

Can Deepfakes be Leveraged Responsibly?

'Deepfakes' refer to synthetic media content created using artificial intelligence ("AI") techniques. Advanced algorithms analyze and manipulate existing images, videos or audio to produce highly realistic (and often deceptive) content. While deepfake technology raises important concerns about misinformation, identity theft, fraud, privacy infringements and potential misuse, it also promises exciting possibilities in various fields. In fact, it has already begun to demonstrate its transformative potential in several business applications, as discussed later in this note.

LEGAL REGIME IN INDIA

As of date, India does not have a specific law to address deepfakes and AI-related crimes. In a few instances, celebrities and other famous people have relied on their personality rights (*i.e.*, the right to publicity and the right to privacy, respectively) to restrain the misuse of their persona, voice, likeness, etc. with respect to deepfake content. More generally, certain provisions under the Information Technology Act, 2000 ("IT Act") and its rules – including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended ("IT Rules") – could prove useful in this regard. However, the validity of such recently amended rules has been judicially challenged.

Nevertheless, in July 2023, when questioned in Parliament about the transmission of deepfake images on social media platforms, India's Ministry of Electronics and Information Technology ("MeitY") argued that the existing legal regime under the IT Act was adequate for the purpose of addressing current issues related to deepfakes.

RECENT CONCERNS

In November last year, the video of an apparently 'real' individual that resembled an Indian actor – but which was based on an original clip featuring a different person – went viral on social media, followed by similar trends involving deepfake videos of several media and political personalities. Such trends caught the government's

attention, leading to urgent concerns about electoral democracy and the need to regulate such technology.

Over the past few weeks, MeitY has made several efforts and issued [statements](#) related to proposals on regulating deepfakes, along with [multiple advisories](#) and [dialogues](#) in respect of [intermediary liability](#) involving social media and internet platforms. In addition, court [interventions](#) have been sought by, and on behalf of, the public – including a recent [petition](#) demanding appropriate guidelines in this regard.

Forthcoming parliamentary elections will likely affect the proposed [rollout](#) of the Digital India Act – which law, in turn, may include dedicated rules on AI and deepfakes (for a discussion on such governance initiatives, see our previous notes [here](#) and [here](#)). However, more [recent reports](#) suggest that, in the interim, MeitY may further amend the IT Rules in connection with AI and deepfakes, including similar regulatory measures in respect of synthetic content and [loan apps](#).

BENEFITS OF DEEPAKES

Despite important concerns related to their misuse, deepfakes offer unique opportunities for innovation, marketing, education and operational efficiency. Some of these are discussed below.

Enhancing marketing and branding

- 1. Personalized advertising:** Deepfakes enable the creation of personalized marketing content, thereby tailoring advertisements to individual preferences. Such enhanced customer engagement and targeted messaging can contribute to increased conversion rates.
- 2. Celebrity endorsements and influencer marketing:** Businesses can leverage deepfakes to feature virtual celebrity endorsements or create lifelike replicas of influencers. This can create cost-effective alternatives (e.g., obtaining an identity license or permission from the concerned individual to use deepfakes for a specific purpose) to traditional celebrity partnerships, even while maintaining a strong impact on consumer perception. Celebrities and influencers could also use deepfakes as a tool for enhancing their public image and commercializing their personality rights more efficiently.
- 3. Product demonstrations and virtual try-ons:** Deepfakes facilitate realistic product demonstrations and virtual try-on experiences. Thus, customers can visualize products in real-world scenarios, enhancing online shopping experiences.

Improving customer service and communication

1. **Virtual customer service representatives:** Deepfakes can be employed to create virtual customer service representatives, providing human-like interactions. This can produce efficient handling of customer queries and support, contributing to an enhanced user experience.
2. **Multilingual communication:** Businesses which operate globally and/or in scattered geographies can use deepfakes to create multilingual communication tools. This helps overcome language barriers, ensuring effective communication with diverse customer bases.

Streamlining operations, staffing and training

1. **Employee training and recruitment simulations:** Deepfakes enable the creation of realistic training simulations for employees. Such immersive learning experiences can contribute to quicker skill acquisition and improved job performance. Deepfake technology can also be utilized in the recruitment process to simulate interviews and assess candidate suitability.
2. **Virtual board meetings and presentations:** Executives can use deepfake technology for virtual board meetings and presentations, thus overcoming logistical constraints to facilitate remote collaboration.
3. **Talent shortages:** Businesses that face talent shortages could use deepfakes to create virtual personnel or spokespersons, thereby ensuring continuity in marketing and communication efforts during talent gaps.

Innovation in entertainment and creative industries

1. **Digital avatars in gaming and films:** Deepfakes can be utilized to create highly realistic digital avatars for gaming and film industries. In turn, by enhancing visual effects and creating lifelike characters, deepfakes can contribute to the growth of the entertainment sector. Further, the use of deepfakes may be helpful in protecting the privacy of participants during online gaming.
2. **Virtual concerts and performances:** Artists and musicians can use deepfake technology to create virtual concerts or performances. Thus, existing opportunities can be substantially expanded upon, and global audiences can be regularly engaged with.

Education, research and development

1. **Education:** Deepfake technology can be harnessed for multiple applications in the field of education, including with respect to the creation of specialized AI instructors to provide tailored support to students; the simulation of surgeries and other complex procedures to provide hands-on training opportunities for medical students; the development of interactive simulations for role-playing exercises, to name a few.
2. **Prototype testing and simulations:** Deepfakes assist in creating realistic prototypes for testing and simulation purposes. This accelerates product development cycles and reduces costs associated with physical prototypes. This may particularly benefit the enhancement of products that are used for security purposes, e.g., facial recognition and biometric systems.
3. **Market research and consumer behavior analysis:** Gathering insights into potential product preferences and market trends is increasingly important. In this regard, businesses can use deepfakes to simulate consumer behavior for market research purposes.

