# Deepfakes in the metaverse

Deepfakes take the form of face reenactment (where software manipulates an individual's facial features), face generation (where a new face is created that does not relate to a specific individual), face swapping (where one person's face is swapped with another's), and speech synthesis (where voices are re-created). Shallowfakes are similar, but they involve more basic editing techniques.

## How do deepfakes and shallowfakes relate to the metaverse?

By their very nature, deepfakes and shallowfakes are a direct threat to the accuracy of information relating to any individual in the existing digital environment. However, the threat that they pose will only increase as our interactions with the metaverse increase, given that there will be more opportunities for the use of deepfake technology. While many deepfakes have been created as obvious parodies (such as a 2020 deepfake of Richard Nixon announcing the failure of the 1969 Moon landing or the use of deepfakes of Queen Elizabeth II by a UK public service television network in their 2020 "Alternative Christmas Message"), their increasingly convincing nature means that this technology can be used for more troubling purposes. By way of example, in June 2022 it was reported that the mayors of several European capitals had been duped into taking part in video calls with a deepfake of the Mayor of Kyiv, Vitali Klitschko.

## What are the legal issues?

Deepfakes and shallowfakes can be used for the manipulation of pornographic material (for example, revenge porn) and for political purposes (for example, to fake political statements or actions). Such uses (which are just two examples among many) can have an obvious and dangerous impact on the privacy and reputation of individuals. This is particularly the case for those in the public eye, but also more widely.

Deepfakes and shallowfakes can be used to suggest that individuals have made comments or taken part in activities (ranging from the controversial or socially unacceptable to the illegal) when they did not. There are also clear implications for the safety of convictions in the criminal justice system.

On the other side of the coin, the existence of such technology allows wrongdoers appearing in unaltered material to claim that it has been altered – again with potential implications for the justice system and the political landscape – potentially allowing wrongdoers to claim that video evidence is "fake news."

There are a number of ways that the law can tackle deepfakes and shallowfakes. For example:

- Revenge porn could be dealt with under the Criminal Justice and Courts Act 2015.
- The Protection from Harassment Act 1997 may be helpful in some cases.
- The owner of the copyright in the footage used may be able to bring an action for copyright infringement (although in many cases, the owner may not be the individual featured). Deepfakes created for comedic purposes may be protected by the parody exception under the Copyright, Designs and Patents Act 1988, relating to any work that "evokes an existing work while being noticeably different from it, and constitutes an expression of humour or mockery."
- Defamation is a potential route in the case of deepfakes that "lower the claimant in the eyes of right-thinking members of society" or cause such members to "shun or avoid" them provided that serious harm is caused. This would be a viable cause of action for more serious deepfakes, such as those wrongly suggesting that individuals in the public eye have made a statement or carried out an activity that might cause serious harm to their reputation.
- Passing off may be helpful, for instance, where a deepfake is used to fake endorsement of a product.
- Privacy law and the tort of misuse of private information may be helpful where footage not intended for public distribution is used, but the fact that most deepfakes are derived from widely available footage may mean that its use is limited.
- If the deepfake is being used in connection with advertising, the affected individual (including a deceased individual) may have a right of publicity claim within the United States. Right of publicity laws vary by state, with some states, such as New York, California, and Tennessee, extending that protection to after death.

In terms of upcoming changes to the law, the European Parliament recently ratified amendments to the draft EU Digital Services Act (due to come into force in 2023) to require "very large online platforms" to label that footage is a deepfake and inauthentic in a "clearly visible" format. It has however been noted that the UK Online Safety Bill does not appear to include equivalent proposals.

## Authors

**Carolyn Pepper**
Partner
London
cpepper@reedsmith.com

**Jonathan Andrews**
Associate
London
jandrews@reedsmith.com