ELSEVIER

biometric TECHNOLOGY TODAY

ISSN 0969-4765 June 2020

www.biometricstoday.com

COVID-19 THREAT

Biometrics vendors point way to Covid-19 'immunity passports'

Biometric technology is driving global efforts to develop Covid-19 'immunity passports' that could enable people to prove they have recovered from the virus, escape lockdown and so help national economies restart after the pandemic.

In the US, biometric identity specialist CLEAR last month launched a 'Health Pass by CLEAR' system, which enables businesses to screen their employees and customers for the coronavirus. The system allows enrolled users to identify themselves via a phone selfie, but tied to their health profile – meaning individuals can be health-checked before being allowed to enter their workplace, or shops, restaurants and sports venues. CLEAR said that in future the Health Pass could build in factors like coronavirus test results and vaccine status – potentially providing the user with a Covid-19 'immunity passport'.

Users will be able to download the CLEAR app on their smartphones and enrol in the service for free by verifying their identity using facial recognition. To enter a business or venue that employs Health Pass, users will snap a selfie to authenticate their identity and take a health quiz on possible Covid-19 symptoms. The company says that it plans for users to be able to link Covid-19 test results with their digital identity in the future.

In the UK, biometrics vendor iProov has launched a facial recognition front-end for a core National Health Service (NHS) app which allows citizens to order prescriptions, book appointments and access medical data online. And iProov founder Andrew Bud told the *BBC* this system could potentially be used as the basis for Covid-19 immunity tests, opening a route to immunity passports.

He said: "NHS Digital has built a strong and trusted identity system in NHS login, which, in my opinion, should form the basis of the UK's immunity passport. Whether they do so is a decision for them." NHS Digital said it is not currently applying the technology to any other purposes beyond secure login.

The NHS app now uses iProov's Flashmark facial verification system in England to allow Android and iOS device users to submit their selfie, then log into the app via their phone and access all the services. More than 1 million UK citizens have registered with NHS login, with a peak of over 60,000 new IDs verified during the first week of April.

Immunity passports would work by securely linking a person's identity to their coronavirus test results. Estonia has begun testing an immunity passport, based on technology developed by Transferwise. And the *Financial Times* has reported that a number of European start-up tech companies are racing to develop Covid-19 passports.

They include Onfido, which recently raised $100 million extra financing (see *BTT*, May issue). Onfido CEO Husayn Kassai told the *FT* that his company is actively considering how to adapt its existing anti-fraud systems for immunity passports. Onfido uses AI facial recognition systems to authenticate photo IDs and other identity documents. The *FT* also identified other UK biometric tech vendors such as VST Enterprises and Centre Pass Enterprises as active in this area.

But the use of biometric authentication to counter Covid-19 long-term has raised fears over privacy and security.

CLEAR's Health Pass has come under fire from two US lawmakers, Senators Jeff Merkley and Cory Booker, who have called on the company to detail what privacy and security steps it is taking to protect the data. In an open letter to CLEAR CEO Caryn Seidman Becker, the Senators acknowledged CLEAR's "potential benefits" but warned of the risk of "undetectable, constant government surveillance" from over or misused facial recognition technology. They

Continued on page 2...

Contents

Editorial Office:
Elsevier Ltd
The Boulevard
Langford Lane
Kidlington
Oxford OX5 1GB, UK
Tel: +44 1865 843239
Email: timring@ntlworld.com
Website: www.biometricstoday.com

Publishing Director: Sarah Jenkins

Editor: Tim Ring
Email: timring@ntlworld.com

Production Support Manager: Lin Lucas
Email: l.lucas@elsevier.com

Subscription Information
An annual subscription to Biometric Technology Today includes 10 issues and online access for up to 5 users. Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/biometric-technology-today/0969-4765

12985
Digitally Produced by
Mayfield Press (Oxford) Ltd

...Continued from front page

cited the recent hack of US-based Clearview AI, which offers a database of over 3 billion faces to police forces worldwide (see *BTT*, March issue).

In Europe, a coalition of 44 privacy campaign groups, the European Digital Rights (EDRi) alliance, last month called on all EU countries to ban biometric mass surveillance – and specifically warned against introducing health surveillance systems under the guise of combatting Covid-19.

EDRi said: "There is a real risk the damage caused by widening surveillance measures will last long after the pandemic is over. For example, will employers remove the cameras doing temperature checks in offices after the pandemic?" Lotte Houwing, policy advisor at EDRi member Bits of Freedom, added: "It is of utmost importance that we do not let the Covid-19 crisis scare us into a mass surveillance state. Surveillance is not a medicine."

Addressing immunity passports specifically, Dr Tom Fisher, a senior researcher at campaign group Privacy International, told the *BBC* that the introduction of any such measures needed to be "necessary, proportionate and based on the epidemiological evidence. For the moment, immunity passports do not meet this test."

