WILL 2030 BE REAL?

We've all been warned about deepfakes, but how real, and how imminent is the threat?

Figure 1 *A side-by-side comparison of Chris Ume's Tom Cruise deepfake*

With deepfakes cropping up all over the internet, many people have been perplexed over their use. Are they some harmless fun on TikTok, or do they pose a more sinister threat to society?

The term "deepfake" refers to a video where artificial intelligence (AI) and deep learning—an algorithmic learning method used to train computers—has been used to make a person appear to say or do things.

This video of Tom Cruise originally started on TikTok, but went viral after people worldwide were shocked to find out that it's not Tom Cruise, but a deepfake. In fact, some people still report struggling to believe it's not real due to how authentic the video appears.

The video, however, invites more profound questions. Could somebody's face be misused for crime or identity theft?

On CogX's panel, Henry Ajder, Nina Schick, and creator of the Tom Cruise deepfake, Chris Ume explore such questions in their 'Will 2030 be real?' panel.

Henry Adjer, a leading deepfake researcher, expresses concern that deepfakes may be used for espionage "Malicious use of synthetic media will become a very real and viable cyber threat."

With misuse, Adjer warns of the potential of political disinformation, as citizens may be unable to discern its authenticity. This could have significant political ramifications.

> "Technology is advancing quickly, and one of the features of that is the democratisation"

Furthermore, he highlights of the possibility of 'cheap fakes', created by the everyday person, posing a concerning cyber threat that "will inevitably be weaponised" in a cyber context.

But how much of an imminent threat are deepfakes?

Meanwhile, Chris Ume, creator of the Tom Cruise deepfake above, explains that the answer may not be as straightforward as some might think: "Deepfakes are difficult to achieve such a level of realism and they also require a good actor."

Additionally, deepfakes at this time can only be applied to faces. As such, a young face to an older older body, may be indicative that something isn't quite right. Ultimately, Ume warns society is "just five to seven years away" from regular people being able to make hyper realsitic deepfakes.

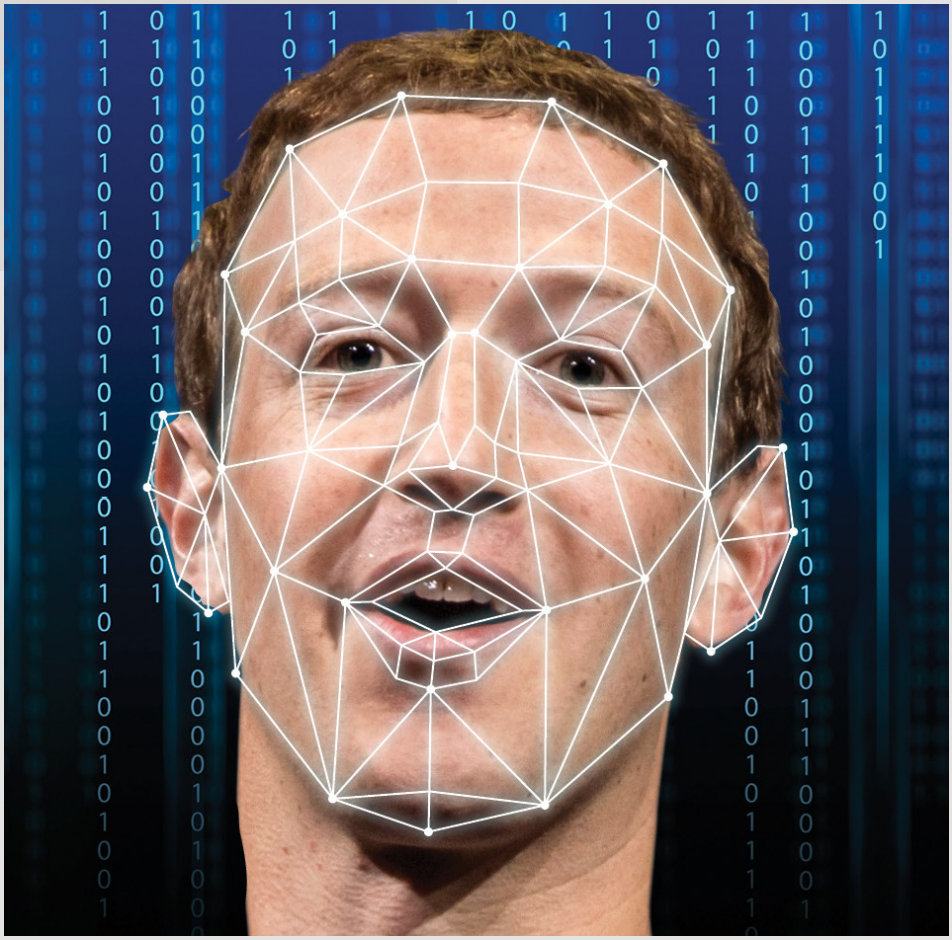
Yet for Nina Schick, author and cyber security/geopolitics expert, there is only one solution:

> "We must prepare. We should get ready"

ELLE FARRELL-KINGSLEY

Figure 2

A closer look into the facial scans behind deepfake technology



By 2030, it is estimted that 90% of video content will be synthetically generated, according to Schtick's research—reflecting the rapidly changing and evolving information ecosystem.

Is there a solution?

Nina proposes two technical solutions to deepfakes:

1. Build an AI to detect deepfakes or synthetic media. This design would use a detection model, as deepfakes would be undetectable to the human eye, and there would be far too much content for humans to sift through. Facebook has been working on a similar solution.

However, she outlines concerns that as soon technology is developed and built, generators will find a way to overcome the system.

"There will never be one size that fits all"

An additional risk outlines the potential that if synthetic material becomes highly sophisticated, that no detector is able to pick it up.

As of 2021, academic researchers are still undecided and often divided on this idea. University College London (UCL) reported that deepfakes are currently the most dangerous form of crime through AI.

2. Content Authenticity

Content Authenticity has been considered by tech software already, as seen by the Content Authenticity Initiative, with the following three steps:

1. Detection

Detection of deliberately deceptive media using algorithmic identification and human-centred verification. A concern, however, is that synthetic content will become faster and better, resulting in these detection techniques struggling to keep pace.

2. Education

Creators must understand ways to use these high-tech creative tools responsibly, and skills must be learned and promoted through media literacy campaigns and formal education. People must become equipped with the tools and knowledge to discern synthetic media and misinformation.

3. Content attribution

Where a tracker is built inside and can track and expose indicators of authenticity so that consumers can have awareness of who has altered content and what exactly has been changed. This ability to provide content attribution for creators, publishers and consumers is essential to engender trust online. However, the legal aspect is conflicted and is thought by researchers to have societal impacts upon privacy.

"Am I harming somebody or their reputation?"

"Am I making somebody say something they would never say?"

Can deepfakes be ethical?

Chris Ume urges ethical standards and regulations to be imposed amongst creators, such as gaining permission from the person whose face is being imitated.

Responsibility also needs to be taken by the creators, who should be asking self-reflective questions such as: "Am I harming somebody or their reputation?"