HARNESSING DEEPFAKE TECHNOLOGY SAFELY AND RESPONSIBLY

By adopting ethical guidelines and stringent security measures, businesses can utilize deepfakes safely and responsibly for a range of applications that contribute to operational efficiency, marketing strategies and overall business growth. Some such measures are discussed below.

Ethical framework and guidelines

Transparent use policies:

1. Businesses should establish clear and transparent policies regarding the use of deepfake technology.
2. Further, they should communicate openly with stakeholders, including customers and employees, about the purpose and extent of deepfake applications.

Consent and privacy protection:

1. Organizations should obtain explicit consent before using deepfake technology for applications involving individuals.

-
2. In addition, organizations need to implement robust privacy protection measures for ensuring that personal information is handled responsibly, in accordance with data protection rules (including those under the IT Act and the IT Rules at present, as well as the Digital Personal Data Protection Act, 2023 and the proposed Digital India Act in the future).

Security measures

Authentication protocols:

1. Companies should implement secure authentication protocols to verify the authenticity of deepfake-generated content.
2. Various commercially available solutions, such as digital watermarking technology and other media verification markers, can be adopted for this purpose.

Blockchain technology:

1. By integrating blockchain technology, organizations could better secure and authenticate deepfake content.
2. Further, businesses need to ensure the integrity and traceability of both content creation and distribution.

Collectively, such security measures may help prevent malicious actors from exploiting the underlying technology for fraudulent purposes.

Employee training and awareness

Ethical use workshops:

1. Organizations should conduct periodic workshops and training sessions for their employees in order to raise awareness about the ethical use of deepfake technology.
2. This involves empowering staff with the knowledge to identify and report potential misuse.

Clear policies for employee-generated content:

1. In addition, organizations need to establish guidelines on the creation and dissemination of deepfake content by their employees.
2. Such policies also need to encourage the responsible use of deepfake technology both within, and stemming from, the organization.

Content verification, monitoring and risk mitigation

Deepfake detection tools:

1. Advanced AI-driven tools that are designed to detect and verify deepfake content should be employed for verifying and monitoring the content generated or hosted by, or on behalf of, an organization.
2. Further, organizations should regularly update such detection systems to stay ahead of evolving deepfake techniques.

Third-party audits:

1. It is also a good idea to engage third-party auditors to assess and verify the authenticity of deepfake content.
2. Independent verification adds an extra layer of security and trust.

Strategy for crisis management:

Despite the adoption of appropriate security measures and ongoing monitoring protocols, deepfakes that are detrimental to businesses, employees and/or customers, might emerge. In such situations, having a templated crisis response strategy may help an affected organization to address the issue expeditiously, which, in turn, could mitigate the extent of damage caused.

1. **Response team:** Organizations should have a designated team empowered with the tools and authority necessary to expeditiously address a potential deepfake crisis.
2. **Communication templates:** Existing, pre-approved templates for immediate communication to the government, media and affected individuals (including employees, vendors, customers and other third parties) in the event of a deepfake crisis may help an organization to swiftly address issues related to misinformation, personal data and/or intermediary liability, as well as reputational loss.

Collaboration with experts

Collaboration with ethical AI researchers:

1. Organizations could partner with ethical AI researchers and domain experts for the purpose of being guided appropriately in terms of responsible deepfake use.
2. Further, organizations could explore channels through which they are able to contribute to, and participate in, ongoing discussions on ethical AI practices.

Industry collaboration:

1. In addition, organizations could collaborate with industry peers to share best practices and relevant insights on ethical deepfake use, as well as for the purpose of staying updated on the latest security mechanisms.
2. Such collaborations could lead to the establishment of industry-wide and sector-specific standards for responsible AI adoption.

CONCLUSION: A BALANCED APPROACH

While the ethical considerations and potential risks associated with deepfake technology are significant and must be acknowledged, businesses are increasingly exploring innovative ways to leverage its positive attributes. From personalized marketing to virtual training simulations, the diverse applications of deepfakes in business showcase their potential to contribute towards growth, foster creativity, and address operational challenges. However, as businesses navigate this transformative landscape, the responsible and ethical use of deepfake technology is paramount to ensure a positive impact on the business ecosystem.

Such safe and responsible use requires a combination of ethical frameworks, robust security measures and ongoing awareness efforts. By adopting transparent policies, ensuring adequate security and collaborating with experts, businesses can harness the potential of deepfakes for innovative applications without compromising ethical standards. As AI technology continues to evolve, businesses must remain vigilant and adapt their strategies accordingly. Responsible use ensures that deepfake technology becomes a valuable tool for businesses without affecting trust or integrity.

*This insight has been authored by **Dr. Deborshi Barat** (Counsel), **Reshma (Vaidya) Gupte** (Counsel) and **Nupur Agrawal** (Associate). They can be reached at d Barat@snrlaw.in, r gupte@snrlaw.in and n agrawal@snrlaw.in, respectively, for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

© 2024 S&R Associates

S&R
ASSOCIATES
ADVOCATES



NEW DELHI

64 Okhla Industrial Estate
Phase III
New Delhi 110 020
Tel: +91 11 4069 8000

MUMBAI

One World Center, 1403 Tower 2 B
841 Senapati Bapat Marg, Lower Parel
Mumbai 400 013
Tel: +91 22 4302 8000