• The Biometrics Institute has spotlighted the efforts of 19 leading biometric tech suppliers who have pioneered solutions and ideas to help counter Covid-19. Their products range from secure election e-voting and user verification in healthcare to contactless payments and remote onboarding, evaluating air traveller temperatures and retrofitting fingerprint readers with disinfecting technology. They also feature technology to reduce virus spread in offices, hospitals, airports and secure locations which rely on fingerprint readers, card access or manual processes. "Our community has proved themselves to be agile and versatile in coming up with answers to the new questions the world is being asked," said Institute chief executive Isabelle Moeller.

The 19 vendors are Auraya, Biometix, FaceTec, G+D Mobile Security, ID R&D, Ideco, IDEMIA France, IDEMIA US, InnoValor, Innovatrics, JENETRIC, Peoplekey, Phonexia, Regula Baltija, TECH5, Trust Stamp, Unisys, Vision-Box and WorldReach.

FINGERPRINTING

NIST pans touchless print scanners, but using more fingers helps

The US National Institute of Standards and Technology (NIST) has tested six major contactless fingerprint scanning systems – and found they perform far worse than conventional devices that require physical contact.

The NIST report, published last month, examined the performance of six – unnamed – commercially available systems: four mobile phone-based apps and two stand-alone contactless devices. It tested them on fingerprints from 200 volunteers and found that all six "performed comparatively poorly" when scanning any single finger, showing 60-70% accuracy. In contrast, the match accuracy of contact devices is typically better than 99.5%.

The results will dent the hopes of contactless fingerprint device vendors trying to win over concerned users, as the Covid-19 pandemic drives companies to switch to contactless biometric systems for safety reasons. NIST carried out its test before the virus appeared, so did not examine hygiene specifically.

One positive for touchless device vendors is that NIST found that when these devices scanned multiple fingers on a hand, they produced nearly 90% accuracy, and one of the mobile apps scored 95%. "Our data suggests that multiple finger matching can substantially improve the accuracy of contactless fingerprint matching," said John Libert, one of the report's authors.

He added: "One purpose of the research was to test the hypothesis that multiple finger matching can substantially improve the accuracy of contactless fingerprint matching. Our data suggests it can."

NIST pointed out that contactless acquisition of fingerprints happens in a fundamentally different way from contact capture. Pressing the finger onto a flat surface turns its print into a 2D object, representing its unique features as dark and light lines in essentially their correct position and shape. With contactless capture, lights and darks are the result of the 3D surface being modelled by illumination as reflection and shadow, which means the image lacks the tight coupling with the print's features that occurs with contact capture.

The agency's report is titled 'Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture'. NIST said it is planning a more detailed follow-up analysis of the data. It is also preparing a report on how well facial recognition systems identify people wearing masks.

IDEMIA, Veridium and Thales are among the best-known providers of contactless print scanners.

NIST has tested contactless fingerprint devices as Covid-19 drives users to adopt touchless technology.

VIRUS DEFENCE

Microsoft joins vendors battling pandemic

Eye-catching and innovative products to counter Covid-19 are being launched in large numbers – including a screening app from tech giant Microsoft, temperature checking helmets for the police in Delhi, and health bracelets for Beijing school students.

Microsoft has partnered with the US UnitedHealth Group to launch a free phone app that can screen employees for the Covid-19 virus. The ProtectWell app builds in US Centers for Disease Control and Prevention (CDC) guidelines, so companies can check staff for coronavirus symptoms and set up health & safety policies for their workforce and workplace.

The app works via Microsoft's Healthcare Bot service, which asks users a series of questions to screen them for Covid-19 symptoms or exposure. It also uses Microsoft's Azure, AI and analytics software, combined with UnitedHealth's clinical and data analytics capabilities. If the app identifies any risk of infection, companies can direct staff to a streamlined virus testing process, with results reported directly back to the employer. UnitedHealth will secure the healthcare data involved. The platform is available to all US organisations at no charge.

Meanwhile in New Delhi, India police officers have been equipped with futuristic 'Thermal Corona Combat' helmets. These have cameras that can detect the temperature of crowds of people from 10-15 metres away, according to the *New Indian Express*. The technology has been supplied by Indian Robotics Solution (IRS), whose founder Sagar Gupta Naugriua said: "It is a first-of-its-kind equipment to ensure the safety of the frontline warriors." Delhi's police are also deploying 'Thermal Corona Combat' drones. These have day and night-vision cameras to identify people and a disinfectant tank to sanitise any area when a suspected person is identified, the *New Indian Express* reports.

In China's capital city Beijing, five school districts are trialling biometric temperature-checking bracelets, which students wear on their wrists and which send an alert if they have a fever, according to the *Mail Online*. The bands' real-time temperature data can be monitored by teachers and parents via an app, and if a student's temperature rises above 37.2 degrees Celsius, the bracelet will prompt their teacher to alert the police. "The bracelet is similar to a normal fitness tracker. We recommend students wear them 24 hours a day," one unnamed teacher told the *Beijing Daily*.

