FACE TIME

Sanjay Gupta *on biometrics: the changing face of facial recognition technology*

From facial recognition scans that unlock our smartphones to medical wearables monitoring our heart rates, biometrics technologies have become a near inescapable part of our daily lives.

For those who'll be lucky enough to travel in the coming years, biometric screenings and contactless travel experiences will quickly become the norm. Across the globe, governments and businesses have put a focus on reducing physical contact where possible. Everything from getting to the airport, to checking in at the hotel, to even ordering a coffee at the café downstairs is being transformed to be as physically distant and safe as possible.

Additionally, many companies and governments have introduced biometric solutions to ensure travellers remain healthy. Holiday goers will quickly get used to this, especially when travelling overseas. Many global airports have enacted a range of biometric solutions – from scanning travellers' temperatures to ensuring their passport identity is correct.

However, our reliance on digital since the start of the COVID-19 pandemic has led to an avalanche of new fraud activity. Now, criminals are using increasingly sophisticated tools to stretch beyond their usual tactics to perpetrate more subtle methods of online crime. When it comes to deepfakes – which often take the form of realistic videos in which a person can be made to say or do just about anything – the best guess is that there are now hundreds of thousands lurking online, with many more criminals possessing the technology to make them. These can be used to hoodwink the screening systems organisations use and gain access to private data, experiences and even physical locations. So, whether it be defending against deepfakes or stamping out synthetic identity fraud, how can organisations protect their consumers' identities from being stolen and used in this way with biometrics?

Over the last few years, Facebook and other social media companies have struggled to control the spread of misinformation and potential harmful dialogue on their platforms. The introduction of deepfakes has complicated the problem further, to the point that many users are no longer able to completely distinguish fact from fiction.

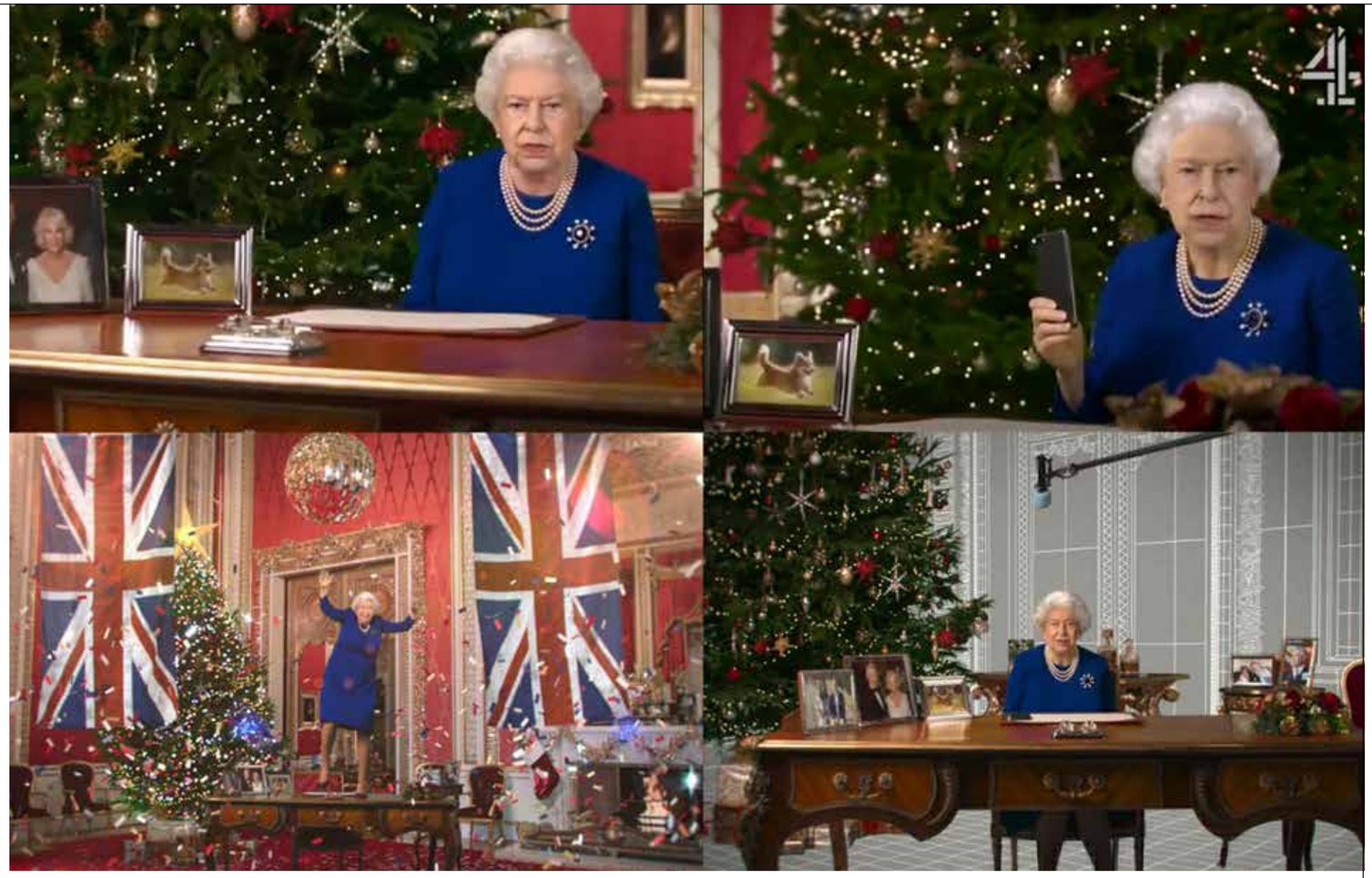
New websites like thispersondoesnotexist.com, which can generate incredibly life-like images in seconds, are compounding the deepfakes problem. The fact that Channel 4's recent deepfakes of Greta Thunberg and the Queen went viral online shows just how incredibly lifelike these manipulated images can look. Fraudsters can essentially transform themselves into these very realistic guises within minutes.

