

Deepfake technology and its regulations

December 18, 2022 • vajiramandravi.com



What's in today's article?

- About Deepfake Technology (Meaning, Origin, How it works, Misuse)
- China's new policy measures to curb Deepfakes
- Measures taken by other countries (India, EU, USA)

Why in News?

- The Cyberspace Administration of China, the country's cyberspace watchdog, is rolling out new regulations to restrict the use of deep synthesis technology and curb disinformation.
- One of the most notorious applications of the technology is **Deepfakes**, where synthetic media is used to swap the face or voice of one person for another.

What are deepfakes?

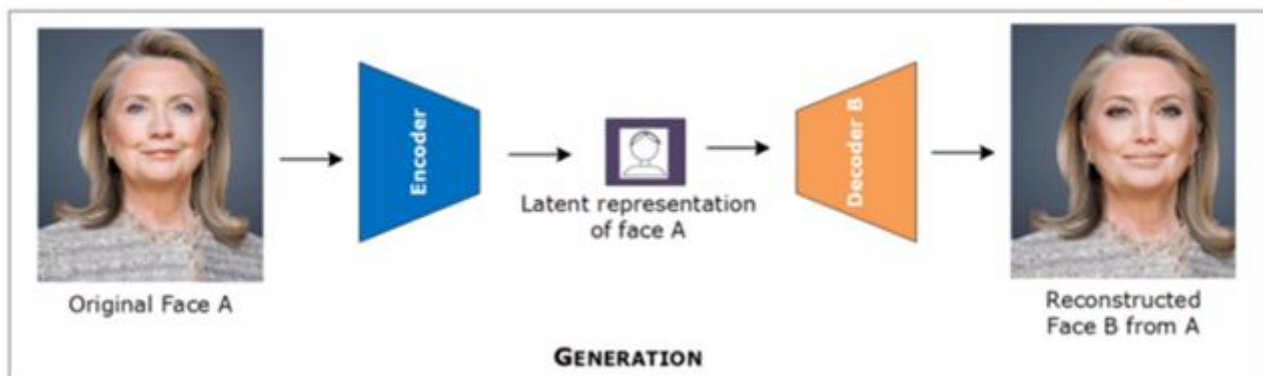


Image Caption: Deepfake Demonstration

- A deepfake is a **digitally forged image or video of a person that makes them appear to be someone else.**
- It is the next level of fake content creation that takes advantage of **Artificial Intelligence (AI)**.
 - Artificial intelligence refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.
- It can create people who do not exist and it can fake real people saying and doing things they did not say or do.

What is the origin of the term?

- The term deepfake originated in 2017, when an anonymous Reddit user called himself “Deepfakes.”
- This user manipulated Google’s open-source, deep-learning technology to create and post pornographic videos.
- The videos were doctored with a technique known as face-swapping. The user “Deepfakes” replaced real faces with celebrity faces.

How this technology is being misused?

- Deepfake technology is now being used for nefarious purposes like –
 - Scams and hoaxes,
 - Celebrity pornography,
 - Election manipulation,
 - Social engineering,
 - Automated disinformation attacks,
 - Identity theft and financial fraud.

- Deepfake technology has been used to impersonate former U.S. Presidents Barack Obama and Donald Trump, India's Prime Minister Narendra Modi, etc.

What is China's new policy to curb deepfakes?

- China's new policy requires deep synthesis service providers and users to ensure that any doctored content using the technology is explicitly labelled and can be traced back to its source.
- The regulation also **mandates people using the technology to edit someone's image or voice, to notify and take the consent of the person in question.**
- When reposting news made by the technology, the source can only be from the government-approved list of news outlets.
- Deep synthesis service providers must also abide by local laws, respect ethics, and maintain the "correct political direction and correct public opinion orientation", according to the new regulation.

What is the need for such policy?

- The Cyberspace Administration of China said that it was concerned that unchecked development and use of deep synthesis could lead to its use in criminal activities like online scams or defamation.
- The new policy aims to curb risks that might arise from activities provided by platforms which use deep learning or virtual reality to alter any online content.
- If successful, China's new policies could set an example and lay down a policy framework that other nations can follow.

What are other countries doing to combat deepfakes?

- **European Union -**
 - The EU has an updated Code of Practice to stop the spread of disinformation through deepfakes.
 - The revised Code requires tech companies including Google, Meta, and Twitter to take measures in countering deepfakes and fake accounts on their platforms.
 - They have six months to implement their measures once they have signed up to the Code.
 - If found non-compliant, these **companies can face fines as much as 6% of their annual global turnover.**
- **United States -**
 - In July 2021, the US **introduced the bipartisan Deepfake Task Force Act** to assist the Department of Homeland Security (DHS) to counter deepfake technology.
 - The measure directs the DHS to conduct an annual study of deepfakes — assess the technology used, track its uses by foreign and domestic entities, and come up with available countermeasures to tackle the same.

- **India -**

- In India, currently, **there are no legal rules against using deepfake technology.**
- However, specific laws can be addressed for misusing the tech, which include Copyright violation, Defamation, etc.

Q1) What are the implications of deepfake?

Deepfakes have potential to create chaos and manipulate public perception makes it a threat, both at individual and societal scales.

Q2) What are the laws against deepfake in India?

At present, India does not have any law specifically for deep fake cybercrime, but various other laws can be combined to deal with it such as IT Act, The Copyright Act, 1957 etc.

Source: Deepfake technology: how and why China is planning to regulate it

Source: <https://vajiramandravi.com/current-affairs/deepfake-technology-and-its-regulations/>

© Vajiram & Ravi. For personal use only.