Pyramid is partnering with ZipKey to provide 'polytouch' thermal sensing kiosks.

A string of other new anti-virus biometric products were launched last month. Among them:

• San Francisco-based Kogniz has developed an all-in-one AI platform to help people return to work despite the pandemic. The Kogniz Health Response Platform offers contactless, high-volume temperature screening, contact tracing, social distancing enforcement and mask detection. Its facial recognition cameras measure the body temperatures of large groups of people entering a building from up to 16 feet away. To enforce social distancing, an optional extra allows the surveillance cameras to alert designated staff when too many people are in an area. Kogniz co-founder Daniel Putterman said: "As we slowly start to re-open communities worldwide, our solution enables organisations to operate as safely and efficiently as possible."

• Germany's Pyramid Computer has announced a new 'polytouch' range of thermal sensing kiosks, designed to counter the spread of Covid-19. The kiosks combine contactless thermal temperature screening sensors with specific software solutions. In the US, Pyramid is providing a check-in system for users that can be integrated with existing HR systems, developed with software partner IntraEdge. For the European market, Pyramid offers the polytouch 32 curve kiosk which can be used in border control passport verification and facial recognition, using software from ZipKey.

• Seattle-based RealNetworks has added additional recognition capability to its SAFR biometric authentication system, enabling it to identify individuals wearing protective clothing. Health professionals can fix the company's new AprilTags augmented reality (AR) badge to the surface of their clothing, and SAFR will identify them without the need to remove any protective suits or masks.

• Taiwanese biometrics firm Aratek has launched a BA8200-T fever-detecting facial recognition terminal, which alerts authorities to the presence of people running a fever. The BA8200-T offers multi-factor facial and fingerprint recognition, with RFID authentication. It carries out touchless, real-time fever screening even on people wearing masks, using a proprietary infrared thermometer and compensation modules that detect raised body temperatures. The system's face recognition algorithm offers 99.72% accuracy on the LFW face database. The terminal also supports live detection to ensure user presence.

EVENTS CALENDAR

We apologise that our regular listing of upcoming conferences and events relating to biometric technology has been suspended for the time being. This is because the global coronavirus pandemic and related travel restrictions have meant that events are subject to cancellation.

• Students at the UK's Cranfield University have developed a system that uses computer vision, machine learning algorithms and deep learning AI frameworks to analyse chest X-rays and accurately identify the presence of the Covid-19 virus. Project leader Dr Zeeshan Rana said: "The research has led to some extremely promising results and we are looking to build on this success rapidly to help in the fight against Covid-19."

• DERMALOG's Automated Biometric Identification System (ABIS), which offers face and fingerprint identification, has been adopted by the Philippines Government's Land Transportation Office (LTO) for its new online payment and service portal for the state's car drivers. DERMALOG claims the new portal makes LTO one of the most advanced government agencies worldwide.

• Tascent has announced its InSight Face EBT (external body temperature) product, which enables organisations to carry out required temperature checks using non-contact thermal infrared facial recognition technologies.

• Britain's biggest airport, Heathrow, is trialling Covid detection systems that include facial recognition cameras to accurately track body temperature. Heathrow CEO, John Holland-Kaye, last month told MPs on the UK's Parliamentary Transport Committee that the trial data will be shared with the Government and industry, and the technologies and processes involved could form the basis of a Common International Standard for health screening at airports globally. The trials have begun in the immigration halls in Heathrow Terminal 2. If successful, the equipment will be installed in the airport's departures, connections and staff search areas.

• Research firm ABI predicts that Covid-19's "profound" impact on the global demand for safer contactless biometric payment cards means an extra 110 million touchless cards will be issued this year, compared to its pre-pandemic forecasts. "The message is clear: contactless payments have a critical role to play in the fight against Covid-19 from a hygiene, health and safety perspective," said ABI research director Phil Sealy.

NEWS IN BRIEF

The US **Department of Homeland Security** (DHS) has begun to migrate America's core biometric database to the Amazon Cloud, according to *Nextgov*. The newly updated HART (Homeland Advanced Recognition Technology) system contains all the core biometrics held by the US Government on its citizens and foreign nationals, including face, fingerprint and iris data. HART will replace the DHS' previous IDENT data store as the primary government system for storing and processing biometric and related personal data for national security and intelligence, law enforcement, immigration and border management purposes. Part of the upgrade is the latest move into the cloud, to allow for future data growth and increased transaction volumes. The project is being managed by Northrop Grumman in a $95 million contract awarded in 2018.