Because of this, younger and more technically savvy demographics will begin to rely less on social media as a source of news and instead return to its original function as a platform for social networking and sharing content. We are already seeing increasing caution among these groups when viewing or sharing content on social sites and that trend will likely continue as misinformation and methods for creating fraudulent content become even more sophisticated in the years ahead.

RELIANCE ON DIGITAL SINCE THE START OF COVID-19 HAS LED TO AN AVALANCHE OF FRAUD

While we understand deepfakes now, the worry is that the threat is only growing. In fact, deepfakes are now being used in conjunction with synthetic identities to provide the photo or video needed to complete the falsified identity when the fraudster is moving through an application process with an app or service. This means deepfakes are starting to infiltrate banks and financial institutions, so preventative technologies need to advance just as quickly.

Encouragingly, the tools to stamp out the threat are on the horizon, in the form of behavioural biometrics. This technology examines how a person types, what words and phrases they often use and even their internet activity to create a unique digital 'fingerprint'. This can then be used to verify an identity or determine if it's a BOT and prevent unauthorised access to devices or documents. For threats intended to bypass physical



Channel 4's Deepfakes of the Queen shows just how incredibly lifelike these manipulated images can appear

biometrics technologies, like deepfakes, behavioural biometrics are likely to be the answer.

Cruel as it is, fraudsters tend to thrive in times of distress and uncertainty, like the global pandemic. The last year has given them the time to perpetrate more subtle, time-consuming methods of identity fraud, like synthetic identity fraud. McKinsey named synthetic identity fraud the US' fastest growing type of financial crime. Synthetic identities used to be difficult to create, but now with AI and machine learning algorithms this type of theft is becoming more commonplace. Not long ago, only large fraud rings had access to this level of technology, but no more.

Here's how it works: obtain a stolen piece of personal identifiable information (PII), ideally one that belongs to someone without much of a credit history, like a young child or someone who is deceased. Download a fake photo of an adult to go with the PII and you are in business. Fake photos are now so good that it is almost impossible to tell the difference between a live person and a digitally created one.

