VOLUME 4 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ECHOES OF DECEPTION: SAFEGUARDING AGAINST AI VOICE CLONING CYBERCRIMES IN INDIA

- Krish Vikram & Palak Kankani[1]

Introduction

The debate over technology being a boon or a bane is a never-ending one, just like the advancements in technology. While there's always rigorous change in the technological landscape because of which it is never an irrelevant topic of discussion, what makes us contemplate technology right now is the whole AI saga.Artificial Intelligence has surprised us each time with its newer dimensions. From giving directions while using maps to talking to Alexa or Siri, to being recommended movies on Netflix based on your watch history, AI has been taking over. While there are immense benefits of AI to industries such as customer service and entertainment, the ills of AI have been disturbing. Very recently Voice cloning or voice spoofing by AI has been on the rise and this has been effectively harnessed by cybercriminals as yet another way of scamming people.

AI voice cloning is essentially the use of machine learning models[2] to replicate the voice of real human beings and that too, to unbelievable accuracy. This is very different from the synthetic speech of the past which was very robotic, stiff, and unnatural. In a survey of 7,054 Indians, 69% of them said, they couldn't distinguish between an AI voice and a real voice. These voice cloning apps just need minute samples of any person's voice and they can mimic the tone, pitch, accent, and cadence. Apps like ElevenLabs are being used by criminals as a newer variant of phishing.

What is concerning is that, unlike traditional crimes, it is easy to replicate digital misconduct which allows the sharing and repetition of these hostile activities. This has also led to the

[1] Students at Symbiosis Law School Pune

[2] JahnaviSivaram and others, 'Adversarial Machine Learning: The Rise in AI-Enabled Crime' (6 July 2022) <https://papers.ssrn.com/abstract=4155496> accessed 12 November 2023.

© 2023 International Journal of Advanced Legal Research

commercialization of sorts of crime services. So now you don't need to be well trained with the technical know-how of the AI to commit crimes, their commercialization has made it easier to just use ready-made software and attack.

Seriousness of the Threat

To stop this menace from plaguing the world, it is necessary to come up with deterrence and combat this growing threat. Stricter legislation that not only remedies the harms suffered by the victims but also provisions that prevent or inhibit this crime, is the need of the hour. McAfee conducted a survey titled "The artificial imposter" that gave stark data about the systematic scams in India[3]. About 83% of the total Indian victims said they have had a money loss and out of that 48% said they lost over Rs. 50, 000. This gives us a sense of urgency to bring in deterrence because even if one is careful, he may fall prey to this voice cloning method of scamming, where you get a call from a very dear friend or relative in distress asking for money because they're in dire need of it. More than half (66%) of the Indian respondents said they would respond to a voicemail or voice call from someone so close in need of money. This makes it imperative to bring in deterrence at this point.

Threats from AI and voice cloning specifically are many but the most important being an invasion of privacy. Many of us use digital assistants in our homes that are equipped with AI. They run in the background and are lightly listening, usually looking for a prompt for them to respond. In the meantime, they might record little bits of conversation. This is also how your Instagram or Facebook will be filled with advertisements of a cooker if your mom has been bringing up that word very often at home. Apart from that, voices put out on social media and other platforms can also be detected by the AI and can be used by attackers to clone. It was found that some AI service variants need only a maximum of 3 seconds of your voice recording to clone it. This is essentially an individual's data being misused by third parties without their consent and hence is a gross violation of their rights.

[3] 'AI Voice Cloning New Weapon of Cyber Criminals; 83% Indians Report Financial Loss: McAfee Report' (*News18*, 2 May 2023) <https://www.news18.com/tech/ai-voice-cloning-new-weapon-of-cyber-criminals-83-indians-report-financial-loss-mcafee-report-7700359.html> accessed 12 November 2023.

© 2023 International Journal of Advanced Legal Research

Another major threat is financial losses as a result of the phishing scams[4]. In one shocking case in Bhopal, a cyber-fraudster used an AI speech synthesizer to clone the voice of a victim's brother. The thief contacted the victim, posing as his brother, and stated their mother was very ill and required immediate treatment. Deceived by the urgency in the voice that sounded exactly like his brother's, the victim instantly paid Rs. 4.75 lakh to the scammer's account. When the victim later phoned his true brother, he realized he had been duped.

In a recent case where court protected Bollywood actor Anil Kapoor’s right to endorsement by preventing the use of his name, voice, likeness, or any other attribute that makes him unique. AI voice cloning and deep fakes[5] are a direct attack on the rights of a celebrity. This crime is so serious that even international celebrities have been tormented. The same can be seen ina most recent case, Scarlett Johansson, famously playing Black Widow, sued an AI app for featuring an AI-generated version of her voice. This was done using an app called Lisa AI. As AI facilities become easier to access, cases of this sort are only going to increase. While AI’s benefits should not be foregone, it is important to realize that at the moment, its harms are weighing beyond the benefits. A regulatory framework restricting the indiscriminate use of AI is the need of the hour.

Situation in India

The current landscape of cybercrimes involving AI voice cloning in India is worrisome[6]. The number of Indians experiencing these voice cloning crimes (47%) is almost double the global average of 25%. One aggravating factor is the lack of awareness among people. In many rural parts of India, smartphones and the internet are gradually making their way but their use of smartphones is not an informed one. These people become gullible targets for scammers, as in the Bhopal victim example cited above. As was found in McAfee’s reports, India had topped the list of victims of AI voice cloning scams.