The five winners of the Security Industry Association's 2020 **Women in Biometrics Awards** have been chosen. They are: Jeni Best, branch chief at the US Customs and Border Protection (CBP) agency, who has led its work in implementing biometrics at 27 US airports; Anne May, lead manager for the US Department of Homeland Security Biometric Support Center, who has directed the deployment of specialised biometric hardware at over 550 border patrol and immigration enforcement field sites; Mei Ngan, a scientist in the NIST Image Group, who develops standards and best practices for biometric systems, notably in the fields of face morphing detection, tattoo recognition and face recognition evaluation; Lauren Reed, a senior programme director at IDEMIA NSS, where she leads the deployment of large-scale multimodal biometric systems to US government foreign partners, enabling them to advance their crime and terrorism detection capabilities; and Annet Steenbergen, co-founder of the Happy Flow Project, for the Government of Aruba – the first seamless airport implementation of a single-token initiative, which created a seamless flow of passengers from curb to gate through the re-use of biometrics.

Norway-based biometric payment card vendor **IDEX** has been given the official 'seal of approval' to mass-market its cards in China. The go-ahead has come from China UnionPay, the world's largest payment network. China UnionPay has issued a formal Letter of Approval (LOA) for a biometric payment card containing IDEX's fingerprint sensor and distributed matcher – confirming that the IDEX offering is compliant with all the requirements needed to operate with ATMs and point of sale (POS) terminals worldwide. It is the first biometric card certification issued by China UnionPay. Independent expert Phil Sealy, research director at ABI, said: "The importance of this cannot be overstated. This is a significant market milestone, as certification and LOA must be met for the biometric card to move into the mass market issuance phase." IDEX CEO Vince Graziani said: "This LOA is a critical step to driving mass adoption in China. IDEX and our partners are now approved for deployment in the world's largest market for payment cards."

PRODUCTS

Vuzix, the leading US supplier of smart glasses, has teamed up with Dubai-based software developer **NNTC** to launch version 2.0 of their iFalcon Face Control Mobile facial recognition system running on Vuzix Blade glasses. The new release is designed for city-wide deployment. It will enable police and security forces to screen crowds and match faces without requiring a network of CCTV cameras, with the added ability to manage hundreds of wearable devices and thousands of stationary cameras in a single interface. For the future, NNTC is also considering adding OpenVino, Intel's AI and computer vision platform, into the product. Vuzix is a public company headquartered in New York, with offices in the UK and Japan.

Slovakia-based identity access management startup **Daltrey** has partnered with biometrics provider **Innovatrics** to develop a frictionless access management and authentication system. The combined Biometrics as a Service (BaaS) solution enables users to set up a verified biometric credential on the Daltrey platform, including face, iris and fingerprints, to give them access to both physical locations and digital apps. The service uses Innovatrics' passive liveness technology to verify the user identities online. Daltrey managing director Blair Crawford said it chose Innovatrics as it "consistently ranks among the best in the world in biometric benchmark evaluations". He added: "There is a growing need for more secure, seamless and convenient authentication spanning both physical and digital access scenarios."

South Korean vendor **Union Community** has unveiled a multi-modal iris and fingerprint recognition biometric terminal, UBio-X Iris, that can perform iris recognition at a distance of 50cm. The company says this comes at a time of rapidly rising demand for contactless biometric solutions during the Covid-19 pandemic. UBio-X Iris offers an auto-tilting function, which automatically finds irises at a distance of up to 50cm and authenticates them. It is expected to be adopted in medical facilities, airports and commercial sites. It also includes a high-performance recognition algorithm that enables up to 20,000 iris authentications a second. The company said: "As the demand for contactless biometric recognition has expanded in the global market, we expect a significant increase in sales with the launch of the iris recognition system this year."

Massachusetts-based **Aware** has released a new version of its Knomi mobile biometric onboarding and authentication system. Knomi 2.6 combines face and speaker recognition in a single platform, enabling users to deploy multifactor authentication. It also includes algorithms for voice liveness, or anti-spoofing. Aware chief commercial officer Rob Mungovan said: "It's a significant advancement in the pursuit of secure passwordless authentication. With Knomi 2.6, our customers can authenticate users through their face or their voice. We believe the combination of face plus voice biometrics, with face liveness and voice liveness, makes Knomi 2.6 a one-of-a-kind offering." Chief technology officer Mohamed Lazzouni added: "Using face and voice liveness detection running on the user's device raises the bar against presentation attacks, with the convenience of taking a selfie and recording a voice memo. Knomi 2.6's architecture that uses minimal on-device software also keeps the management overhead of the platform low and adaptable to customer needs."

COMPANY

Start-up global biometrics company, **Corsight**, has launched new AI facial recognition solutions for the security market. Corsight is headquartered in New Jersey with an R&D centre in Israel, and is headed by industry veterans Gadi Piran, Mulli Diamant and Yoav Millet, former founders and executive members at surveillance software firm OnSSI. Corsight says its recognition solutions use AI neural network technology created from research at Technion, the Israel Institute of Technology. The company claims its systems can recognise faces even at extreme angles with high speed and accuracy, in different perspectives under diverse lighting and environmental conditions. Corsight, which has registered over 250 product patents, recently raised $5 million from Awz Ventures, a Canadian fund focused on intelligence and security technologies.

