FACING UP TO THE RACE TO CREATE A MORE SECURE FUTURE

FACIAL RECOGNITION TECHNOLOGY, BEHAVIOURAL BIOMETRICS, BIOMETRIC AUTHENTICATION, HOMOMORPHIC ENCRYPTION AND MORE - ALL ARE VYING TO EMERGE ON TOP AS OUR DIGITAL LIVES COME UNDER EVER GREATER SCRUTINY AND THREAT

Accelerated by the move to hybrid life brought by the pandemic, almost all services and products have shifted online, points out Amir Nooriala, chief commercial officer, Callsign. "This also includes the way we are authenticated, but the problem is that the ways we are authenticated online are based on analogue methods and are not fit for purpose. They are digitised processes that have not been built for the digital world, as highlighted by the amount of fraud and scams that we continue to see in the news agenda. Because of this, it's clear that digital identity is broken and verifying genuine users online isn't working.

"There are solutions the tech industry can put in place to resolve this issue. The NEC's secure biometric authentication technology is a step in the right direction. However, it's important to highlight that static biometrics, such as facial recognition, are only appropriate in some circumstances and will not fix the digital identity problem."

For example, facial recognition shouldn't really be used for day-to-day logins, but rather for step-up checks when nothing else can be verified, no matter how secure the underlying tech might seem, he argues. "Once our facial features are compromised, there is no going back. We cannot get a new face and the fraudsters will own that information. As a standalone method of verification, it is not good enough, because it is not privacy preserving and adds friction to the user journey," adds Nooriala.

STATIC BIOMETRICS

Because of this, organisations must never rely on static biometrics in the user journey, he points out. "Instead, businesses should consider layering contextual data over authentication, such as behavioural biometrics, to ensure consumers can access services quickly, easily, and securely."

Behavioural biometrics considers the behavioural factors of an individual to authenticate them. This includes the device used by the user, how quickly they type, how they hold and swipe their phone or the way their mouse moves on a computer, Nooriala comments. "These contextual attributes learn and adapt with the consumer, as the business relationship progresses. It provides privacy preserving, frictionless, accessible, and inclusive methods to authenticate users in robust and failsafe ways. With all this in mind, it's easy to see why behavioural biometrics is a better authentication method than its physical counterparts to fix digital identity. It's easy for consumers, businesses and governments to use, but, importantly, once consumers understand that behavioural biometrics doesn't use or store personal data, we can expect to see more adoption in these technologies."

NEW RISKS INTRODUCED

Although society has seen drastic improvements in security, thanks to the rise of digital technology, new risks, such as has emerged with impersonation, have also been introduced. This is why biometric authentication technology has become a critical factor in determining authenticity and protecting privacy, says NEC.

"Border controls, airlines, airports, transport hubs, stadiums, mega events, concerts, conferences: biometrics are playing a growing role not only in the real-time policing and securing of increasingly crowded and varied venues worldwide, but also in ensuring a smooth, enjoyable experience for those who visit them." Since the 1970s, NEC has been researching and developing biometrics authentication technologies, such as fingerprint recognition, palmprint recognition and face recognition. NEC has also established technologies in the fields of iris recognition, voice recognition, as well as its original ear acoustic authentication technologies, and supplemented them with AI and data analytics to enhance situational awareness and facilitate effective real-time or post-event action in both law-enforcement and consumer-oriented spheres. NEC uses these biometric technologies under the 'Bio-Idiom' brand in various applications and in effective combinations to realise a world where, it states, "anyone can utilise digital contents safely and securely".

Amir Nooriala, Callsign: businesses should consider layering contextual data over authentication, such as behavioural biometrics.

Jim Close, Kofax: digital identity's strength lies in the way cognitive capture and artificial intelligence technologies are leveraged.

Explains the company: "Face recognition can often prove one of the best biometrics, because images can be taken without touching or interacting with the individual." With the ability to process and analyse multiple camera feeds and thousands of faces per minute, the company adds that its face recognition is able to "police the largest and most difficult security challenges with efficiency, sensitivity and perception".

ENCRYPTED FACE INFORMATION

Meanwhile, NEC has developed a biometric authentication technology that allows users to authenticate themselves with encrypted face information. This technology reduces the risk of misuse, it states, if face information is leaked and contributes to the expansion of safe and secure biometric authentication use cases. "With the application of this technology, all face information handled by service providers is encrypted. Therefore, even if encrypted face information is leaked, the risk of being misused for spoofing is low. Moreover, since users have a secret key for decryption, service providers cannot decrypt face information, enabling users to take advantage of the face recognition service with peace of mind."

Face recognition is increasingly being introduced as a means of identity verification, but, in the unlikely event that registered face information is leaked, it may lead to misuse, such as spoofing. "As a result, greater attention is being paid to technologies that perform biometric authentication while encrypting information, such as face information," states NEC. One such technology it singles out, is 'homomorphic encryption'. This cryptographic technology, which can perform operations such as addition and multiplication while encrypting data, is known to perform authentication processing while biometric features are encrypted - and without deteriorating the accuracy of certification.

