel the spread of misinformation, with real implications for both personal lives and society as a whole. Worse yet, as this technology becomes more accessible, the potential for misuse grows, threatening to damage public trust and even disrupt democratic processes.

Unfortunately, our current legal system is struggling to keep up. Privacy laws, many of which were written before the rise of deepfakes, don’t fully address the unique threats posed by this technology. Laws around defamation, intellectual property, or data protection often fall short in capturing the full extent of the damage deepfakes can cause.

This paper examines how effective current legal protections are against deepfakes, arguing that privacy laws need to be updated and strengthened to tackle these challenges. It will also explore how future reforms

[1] Shinu Vig, Regulating Deepfakes: An Indian perspective, 17 J. SOC 70, (2024), https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2245&context=jss#:~:text=Indian%20policymakers%20can%20also%20strengthen,distributing%2C%20or%20using%20deepfakes%20for.

can better protect individuals and society from this emerging threat. Advances in AI have enabled the development of deepfakes AI-generated synthetic media with convincing manipulations of visual and auditory content. It was first utilized for entertainment purposes, but it has become a means to commit identity fraud, political manipulation, and nonconsensual pornography. This makes the bad use of deepfakes a direct threat to the privacy of the individual as well as to the integrity of the public institution.

Current legal landscape in terms of **privacy protections** is incapable of countering the emerging nature of deepfakes. More or less, most modern privacy laws were formulated before the emergence of AI-driven media manipulation and are not well-suited to address the nuances of this technology. This paper aims to find out these gaps, assess the possible solutions, and outline future directions for legal reform and also for inter-country collaborations.

WHAT IS DEEPFAKE

Deepfakes refer to artificially generated media that utilize artificial intelligence (AI) methods, especially deep learning algorithms. These advanced technologies allow for the alteration or creation of audio, video, and images, resulting in content that appears highly realistic yet is entirely fabricated. The term "deepfake" is a blend of "deep learning" and "fake," emphasizing the role[2] of AI in the production of such media.

Deepfakes typically employ Generative Adversarial Networks (GANs), which are made up of two neural networks—a generator and a discriminator—that compete against one another. The generator generates fake content, and the discriminator determines its authenticity. This adversarial process gradually improves the quality of the generated media, making it more difficult to detect.

VIOLATION OF PRIVACY BY DEEPFAKES

Deepfakes are a profound attack on individual privacy, most obviously in the form of deepfake pornography created without consent. Women are frequently victims, with manipulated images causing them serious psychological harm and reputational injury.[3] That the material goes viral is an aggravating factor; no victim can control or remove the content from circulation. The recourse to law to correct them is often inadequate, offering little way to restore reputation or vindicate rights.

Threats to Public Trust and Misinformation

It also puts public trust at risk as it reflects in the more political and social narratives.[4] The deepfakes concerning politics - literally, videos of public figures speaking falsely - can easily be used as tools to sway public opinion, especially during an election. Deepfakes spread authenticity goes out of the window, people lose confidence in democratic institutions, and it becomes more challenging to know the truth from falsehood.

Law Enforcement Challenges

Detecting, tracking, and prosecuting the producers of deepfakes is an altogether different challenge for

[2] MIT MANAGEMENT, https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained, (last visited Oct. 6, 2024).

[3] Mika Westerlund, The Emergence of Deepfake Technology: A Review, 9 Tech. Innovation Mgmt. Rev. 39 (2019), https://timreview.ca/article/1282.

[4] Hemangini Singh & Priya Abraham, Exploring the Depth: Ethical and Legal Challenges of Deepfakes, in Emerging Technologies and Ethics in the Digital Era 73 (IGI Global, 2024), https://www.igiglobal.com/chapter/exploring-the-depth/353617.

law enforcement. Since the increasing complexity of deepfakes leaves[5] it beyond the sensitivity of sharp forensic tools to differentiate between authentic and manipulated media with ease, combined with the anonymity afforded by the internet to enable global dissemination of deepfake content, there is little hope of identifying the criminals who produce them. Existing legal frameworks are insufficient in grappling with these new challenges because they were designed to cope with traditional forms of media manipulation.