Building a governance framework for facial recognition

Lofred Madzou

Sebastien Louradour

Lofred Madzou and Sebastien Louradour, World Economic Forum

Over the past decade, facial recognition technology has spread across a number of industries. In many stores in China, you can now pay with your face[1]. And as airports worldwide increasingly deploy facial recognition to speed up border control, passengers can board planes with a simple smile[2]. The technology has also been used for safety and security purposes primarily by law enforcement agencies, and more recently in the fight against Covid-19 in combination with body temperature measurement[3].

But while the development of face technology can provide a positive impact, its growing use by companies and governments also creates legitimate concerns. First, some use-cases pose a threat to human rights, especially privacy[4], and civil liberties. Secondly, its susceptibility to unfair bias can lead to discriminatory outcomes and potentially infringe both individual and collective rights.

Public and private organisations worldwide are now grappling with this challenge and exploring various policy responses. These initiatives have been developed by advocacy groups, tech companies and governments to mention a few, and the propositions can be classified into three main types:

1. High-level principles on AI, that sometimes include examples for facial recognition[5].
2. Proposals for the self-regulation of AI, put forward by the research labs of tech companies such as Google, IBM and others[6].
3. The definition of laws by governments to limit the use of the technology, which can vary from strict bans[7] to its allowance with limits.

To help these organisations define governance models for facial recognition, the Centre for the Fourth Industrial Revolution[8] (C4IR) at the World Economic Forum is spearheading a multi-stakeholder, evidence-based policy project in France. This involves industry actors, policy makers, civil society representatives and academics, who have developed a governance framework to ensure the safe and trustworthy use of facial technology (see *The WEF framework* box).

Our project community followed the multi-stakeholder, pilot-based approach to policy making favoured at the C4IR – we tackle governance issues through real-world use-cases, to ensure that our governance frameworks are effectively actionable by policy makers[9].

In doing this, we decided to focus first on the use-case of 'flow management'. This primarily refers to situations where faces are used as a means of authentication or identification to access services that include check-in to board airplanes, trains, rent hotel rooms, etc. This application of facial recognition is likely to develop in the coming years as transportation organisations (eg, airports) and organisers of large-scale gathering events (eg, the International Olympic Committee[10]) increasingly adopt this technology.

Despite their various perspectives, the working group established a shared definition of what constitutes the responsible use of facial recognition, and what checks and balances should be in place to ensure the trustworthy and safe use of this technology for flow management (see Figure 1, next page). They also agreed on the need to allow external audits and a certification scheme to ensure greater accountability.

Most AI principles[11] drafted by public and

The WEF framework

For the past year, the AI and ML teams at the World Economic Forum have been drafting a framework to encourage and ensure the responsible design and use of facial recognition technology for flow management use-cases. Co-designed by a multi-stakeholder community involving policy makers, industry players, civil society and academics, the framework seeks to address the need for a set of concrete guidelines to ensure the trustworthy and safe use of this technology. For engineers, it provides a practical guide to implementing solid, robust risk mitigation processes – while enabling policy makers to ensure that citizens' and consumers' rights and freedoms are effectively protected.

In this work, our project community set out to tackle governance issues through real-world use-cases, to ensure that the governance frameworks are effectively actionable by policy makers. The community involves major transportation companies including Paris Airport (Groupe ADP) and SNCF (the French railway company), technology providers (AWS, IBM, IDEMIA, IN Groupe, Microsoft and NEC), policy makers (members of the French Parliament), academics, civil society organisations, and AFNOR Certification. Insights have also been provided by the European Commission. This community have held numerous workshops and webinars in order to gather insights, review the working documents and build consensus among the working group.

• The framework we have produced is presented in the recently published white paper, 'A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management' (available at www.weforum.org/whitepapers/a-framework-for-responsible-limits-on-facial-recognition-use-case-flow-management).

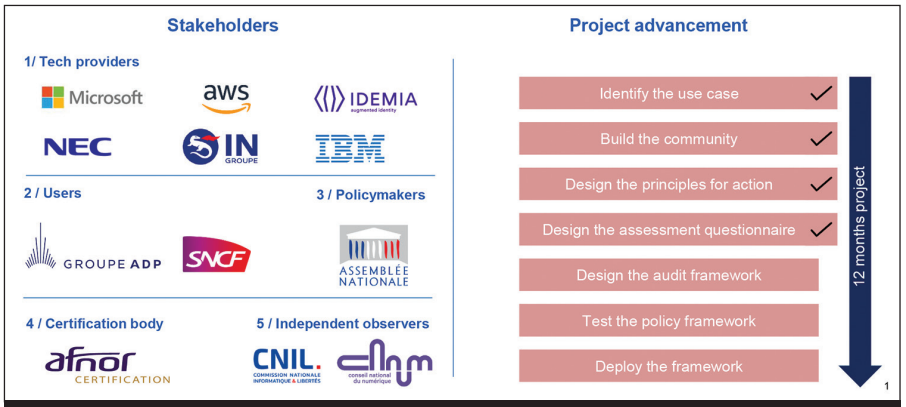


Figure 1: Flow management stakeholders and activities.

