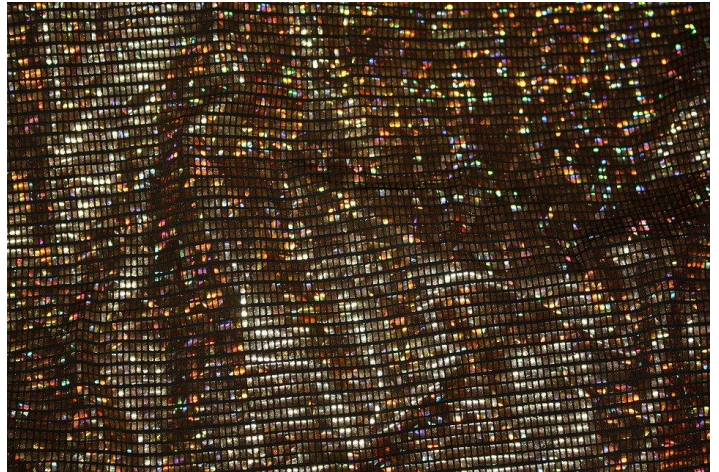


Deepfake it 'til you make it

November 2021

For those of a certain age, or taste, the news that the pop group ABBA will be reforming as digital avatars, to play virtual concerts, was met with the reverence normally reserved for Popes. They are not the first celebrities to have tried it – holograms of Frank Sinatra and Whitney Houston have been doing the rounds for years. Master of understatement Kanye West brought back his then-wife's late father, in holographic form, to tell her that she was



married to 'the most genius man in the world'. So far, so box-office. But as always, the supposed benefits of new technology tend to take the column inches, rather than the threats it poses. Even Kanye would perhaps find the hyping of virtual holographic technology 'Yeezier' said than done.

Leaving aside the moral precedent of whether bringing back a deceased individual to perform actions they cannot possibly have consented to, is something that of which humanity can be proud. The problems posed by its application to still-living individuals are clear. The ability to duplicate, or imitate, someone else without their knowledge is like a thousand Christmases coming at once for bad actors. It need not be full-scale holographic technology. A particularly distasteful and common practice is to place the heads of celebrities on the bodies of adult actresses. But what these 'deepfakes' can do is not only embarrassing and reputationally damaging, but they can also change the tide of politics and business.

In 2020, \$35m USD was moved from Hong Kong to destinations worldwide, including Dubai, after a personal phone call from a company director backed up the email instructions sent to a particular bank manager. The problem was, this voice, which the bank manager recognised as belonging to the relevant director, had in fact been cloned and recreated, and was being used by fraudsters to divert the money. This opens a new front in the phishing wars. Not only can fraudsters use compromised emails to attempt to convince their victims but add an extra layer of apparent verification through vocal, or even visual, recognition. All more marks in the 'convincing' column for how the fraudsters manipulate the situation to their advantage. Particularly as, if the conscientious administrator makes the back-up check to verify the instruction, only to be met by the 'deepfake' persona who assures them that all is well.

Although audio-only reconstruction is far easier to accomplish than a full visual, with the pace of the technological advancement, to say nothing of the potential upscaling in ‘takes’ that can be accomplished by criminal groups who will thus devote more funds and attention to making these a reality, ‘deepfakes’ could become a cottage industry all of their own. This puts risk placing security on a back foot from which it may not be able to fully recover. Already, both humans and ‘smart assistants’ have been fooled by AI-constructed ‘deepfake’ voices, and there have been concerns since 2018 that hostile governments would use full-scale audio- and visual-based ‘deepfakes’ to disseminate propaganda that could swing elections. For instance, making it appear as if a candidate had said something damning when in fact, he had said nothing of the sort.

And all of this ties into Facebook’s recent promotion of ‘the metaverse’ and cut-price Bond villain, Mark Zuckerberg’s assertion that we will some day all be living and working in an entirely interconnected, virtual world. Presumably because he and his billionaire friends will have destroyed the real one. Imagine a metaverse meeting space where an avatar of your boss, who looks and sounds like them, insists on a series of payments or actions – but with no proof at all that they are actually who they say they are. If empiricism is the test of last resort – to trust only what you experience – any aspect of AI, from a vocal ‘deepfake’ to the full-blown metaverse, essentially gives the final deathblow to the idea of evidence and verification. And no amount of dancing Swedish holograms can cover that up. *Voulez-vous?* No thank you.

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world’s most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include:

Corporate Intelligence Services - New market or sector entry research - Know your customer screening

In addition, through our specialist team at KCS IS, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits - providing unparalleled analysis, contingency planning, and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgruppeurope.com or call (00 44) 2072451191.