Cross-Border Jurisdictional Challenges

The viral nature of deepfakes is that they can be created in one jurisdiction and disseminated across international borders in the blink of an eye. It is thus almost impossible to apply national laws against the creators and distributors of deepfakes across international borders. Different countries have various degrees of regulation and even no enforcement at all in some jurisdictions. International cooperation and harmonized legal frameworks are necessary to overcome these jurisdictional challenges in combating the spread of deepfakes.

CURRENT LEGAL PROTECTIONS

Deepfake technology poses significant challenges to privacy, and existing legal frameworks around the world need to be addressed so as to understand the current stance of the laws revolving around the current issue.

Global Insights

The regulation of deepfakes varies among countries and different jurisdictions, being not applicable at all, like in the case of the United Kingdom to have at least some outlines of regulation like in the case of the United States. The United States is currently the biggest market for deepfakes around the globe and the lack of adequate personal privacy regulations makes it the largest risk area. Even after the **National Defense Authorization Act in 2019** requiring the Congress to receive an annual report on deepfake threats related to national security, personal privacy violations and misuse of deepfakes are still left unaddressed. The United States is also regulated by the **California Privacy Rights Act (CPRA)[6].** Besides these, the convention **United Nations Declaration of Human Rights (1948)[7]** hugely regulates the right to privacy of individuals.

The relevant provisions regarding the **Information Technology Act 2000 (IT Act)[8]** of India could be applied to the offenses of deepfakes, especially regarding obscene or explicit content. The IT Act is outdated and not really eligible to the exigent challenges of deepfakes, like the one in question. The General Data Protection Regulation in the EU has very strong data protection, but no explicit laws are found related to deepfakes.

Privacy Laws

The landmark case of **Puttaswamy v. Union of India (2017)[9]** established privacy as a basic right and established a base for digital-era privacy protection. However, neither the **Personal Data Protection Bill,**

[5] Niveditha, Z. H. P., Sharma, S., Paranjape, V., & Singh, A. (2022). Review of Deep Learning Techniques for Deepfake Image Detection. International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering. https://doi.org/10.15662/ijareeie.2022.1102021 .

[6] California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100–1798.199.100 (2020).

[7] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948).

[8] The Information Technology Act, No. 21, Acts of Parliament 2000.

[9] Justice K.S. Puttaswamy (Retd) v. Union of India, (2017) 1 SCC 809 (India).

2023[10], nor the **Digital Personal Data Protection Act, 2023**,[11] introduced and substituted, has discussed or mentioned the topic of misuse or AI-generated media misuse, including deepfakes. In the EU, while the **General Data Protection Regulation (GDPR)** offers some protection with the regulation for processing personal data, it does not fully cover the problems related to deepfakes. Furthermore, there are even provisions of **Bhartiya Nyaya**
Sanhita, 2023[12] that deal with cybercrimes.[13]

CHALLENGES IN THE CURRENT LEGAL FRAMEWORKS

After looking at the current legislation, circling the issue of deepfakes, we need to analyse the gap in the legislation that is present so as, to solve the contemporary problem of privacy violation in the digital age. Which can be divided into two main heads:

Growth in Technological Advancements

Deepfakes' technology is so fast that the development is even more speedier than the laws and other legal mechanisms can adopt and implement modifications. AI tools used in creating deepfakes are easily accessible these days and have made it possible for a layman to produce perfectly realistic deepfakes. Before regulations come into play, new and better techniques keep popping out of the shelf, leaving the current legal mechanism useless.

No Specifically Formulated Laws

Most nations do not have specific laws to target the production and diffusion of deepfakes. General laws against defamation, harassment, and identity theft can sometimes be used, but in most other cases, those prove anything less than even-handed legal protection to address the kinds of harms that are unique to deepfakes. This gap in legislation leaves deepfake technology open to malicious exploitation without much chance of serious legal sanctions.

FUTURE DEVELOPMENT ON LEGAL REFORMS

The need for change in the legal landscape, in a manner of codifying laws taking into account present dangers, is what threats by deepfakes call for.

Strengthening Current Privacy Laws

First, there should be updates to the existing privacy laws and provisions that involve particular details regarding offenses related to deepfakes.[14] There should be amendments in the Information Technology Act of India passed in which there should be deep provisions related to the creation and distribution of deepfakes. Similarly, the existing privacy laws in other jurisdictions also require an update according to the new realities of AI-driven media manipulation. Legislatively, the rise of deepfakes can only be effectively controlled through the formulation of specific laws. Inspired by the **U.S. DEEPFAKE**

[10] Personal Data Protection Bill, 2023, No. _ , Acts of Parliament 2023(India).

