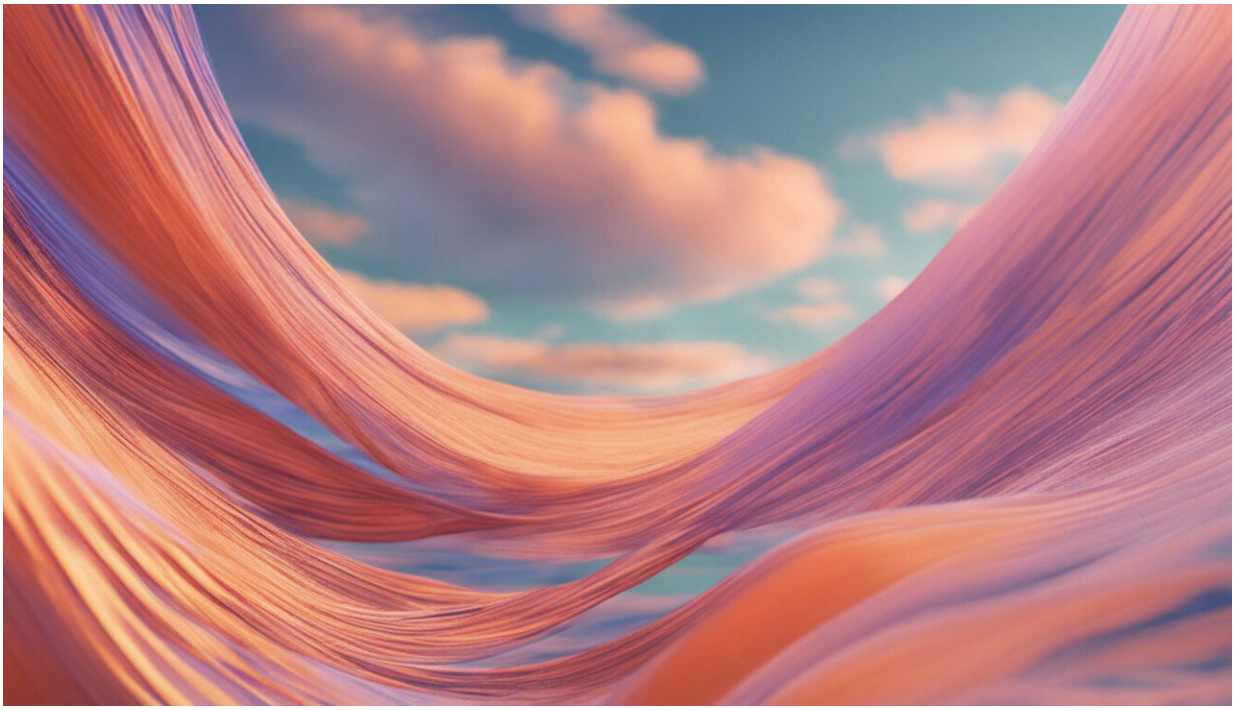
Zao's deepfake face-swapping app shows uploading your photos is riskier than ever

September 6 2019, by Alexandros Antoniou



Credit: AI-generated image (disclaimer)

The latest photo app craze can make you look like a movie star. Zao uses artificial intelligence to replace the faces of characters in film or TV clips with images of anyone whose photo you upload to the app.

The effect is startlingly realistic and shows just how far this sort of

"deepfake" technology has come. But it also highlights how great the risks have become of making your photos available online where anyone can use or abuse them—and the limitation of the law in dealing with this issue.

One of the key problems is the legal right that companies have to use your photos once you upload them to their apps or websites. Several media reports state that Zao's terms and conditions initially gave it "free, irrevocable, permanent, transferable, and relicenseable" rights. A backlash against this has now pushed the company that makes the app, Momo Inc, to change its terms. It says it won't use headshots or videos uploaded by users except to improve the app and won't store images if users delete them from their accounts.

