

The use of deepfakes can sow doubt, creating confusion and distrust in viewers

May 9 2022, by Sze-Fung Lee and Benjamin C. M. Fung



Credit: Andrea Piacquadio from Pexels

In early March, a [manipulated video of Ukrainian President Volodymyr Zelenskyy was circulated](#). In it, a digitally generated Zelenskyy told the Ukrainian national army to surrender. The video was circulated online

but was quickly debunked as a deepfake—a hyper-realistic yet fake and manipulated video produced using artificial intelligence.

While Russian disinformation seems to be having a limited impact, this alarming example illustrated the potential consequences of deepfakes.

However, deepfakes are being used successfully in [assistive technology](#). For instance, [people who suffer from Parkinson's disease can use voice cloning to communicate](#).

Deepfakes are used in education: Ireland-based speech synthesis company CereProc created a synthetic voice for John F. Kennedy, [bringing him back to life to deliver his historical speech](#).

Yet every coin has two sides. Deepfakes can be hyper-realistic, and [basically undetectable by human eyes](#).

Therefore, the same voice-cloning technology could be used for phishing, defamation and blackmailing. When deepfakes are deliberately deployed to reshape [public opinion](#), incite social conflicts and manipulate elections, they have the potential to undermine democracy.

Causing chaos

Deepfakes are based on technology known as [generative adversarial networks](#) in which two algorithms train each other to produce images.

While the technology behind deep fakes may sound complicated, it is a simple matter to produce one. There are numerous online applications such as [Faceswap](#) and [ZAO Deepswap](#) that can produce deepfakes within minutes.

Google Colaboratory—an online repository for code in several

[programming languages](#)—includes examples of code that [can be used to generate fake images and videos](#). With software this accessible, it's easy to see how average users could wreak havoc with deepfakes without realizing the potential security risks.

The popularity of face-swapping apps and [online services](#) like [Deep Nostalgia](#) show how quickly and widely deepfakes could be adopted by the general public. In 2019, [approximately 15,000 videos using deepfakes were detected](#). And this number is expected to increase.

Deepfakes are the perfect tool for disinformation campaigns because they produce believable [fake news](#) that takes time to debunk. Meanwhile, the damages caused by deepfakes—especially those that affect people's reputations—are often long-lasting and irreversible.

Is seeing believing?

Perhaps the most dangerous ramification of deepfakes is how they lend themselves to disinformation in [political campaigns](#).

We saw this when Donald Trump designated any unflattering media coverage as "[fake news](#)." By accusing his critics of circulating fake news, Trump was able to use misinformation in defence of his wrongdoings and as a propaganda tool.

Trump's strategy allows him to maintain support in an environment filled with distrust and disinformation by claiming "[that true events and stories are fake news or deepfakes](#)."

[Credibility in authorities and the media is being undermined](#), creating a climate of distrust. And with the rising proliferation of deepfakes, politicians could easily deny culpability in any emerging scandals. How can someone's identity in a video be confirmed if they deny it?

Combating disinformation, however, has always been a challenge for democracies as they try to uphold freedom of speech. Human-AI partnerships can help deal with the rising risk of deepfakes by having people verify information. Introducing new legislation or applying existing laws to penalize producers of deepfakes for falsifying information and impersonating people could also be considered.

Multidisciplinary approaches by international and national governments, private companies and other organizations are all vital to protect democratic societies from false information.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: The use of deepfakes can sow doubt, creating confusion and distrust in viewers (2022, May 9) retrieved 23 April 2024 from <https://techxplore.com/news/2022-05-deepfakes-distrust-viewers.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.