[11] Digital Personal Data Protection Act, 2023, No. 7, Acts of Parliament 2023(India).

[12] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

[13] Aaratrika bhaumik, Regulating Deepfakes, Generative AI in India, Explained, The Hindu (Oct. 8, 2024, 6:00 AM), https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-indiaexplained/article67591640.ece.

[14] CORUZANT TECHNOLOGIES, https://coruzant.com/tech/deepfakes-and-the-future-of-personalprivacy/#:~:text=Deepfakes%20represent%20a%20significant%20threat,exploit%20deepfakes%20for%20various%20purposes, (last visited Sept 29. 6, 2024).

Accountability Act,[15] countries should enact laws criminalizing malicious creations and distribution of deepfakes, especially their use for political manipulation and non-consensual pornography. Such enactment must contain a definite definition of deepfake offenses and severe punishment for offenders.

Define Deepfake Offences

There is also an immediate need to define what offense consists. In this regard, the production of non-consented explicit content, fraud and theft based on identity due to deepfakes, or furnishing false information because of political manipulation regarding the use of deepfakes can serve to determine offenses. Given the defined nature of offenses, room will be available for lawmakers to find suitable legal remedies.

The correct response from the administration would be to demand that technology companies design their AI tools in such a way as to introduce "privacy by design" through their own technology development process to ensure protection of privacy. This would prevent the abuse of deepfakes proactively, in turn.

Developing Specific Rules/Regulations for Deepfake Technology

Existing privacy laws need to be further beefed up with the development[16] of new, specific legislation to deal with the new, unique threats posed by deepfakes. Some of them are:

Clear Labeling of Deepfakes by Developers

The government can make developers label their deepfakes clearly, eliminating any ambiguity on who is behind the manipulated media. This would, of course, obviously lessen the chance that this spread of misinformation may occur.\

Liability of Internet Hosts Hosting Websites

Social media platforms, and the like, which host the content of individual internet hosts, bear the responsibility for the deepfakes they host. There should be a requirement to implement detection technology promptly and to remove harmful deepfakes.

New Civil Remedies for Victims of Deepfakes

Introduce new civil remedies for persons affected by deepfakes would include the provisions to file a damages suit and injunctions against further dissemination of such deepfake content.

Collaboration with Stakeholders in Technology

Some of the deepfake challenges require collaboration between governments, technology firms, and civil society. Some initiatives on the cards are listed below:

This will be achieved by the government collaborating with technology companies in developing AI-based detection tools that can with high accuracy point out deepfakes. Then these could be applied to scan most social media feeds, news outlets, and other digital media for harmful deepfakes.

Public Awareness Campaign

Publicity of the public on what deepfakes are should be done.[17] Governments should empower public education and awareness activities so that citizens are equipped and empowered to sift through critically and determine the authenticity of media content so as not to fall victim unintentionally to fake news and propaganda.

[15] Deepfake Accountability Act of 2021, H.R. 2395, 117th Cong. (2021).

[16] Oguzhan Oguz, Deepfakes and Privacy: A Perspective on Legal Regulation, 8 Eur. J. Sci. Tech. Educ. 274 (2020), http://www.epstem.net/tr/download/article-file/3456697 .

[17] World Economic Forum, https://www.weforum.org/agenda/2024/02/4-ways-to-future-proof-againstdeepfakes-in-2024-andbeyond/#:~:text=Future%20challenges%2C%20such%20as%20deepfakes,the%20risks%20we%20face%20toda y (last visited Oct. 6, 2024).

TECHNOLOGICAL SOLUTIONS

Besides, the legal reforms and the need for stronger legislation on the matter as a whole, there is a need to develop reforms and laws specifically around the technological aspect. Which can be the following:

Platforms and AI Developers Control

Social media or video-sharing hosting platforms need to be required to have AI-driven detection capabilities that identify and label the generated synthetic media. Similar to the EU AI Act, a mandatory disclosure requirement in terms of transparency should prevail: if AI generated it or manipulated it, the viewer has the right to know if it is AIgenerated or manipulated content.