However, homomorphic encryption can only perform simple operations and processing speed is greatly reduced when performing the complex processing required by biometric authentication. As a result, it has been limited to '1:1 Identification', which is used for logging into online services with relatively light processing. Conversely, the method has been difficult to apply for '1:N Identification', such as facility entry control and transaction settlements, which require greater processing speed.

In order to overcome this challenge, NEC developed a secure biometric authentication technology that can be applied to 1:N Identification by streamlining the processing of face recognition using homomorphic encryption. Conventionally, 1:N Identification has required authentication processing that includes complex arithmetic operations that are difficult for homomorphic encryption. However, this technology is said to reduce processing by focusing on promising candidates through simple operations, rather than processing all registered users.

"This narrowing down greatly reduces the number of authentication operations, including complex operations, so that 1:N Identification can be performed at high speed, even with homomorphic encryption," reports NEC. "With 1:N Identification for

10,000 registered users, for example, NEC's new technology can narrow down the number of user candidates in about 0.01 seconds. If the system narrows down the number of candidates to about 1% of the total number, it can perform face authentication processing in a speed of about 1 second. In addition, the use of this technology does not impact the accuracy of certification. "

Going forward, NEC will further develop this technology, it confirms, combined with Bio-IDiom (the company's portfolio of biometric authentication technologies), "in order to enhance the safety and security of personal information, entrance control, transaction settlements and more".

PASSING UP PASSWORDS

For Rob Watts, CEO, Corsight AI, passwords are now very much a thing of the past. "Why do we need them when we all have a face? We are already seeing the preference for biometric authentication on our mobiles and it's predicted that facial recognition hardware will be present in 90% of smartphones by 2024. The general public does not see a difference between cyber and physical security, they simply want to go about their daily lives in a safe and secure way. So, why does the technology industry insist on creating siloes, when biometric is far safer for the citizen?"

It is predicted that the total addressable market for facial recognition technology (FRT) is set to experience 12.4% CAGR from 2021 to 2025, growing by $3.78 billion. The explosion here is based upon personal biometrics used on mobile and FRT use at the edge. "The traditional use of facial recognition for security and surveillance will be overwhelmed by personal consumer use," he says. "However, as cybercriminals become increasingly sophisticated with their targets and tactics, end-users will need to ensure that the security of the biometric data in their systems is a top priority, in order to avoid situations where data is compromised." For the financial sector, multi-factor authentication that pairs facial recognition with passwords and codes is a popular solution. "Yet the more sophisticated version of this, gaining traction over the next few years, is dual analytics - pairing behavioural biometrics (like gait or mouse use characteristics) with voice and face recognition, for instance - to mitigate risks of spoofing or fraud."

Ultimately, adds Watts, the speed and accuracy of FRT has come on in leaps and bounds over recent years "and the future of biometric authentication lies in its capability to accurately recognise faces in challenging environments: with masks on, from high angles and in low lighting. Getting it right and having the highest accuracy is where customers will gain confidence. While developers are now also ensuring software is secure by design and secure by default, transparency from organisations leveraging biometric data - in how it is captured, stored and protected - will be key to greater adoption moving forward. Security and personal biometrics using FRT is the future for us all".

States Jim Close, regional vice president of enterprise at Kofax, the need for a digital solution to safe, secure authentication of identity has gained urgency over the last couple of years. "Cyber security in general is a major worry for companies and employees alike, but the pandemic and adoption of remote work has put the risk of identity theft in stark relief. As corporations accelerate their digital transformation initiatives to support hybrid work, they'll have to rely on emerging technologies to ensure privacy and security of employee information."

One option he also endorses is digital identity. "In fact, widespread adoption of this chip-based approach is already well underway. Seventy countries have set up a national ID scheme and most are using electronic national ID cards. In addition, there are more than one billion users of digital identity apps today, and that number is expected to jump to more than 6.2 billion by 2025, according to a recent study.

"While some may be wary about digital identity, modern technology has made this option very secure," he insists. "A key reason is the digital identity trust framework requires all providers to use encryption and set up a security governance framework. As a result, digital identity presents a significant obstacle to fraud. Its strength lies in the way cognitive capture and artificial intelligence technologies are leveraged. A combination of multiple data sources, various digital and biometric attributes, behavioural user data and more work together with these advanced technologies to validate and authenticate a user's identity in seconds, while also identifying anomalies that may indicate the possibility of fraud."

"Another advantage he singles out is that digital identity allows users more control over their data. "For instance, if a consumer is using the digital wallet to purchase tobacco or alcohol, they can choose to only share that portion of information in their identity wallet. When the amount of personal data that needs to be exchanged is minimised during transactions, it reduces the reliance on third parties and enhances security by removing a player from the equation. Perhaps even more crucially, when individuals are the arbiters of the attributes used to create their identity, they gain a higher level of trust and confidence in the technology.

"There are numerous use cases for digital identities, from account creation and website logins to age verification and know-your-customer certification. Most importantly, this many-layered approach offers organisations an effective and robust way of keeping company, and individual data and information, safe and secure," he concludes.