The essential problem that India also faces is the lack of adequate legal safeguards on the crime of voice cloning. Even in the Information and Communication Technology Act, of

[4] ‘AI Voice Cloning Aids Cyber-Crimes, Cops Issue Warning against Scam’ *The Times of India* (18 September 2023) <https://timesofindia.indiatimes.com/city/bhopal/ai-voice-cloning-aids-cyber-crimes-cops-issue-warning-against-scam/articleshow/103743850.cms> accessed 12 November 2023.

[5] Naroa Amezaga and Jeremy Hajek, ‘Availability of Voice Deepfake Technology and Its Impact for Good and Evil’, *Proceedings of the 23rd Annual Conference on Information Technology Education* (ACM 2022) <https://dl.acm.org/doi/10.1145/3537674.3554742> accessed 12 November 2023.

[6] Jon Bateman, ‘Scenarios Targeting Individuals’ (Carnegie Endowment for International Peace 2020) <https://www.jstor.org/stable/resrep25783.10> accessed 12 November 2023.

© 2023 International Journal of Advanced Legal Research

2000, or The Personal Data Protection Act, of 2023 no specific provision exists on voice cloning. All that exists are safeguards listed in the copyrights and trademark laws in India, nevertheless, this calls for an urgent need to address the crime of voice cloning by drafting laws that uniquely focus on voice cloning technology and its misuse. Not just the above, but even general awareness of such crimes needs to be raised such that the general populace doesn't fall prey to such offenses. Nevertheless, it's imperative to understand that the very existence of voice cloning should not be affected by any future legislation on the same since there exist several positive benefits from voice cloning such as dubbing, voice assistants, customized marketing, call center usage, etc.

Solutions Recommended

Lastry, it is high time apart from the policymakers; the people also pull their guard up by following the below-stated precautionary measures such as –

- Be Mindful of Voice Recordings: Limit sharing personal voice recordings on public platforms, including social media. Be aware that such recordings can be misused, particularly as training data[7] for AI voice cloning technology.
- Strlengthen Password Security: Create robust and unique passwords for each account. Utilize a mix of characters, numbers, and symbols to make them harder to crack. Consider using a reputable password manager to securely store and manage your passwords.
- Promote Awareness: Stay updated on the evolving landscape of AI voice cloning technology and educate friends and family about potential risks and precautions to take regarding personal voice recordings and online security.
- Use Secure Communication Channels: When engaging in sensitive voice communication, opt for platforms or apps that provide end-to-end encryption. This ensures that your conversations remain secure and private.
- Keep Software Updated: Regularly update your devices and applications to install the latest security patches. Software updates often include essential fixes to guard against new threats.

By implementing these measures, you can significantly bolster your online security and reduce the risks associated with the potential misuse of voice recordings or personal

[7] Luca Cagliero and Alessandro Emmanuel Pecora, 'Data Driven: AI Voice Cloning'.

© 2023 International Journal of Advanced Legal Research

information. Remember, vigilance and proactive steps play a vital role in safeguarding your digital identity and privacy.

BIBLIOGRAPHY

1. ‘Cyber-Crimes: Ai Voice Cloning Aids Cyber-Crimes, Cops Issue Warning Against Scam | Bhopal News - Times of India’ <https://timesofindia.indiatimes.com/city/bhopal/ai-voice-cloning-aids-cyber-crimes-cops-issue-warning-against-scam/articleshow/103743850.cms> accessed 12 November 2023.
2. ‘AI Voice Cloning New Weapon of Cyber Criminals; 83% Indians Report Financial Loss: McAfee Report’ (*News18*, 2 May 2023) <https://www.news18.com/tech/ai-voice-cloning-new-weapon-of-cyber-criminals-83-indians-report-financial-loss-mcafee-report-7700359.html> accessed 12 November 2023.
3. Jahnavi Sivaram and others, ‘Adversarial Machine Learning: The Rise in AI-Enabled Crime’ (6 July 2022) <https://papers.ssrn.com/abstract=4155496> accessed 12 November 2023.
4. Naroa Amezaga and Jeremy Hajek, ‘Availability of Voice Deepfake Technology and Its Impact for Good and Evil’, *Proceedings of the 23rd Annual Conference on Information Technology Education* (ACM 2022) <https://dl.acm.org/doi/10.1145/3537674.3554742>accessd 12 November 2023.
5. Zhaoyu Liu and Brian Mak, ‘Cross-Lingual Multi-Speaker Text-to-Speech Synthesis for Voice Cloning without Using Parallel Corpus for Unseen Speakers’ (arXiv, 26 November 2019) <http://arxiv.org/abs/1911.11601> accessed 12 November 2023.
6. Luca Cagliero and Alessandro Emmanuel Pecora, ‘Data Driven: AI Voice Cloning’.
7. Jon Bateman, ‘Scenarios Targeting Individuals’ (Carnegie Endowment for International Peace 2020) <https://www.jstor.org/stable/resrep25783.10> accessed 12 November 2023.
8. ‘Voice Cloning.Pdf’ <https://ijaem.net/issue_dcp/Voice%20Cloning.pdf> accessed 12 November 2023.

© 2023 International Journal of Advanced Legal Research