Stronger Accountability for Platforms

Legal liability must be enforced for platforms against harmful deepfakes. Mechanism for a fast takedown should be mandated in order for victims[18] to ask for the fast removal of malicious content. Platforms require incentive motivation with early detection mechanism- firstly, to prevent it to go viral.

Technological Detection Solutions

The control over the spread of bad content can be achieved through artificial intelligence-based deepfake detection tools. Governments and private entities must come together to create and implement more advanced detection technologies that will distinguish between deepfakes and real content. These tools must be incorporated into law enforcement strategies in the efforts of finding and putting culprits behind bars when crimes related to deepfakes are committed.

INTERNATIONAL COOPERATION AND HARMONIZATION OF LAWS

It is an issue for the global community as a whole and therefore understanding the importance of cooperation among the countries becomes an important aspect. It is needed to analyse laws like treatise and agreements among the countries to reach a better situation overall. Which can be done in following ways:

Cross-Border Collaboration on Deepfakes

International cooperation will play a critical role in addressing the challenge of deepfakes given the way they are widely distributed worldwide. Countries should strive towards an international agreement or treaty which would outline and standardize how the law views deepfakes, further bringing borderless-ness to enforcement. International cooperation between law enforcement agencies and platforms is needed to contain the dispersal of deepfakes around the world.

From International Legal Systems Lessons

Other countries, for example, U.S., EU, and China,[19] have taken steps to tackle the deep fake issue. Best practices in these systems would be noteworthy to be adopted by other countries. For instance, India can learn best practices from the U.S. DEEPFAKE Accountability Act, the EU's AI Act, and China's emerging cybersecurity laws and adapt them according to its legal and regulatory environment.

CONCLUSION

The rapid spread of deepfake technology throws such unprecedented challenges at the world in terms of

[18] Jack Langa, Deepfakes, Real Consequences: Crafting Legislation to Combat Threats Posed by Deepfakes, 101 B.U. L. REV. 761 (March 2021).

[19] Ramluckan Trishana, Deepfakes: The Legal Implications, ResearchGate (Sept. 27, 2024, 9:29 PM), https://www.researchgate.net/publication/379221500_Deepfakes_The_Legal_Implications.

privacy, public trust, and legal systems. Deepfakes can cause widespread psychological trauma and reputational damage,[20] as well as destabilize democratic processes through misinformation-fueled manipulations. This cannot be said about existing frameworks of law, however, which remain ineffectual in responding to those threats.

Such legislation on deepfakes should be made to criminalize its misuse for personal privacy protection and reviving public trust. Host platforms will need to be responsible for detecting and expelling harmful media; AI developers must be mandated to devise tools that can detect deepfakes within a real-time frame. Cooperation on an international scale is quite essential regarding cross-border deep fake dissemination.

As deepfakes are progressing, so will be the legal and technological responses. Deepfakes will need comprehensive legislation, regulation of platforms, innovation in technology, and international cooperation to address all the harms caused due to them and protect individuals in the digital age.

Collaboration on an international scale is essential to address the cross-border nature of deepfakes. Countries should consider harmonizing their legal[21] frameworks and establishing international agreements to combat the dissemination of harmful deepfakes effectively. Learning from the experiences of jurisdictions like the U.S., EU, and China can provide valuable insights into best practices and effective regulatory approaches.

The future of addressing deepfakes lies not only in legal reform but also in technological innovation. Governments and tech companies must collaborate to develop[22] AI-driven detection tools that can accurately distinguish between real and manipulated media. Public awareness campaigns are also necessary to educate citizens about deepfakes and empower them to critically assess the content they encounter online.

In summary, as deepfake technology continues to evolve, so too must the responses from legal, technological, and societal perspectives. Comprehensive legislation, platform regulation, and international cooperation are vital to mitigate the harms caused by deepfakes and protect individuals in the digital age. By proactively addressing these challenges, we can work towards fostering a more secure and trustworthy online environment.

[20] SCC ONLINE, https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-statusof-tackling-crimes-relating-to-deepfakes-in-india/, (last visited Sept. 26, 2024).

[21] Abhyankar Panth, Deepfakes: A Defamatory Dilemma, 5 INDIAN J.L. & LEGAL RSCH. 1 (2023).

[22] Jack Langa, Deepfakes, Real Consequences: Crafting Legislation to Combat Threats Posed by Deepfakes, 101 B.U. L. REV. 761 (March 2021).