Deepfakes: the implications for business

Published 16 October 2019

Tim Ryan, Partner and Head of Technology and Kelsey Farish, Solicitor, look at deepfake, a nascent technology which poses particular dangers to insurance companies. Deepfakes could potentially be used by unscrupulous claimants to 'prove' liability of an insured defendant.

Earlier this year, in his Worldwide Threat Assessment address to the US senate, Director of National Intelligence Dan Coates listed two threats as more pressing than any other: cyber-attacks and online influence operations. Deepfake is a rising, relatively new, manifestation of subversive digital activity.

The term 'deepfake', a portmanteau of 'deep learning' and 'fake', is commonly used to refer to any artificial intelligence-based human image synthesis technique. Put simply, it's a way to superimpose one face over another – cheaper and more easily than ever before.

Artificial intelligence (AI), which takes many forms, is fundamentally a machine-learning application when a computer fulfils a certain task on its own. The machine is 'taught' to complete tasks that were previously done by humans, by doing the task over and over again.

Several years ago, a new form of AI training known as a generative adversarial network was developed. Using GAN, two adversarial copies of the software compete against one another – one generating the imagery and the other spotting its errors, until it learns the skill with eerie precision and can produce sophisticated artificial images. The technology does of course have legitimate uses, especially in the film industry, where an actor's face can be placed on their stunt double's body.

As with more conventional cybercrimes, as the technology becomes more advanced, so the potential for its misuse increases. And with the software used to generate deepfakes now widely available for free online, the technology is rapidly spreading. Earlier this month, a wildly popular Chinese deepfake app called Zao hit global headlines after going viral. Underlining the potential dangers of the technology, social media platform WeChat quickly banned use of Zao videos and Alipay, the world's largest payment platform, was forced to reassure customers that its systems could not be tricked by the app.

The threat posed by deepfake technology has serious systemic implications. The proliferation of the technology can undermine the trust people have in established government and public institutions such as law enforcement and regulators. It can also undermines the trust people have in each other.

By way of example, a video could purport to show a CEO admitting in a press statement that the company has been hit by a large regulatory fine or class-action lawsuit. If hackers are able to share the video from the company's own website or social media account, it is unlikely that anyone would question the veracity of the deepfake. This could spook customers and investors alike, and cause particular financial harm if the company were listed on a public exchange. Another possible scenario involves a deepfaked conference call, in which an accounts manager asks a subordinate to transfer company money to a new destination, which turns out to be that of the fraudster's.

As with other areas of AI and the wider technology industry, the law hasn't kept up with the development of new tech. Without proper regulation, the potential for genuine harm – to businesses as well as individuals – caused by deepfaking technology in the wrong hands cannot be overstated. While outlawing or attempting to ban deepfakes is neither possible nor desirable, stronger regulation and legislation around AI is a viable option. But until our legislation catches up with the malicious use of deepfakes, firms and individuals will have to be vigilant.

This article was first published in Insurance Day on 20 September 2019.

Authors

Tim Ryan
London - Walbrook
+44(0)20 7894 6978

Kelsey Farish
London - Walbrook
+44 (0) 20 7894 6320

tryan@dacbeachcroft.com

kfarish@dacbeachcroft.com

DAC BEACHCROFT