private organisations address high-level ethical considerations about AI such as transparency, safety or fairness. We think this work is valuable, but needs to be complemented with a more practical approach that captures three key elements: how these concerns manifest in the real world; how they can be effectively addressed by an agile governance framework; and the need to include a well-balanced multi-stakeholder community.

Dealing with the risks

The use-case based approach taken in building the framework highlights the fact that the risks associated with using facial recognition technologies are highly context-dependent. In other words, utilising this technology to speed up the checking process at airports or to ensure safety at public events carry very different risks. For example, a false positive in the flow management use-case generally means that the wrong person gets access to a service instead of the right one. But a false positive in the law enforcement context can lead to an individual being misidentified and even losing their liberty.

This distinction may seem obvious to engineers and experts, but it is not to everyone. So we felt that adopting a use-case based approach for policymaking was essential in order to appropriately identify the risks associated with various applications, and improve public understanding of the issues at stake. This approach provides policy makers with an agile method to account for these different contexts, in order to maximise the benefits of facial recognition while mitigating its adverse impacts. We also think it is faster than existing public policy projects (the governance framework was co-designed in 12 months).

Four-step solution

As Figure 2 shows, the governance framework is structured around four key steps:

1. **Define** what constitutes the responsible use of facial recognition, through a set of principles for action. These principles focus on privacy, bias mitigation, the proportional use of the technology, accountability, consent, right to accessibility, children's rights and alternative options.
2. **Design** a set of best-practice methodologies, tailored by use-cases, to support product teams in the development of systems that are 'responsible by design'.
3. **Assess** to what extent the system designed is responsible, through an assessment questionnaire that describes what rules should be respected to comply with the principles for action.
4. **Validate** the compliance with the principles for action through the design of an audit framework by a trusted third party. The goal is to provide a certification to organisations able to prove their ability to deploy a system respecting the principles for action.

In practical terms, the framework provides engineers with a structured approach to risk mitigation, including best practices and an assessment questionnaire that they can readily apply in their work (see Figure 3). In addition,

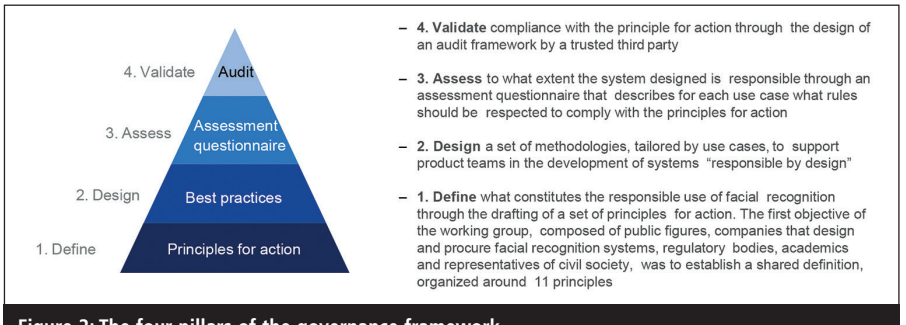


Figure 2: The four pillars of the governance framework.

the external audit represents a robust mechanism for creating trust between technology providers, users, and society at large. The industry actors that comply with our governance framework can therefore demonstrate that they have implemented effective processes to protect consumers.

Building trust and awareness

The aim is that engineers and product teams can use the framework at the design stage to inform the development of their systems. This could include asking upfront if there is a better (eg, less privacy-invasive) alternative to facial recognition technology for the problem being considered, and therefore justifying this choice with sound arguments. Equally, the process of reflecting on the data plan design, and how unfair biases should be continually identified and mitigated – before even deploying any system – enables project teams to ensure greater accountability and create trust with users, policy makers and society at large.

Meanwhile, those organisations that have a running facial recognition system can use the results of the assessment questionnaire (with an auto-diagnostic) to ensure they are compliant with the 'principles for action'. This is also a means of demonstrating that they have proactively addressed the ethical challenges associated with their systems. More fundamentally, the framework encourages organisations to run internal and external audits to mitigate the risks associated with biases.

Again, delegating the ability to run external audits to a trusted third party could be a powerful way for policy makers to restore citizens' trust. This is particularly relevant at this time of growing public concern about facial recognition technology, fuelled by various controversies around privacy abuses and biased systems. Indeed, consumers' and citizens' concerns are currently largely unaddressed, besides cases of privacy violations.

