

Citing Deepfakes, Government to make WhatsApp Disclose Source ID

October 16, 2023 • vajiramandravi.com



What's in Today's Article?

- Why in News?
- About Deepfake
- Origin of the Term 'Deepfake'
- How this Technology is Being Misused?
- What are Countries Across the World Doing to Combat Deepfakes?
- News Summary
- Provision of Disclosing the Identity of a Person under the IT Rules

Why in News?

- The Central government is looking to invoke a law that would require WhatsApp to share details about the first originator of a message.
- The basis for this are multiple deepfake videos of politicians circulating on WhatsApp.

About Deepfake

- 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.

Origin of the Term 'Deepfake'

- 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 are Countries Across the World Doing to Combat Deepfakes?

- **China:**
 - In China, it is mandatory for 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.

- **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.

News Summary

- As the country heads to Lok Sabha elections in 2024, the Central government is looking to invoke a law that would require WhatsApp to share details about the first originator of a message.
- The basis for this are multiple deepfake videos of politicians circulating on WhatsApp.
- The Government is in the process of sending an order to the messaging company under the **Information Technology (IT) Rules, 2021**, seeking the identity of the people who first shared the videos on the platform.
- This would be the first time that the Central government will directly send an Internet platform an order under Section 4 (2) of the IT Rules, 2021.

Provision of Disclosing the Identity of a Person under the IT Rules

- The IT Rules say that online messaging companies will be required to divulge the identity of a person who first sends a particular message on their platform.
- The order for the requirement, colloquially known as traceability, can be passed either by a court, or the government.
- The orders, however, can only be issued for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to national security issues, public order, friendly relations with a foreign government, among other things.
- No order, the rules say, shall be passed in cases where other less intrusive means are effective in identifying the originator of the information.

Stand of WhatsApp

- WhatsApp, which is the most used messaging platform in India, has said that the provision is a threat to its end-to-end encryption system which keeps communications between two people private from even the company itself.
 - It has questioned the technical feasibility of enforcing the measure, saying it will break its security systems and lead to mass surveillance.
-

Q1) What is Machine Learning in simple words?

Machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.

Q2) What are IT Rules in India?

The IT Act regulates intermediaries through a safe harbour model. Under this, they are granted protection from liability for any illegal user-generated content, if they fulfil certain obligations. The IT Rules specify intermediary obligations to claim safe harbour.

Source: [Citing Deepfakes, Government to make WhatsApp Disclose Source ID](#)

Source: <https://vajiramandravi.com/current-affairs/deepfake/>

© Vajiram & Ravi. For personal use only.