The next step: create a trail of breadcrumbs. Give your synthetic person an email address and make sure they are active on Facebook and LinkedIn. Then use the new fake identity to apply for a credit card, request a loan or open a bank account. In the US, while the bank likely will reject the application, it will send the inquiry to a credit reporting agency, which then will open a profile for that "person", which we call a thin file. Then, fraudsters can apply at different institutions and start to build a more robust credit file.

Fraudsters don't have to look far to find the data they need to get started. Unfortunately, a huge rise in data breaches is the gift that keeps giving – especially those affecting millions, like the Marriott International breach last year. From stolen data, they can craft synthetic identities, using contact details, dates of birth, banking information and more. Advances in AI and machine learning are only speeding this process up, meaning fraudsters can quickly create a unique and believable 'Frankenstein' identity.

To combat the threat, we have to strengthen our defences. Having a new user take a picture of their ID document to match with a selfie, taken using liveness detection, fends off fraudsters – after all, they don't want to commit fraud with a picture of their own face. Link analysis is the other critical defence. This software can look for overlaps in personal information to quickly spot suspicious identities and catch fraudsters in the act. The sooner businesses adopt these defences, the better.

Think of your phone – how often do you access it using facial recognition rather than a password? Many organisations will ask you to do this not just because it's easier, but because the unique patterns of your face are

infinitely more complex than a four-digit passcode. The majority of consumers already prefer biometrics to traditional security measures and – as the technology becomes a regular feature in public spaces – it provides an opportunity for businesses to further highlight how they're protecting their customer's data when they take the bus, shop for new clothes and more.

Now, biometric authentication is leading the charge in the fight against identity fraud. Banks are already using facial biometrics, in conjunction with liveness detection, to verify faces and documents, and ensure fraudsters aren't bypassing screening processes with photos of a photo, for example. But as the capabilities of deepfakes continue to develop, the weapons in a fraudster's armoury could put them ahead of banks' own systems.

BIOMETRIC SCREENINGS AND CONTACTLESS TRAVEL EXPERIENCES WILL BECOME THE NORM

In the next five to ten years, we will see identity verification methods take a 360° approach, with voice biometrics and behavioural biometrics becoming part of the toolbox. Traditional biometric technologies rely on physical parameters, such as facial, fingerprint or retinal features to confirm a user's identity. This is where new innovations come in: either by layering their facial features with their voice and liveness in one fell swoop or by looking at their behaviour – including the way they type, hold their phone or the websites they visit – to create a unique digital fingerprint. In cases when physical biometrics may not be enough to fend off fraudsters, behavioural biometrics can fill the missing gaps. In any case, the more layers, the stronger the defences.

While we will soon see technology advance to a point where it is able to verify a user's identity by analysing how they use their digital device, businesses will never be 100 percent protected. Any product which promised total security would ultimately be unusable by consumers. Instead, risk management is the name of the game. Combining traditional security steps and layered biometrics will give us the strongest chance of forcing fraudsters onto the back foot – especially in our new 'digital-everything' world.

Most people would agree that using biometrics for the purposes of mass public surveillance is problematic. However, when consent is given by users, the benefits to security and digital commerce are enormous. As many consumers lean more toward either contactless or completely digital commerce experiences, the ethical use of biometric ID verification will be even more vital.

It's the value that the ethical use of biometric technology can bring business, which will ultimately drive R&D investment in the space. With legislative moves like the EU's proposed AI regulation, as long as businesses adopt an ethical approach, this shouldn't bring innovation to standstill. While there is a requirement for consumers to 'opt-in', this hasn't diminished the value these technologies provide to businesses. That experience shows that even with explicit opt-in and consumer consent requirements, biometrics can play an important role in pushing safe, frictionless technology experiences forward.

So, what does the future of biometrics look like? It's impossible to know exactly how widescale deployment will unfold in the years to come, but the pandemic is likely to become a catalyst for much broader investment in the technology – for the better of all of us ●

Sanjay Gupta is VP Global Head of Product & Corporate Development at Mitek.

Combining traditional security steps and layered biometrics offers the best chance of beating fraudsters