In this area, we've partnered with the leading French certification organisation, AFNOR Certification, to illustrate how an external audit could be conducted and a certification process implemented. Over the next months, our project community is going to co-design the requirements of the external audit framework, which will eventually lead to the issuance of certification for facial recognition systems used for flow management.

Future moves

The next step in the development of the governance framework is to test and update it, based on the findings of the pilot. In this regard, the first

version of the assessment questionnaire and principles for action was designed primarily for facial recognition systems deployed for flow management, in order to ensure their compliance with the principles for action presented in the framework. This is likely to evolve depending on the results of the testing phase, which was due to take place in France in mid-March but will be rescheduled due to the Covid-19 pandemic.

Our project community is also currently finalising the audit framework, the cornerstone of the framework. Once this is completed, certification organisations will be able to use it to assess the compliance of their facial recognition systems with the principles for action. The purpose of the certification model is to provide a label for systems that prove to comply with these principles. Essentially, the audit will verify firstly that risk-mitigation processes are in place and relevant enough to ensure, for example, that end users who may be subject to algorithm biases will get the same level of service provided for all end users; and secondly, that the system effectively conforms with the principles for action. In this sense, the purpose of the certification model is to label companies and organisations using facial recognition rather than platform providers.

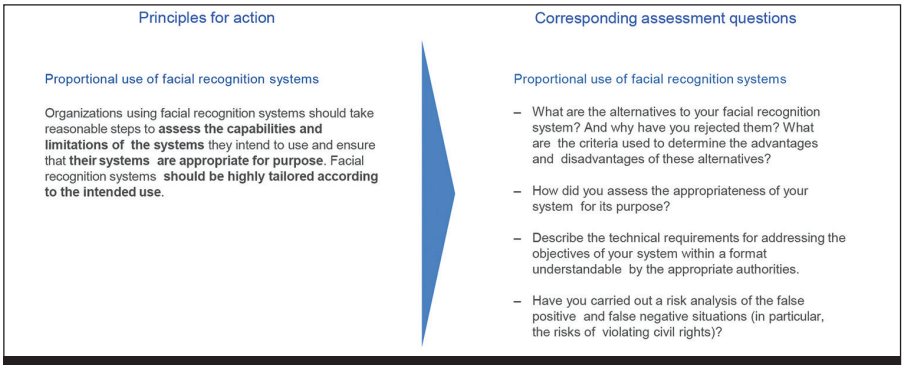


Figure 3: Framework's principles for action and related assessment questionnaire.

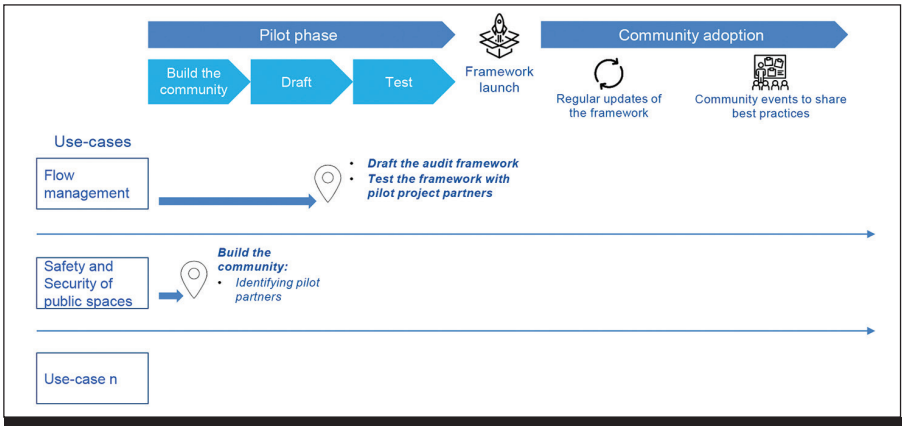


Figure 4: Project timeline and next steps.

Conclusion

The core thinking behind the governance framework is that, given the sensitivity of biometric data, the use of facial recognition is intrinsically risky. This is particularly the case when it is deployed for safety and security purposes, as it may lead to a new form of automated surveillance. Therefore, there is a pressing need to create a robust governance framework to mitigate these risks.

We hope that the method we've developed and the results of our policy pilot can pave the way to designing a standard for the responsible application of facial recognition. To achieve this goal, we have started by building a global multi-stakeholder community, then co-drafting a governance framework. Once our industry partners fully resume their operations, we will test this on the flow management use-case. At the same time, we're actively considering drafting similar frameworks on other use-cases such as safety and security of public spaces (see Figure 4), and are actively encouraging those operating in this domain to join our project community.