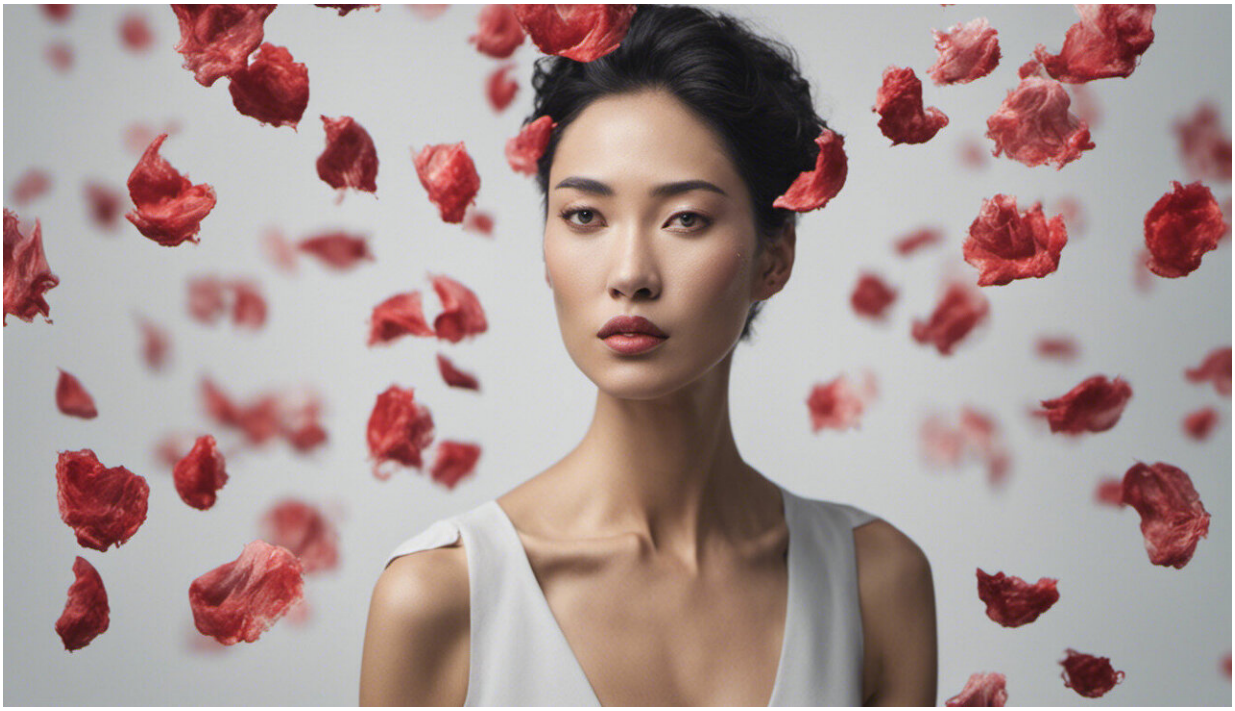
But many other photo applications, such as the age or gender-changing FaceApp, retain similar rights to effectively do whatever they want with the uploaded content. With "a perpetual, irrevocable, non-exclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license," FaceApp essentially gains all of the original owner's rights to the photo (except that it does not have an exclusive license).

These terms are not dissimilar to those of even more popular and mainstream apps such as Instagram, which opens its photo-feed to advertisers. Instagram can let other companies exploit users' photos without any compensation and further pass this right on to a third party without additional permission.

And, of course, you don't even have to give permission for someone to use your photos for them to do so anyway. Once they're online, your images can be circulated without your knowledge. Studies have demonstrated that people's understanding of online privacy settings remains largely limited. If privacy settings aren't sufficient, anyone could access your photos.

This can include journalists, who can republish images from social media without necessarily violating privacy laws if the images have already entered the public domain. Photos are still protected by copyright law but images taken from videos can sometimes be published under "fair dealing" provisions." It is also not uncommon for journalists to use screenshots of the web page on which an image is published, which the publication would not automatically have to remove if a user deleted the original photo.

The development of AI makes the potential consequences of giving up control of your photos even greater. The deepfake technology used by Zao and other apps can create manipulated photos and videos that are very hard to tell from the real thing.



Credit: AI-generated image (disclaimer)

This has already led to deepfake pornography, which involves superimposing someone's face onto explicit images using an AI-based synthesis technique. This type of online abuse can expose victims to financial or emotional blackmail and ultimately cause them serious psychological and emotional harm.

Legal recourse

If you do find your image has been used in ways you never wanted, how can the law help? If it's simply a case of the image being used within the terms and conditions you agreed to (and no other laws have been broken), you probably don't have much recourse. Under the EU's "right to be forgotten," you could ask for your photos to be deleted from a company's servers so they can't make further use of them, although this isn't an absolute right.

But the advent of AI-apps creates another issue. While a company can delete your images from their servers, it may be impossible to remove the related data from AI software that has processed and learned from the pictures. This data may be effectively unavailable but it cannot be truly "forgotten."

There are other ways in which the law seems out of step with the evolution of AI-altered images, particularly when they're used for abusive and offensive purposes. In the UK, the recent law targeting "revenge pornography" only applies to private sexual images, which might not include non-private photographs transposed onto a sexual image of another person.

There might be other options for those who fall victim to the creation of deepfake pornography. The fact that people have been convicted of posting other people's images on pornographic websites shows that the law of harassment can also be relied upon under certain circumstances. It

might also be possible to make claims for misuse of private information, defamation or breach of copyright.

If someone tricks you into granting access to your social media profile and taking photos to generate fake pornographic images, you could also engage data protection legislation. But it's questionable whether civil legal actions such as defamation or privacy suitably recognize the harm that can be done with deepfakes in a way that a specific criminal charge would—and as yet no such charge exists.

The advent of social media has fundamentally challenged our expectations over how we control our photographs. The current patchwork of legal provisions needs to be reviewed to consider the emerging ways images are created and shared without a subject's consent, so that these issues are addressed more widely with a lasting impact. Along with a new regulatory framework for online safety, users need to be educated to appreciate risks of online activity and navigate online spaces responsibly.

Provided by The Conversation