When the policy pilot is completed, we will build a coalition of actors committed to respecting and promoting this governance framework. Considering the pace of technological change, we're fully aware of the need to regularly update the framework to take into account the new challenges faced by those organisations designing and procuring facial recognition technology. That is why our long-term goal is to establish a community of trusted practitioners able and willing to discuss their issues and best practices, so as to update the framework over time.

We believe that to ensure the effective governance of facial recognition technology, we must create the conditions for a continuous dialogue and co-ordinated action between policy makers, industry players, citizens and academics. This will enable us to strike the right balance between the need to maximise the benefits of this emerging technology, while mitigating its risks. The creation of the governance framework represents a promising step toward this goal.

Finally, given our open and experimental approach, we would encourage other industry players, public actors, civil society, advocacy groups, policy makers and academics to join us on this journey, to strengthen our governance framework and ensure its impact.

About the authors

Lofred Madzou is a project leader for AI at the World Economic Forum, where he is responsible for managing various global multi-stakeholder AI policy projects. Before this, he was a policy officer advising the French Government on AI policy and regulation. He co-wrote a section of the French National AI Strategy, entitled 'What Ethics for AI?'. Lofred has an MSc in data science and philosophy from Oxford University.

Sebastien Louradour is an expert in artificial intelligence and innovation with the French Government and a fellow at the World Economic Forum. He is the former head of innovation outpost for an innovation agency based in San Francisco, where he scouted tech trends for European companies. Before that, he conducted digital transformation projects for the public sector, at KPMG then Kurt Salmon. Sebastien graduated from Paris Diderot University with a masters degree in sociology.

References

1. Helen Roxburgh. 'Chinese shoppers embrace facial payments'. Asia Times, 5 September 2019. Accessed May 2020. https://asiatimes.com/2019/09/chinese-shoppers-embrace-facial-payments/.
2. Keith Mwanalushi. 'Facial recognition: Adoption of biometric technology at airports'. Aviation Business News, 6 December 2019. Accessed May 2020. https://www.aviationbusinessnews.com/low-cost/facial-recognition-biometric-technology/.
3. Martin Pollard. 'Coronavirus: Chinese facial recognition firm says they can ID people wearing face masks'. Global News, 9 March 2020. Accessed May 2020. https://globalnews.ca/news/6653657/coronavirus-facial-recognition-firm-face-masks/.
4. Kashmir Hill. 'The Secretive Company That Might End Privacy as We Know It'. New York Times, 18 January 2020. Accessed May 2020. https://www.nytimes.

com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
5. 'Introducing the Principled Artificial Intelligence Project'. Harvard Law School, 7 June 2019. Accessed May 2020. http://blogs.harvard.edu/cyberlawclinic/2019/06/07/introducing-the-principled-artificial-intelligence-project/.
6. Examples include: FactSheets model (IBM Research), Model Cards (Google), Framework for Internal Algorithmic Auditing (Google), AI principles (Microsoft).
7. Max Read. 'Why We Should Ban Facial Recognition Technology'. New York Magazine, 30 January 2020. Accessed May 2020. https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html.
8. 'Centre for the Fourth Industrial Revolution'. World Economic Forum. Accessed May 2020. https://www.weforum.org/centre-for-the-fourth-industrial-revolution.
9. 'Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution'. WEF, 24 April 2018. Accessed May 2020. https://www.weforum.org/whitepapers/agile-governance-reimagining-policy-making-in-the-fourth-industrial-revolution.
10. Stephen Shankland. 'Tokyo 2020 Olympics using facial recognition system from NEC, Intel'. CNET, 1 October 2019. Accessed May 2020. https://www.cnet.com/news/tokyo-2020-olympics-using-facial-recognition-system-from-nec-intel/.
11. Jessica Morley, Luciano Floridi, Libby Kinsey and Anat Elhalal. 'From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices'. Springer Nature, 11 December 2019. Accessed May 2020. https://link.springer.com/article/10.1007/s11948-019-00165-5.

How finger vein offers businesses a helping hand

Andy Milton, Hitachi

Andy Milton

Estimates suggest that the average consumer has over 100 separate online accounts – that isn't a typo, it's one hundred. How did we end up in this situation?

When the world first began moving online, passwords became the *de facto* choice for verification – given the absence of other widely and cheaply available technologies and, for consumers, the ease with which they can be set up. Even so, for the past 20 years compromised or stolen passwords have accounted for more security breaches than any other verification method. And even though modern biometric systems emerged at the same time as computer systems, in the second half of the 20th century – to this day, consumers and businesses still use passwords to set up and secure their multiple online accounts.

Why is this? The answer is that they remain the simplest verification method, and therefore the default option. However, it is precisely this ease that makes them an ineffective means of guarding against data breaches in the 21st century. As technology has become more developed, so have the hackers, and businesses cannot effectively compete with mounting cyber-crime while continuing to rely on password authentication.

What's wrong with passwords

There remain a range of problems associated with the use of passwords. Many of us are still guilty of not choosing secure passwords. A 2019 survey by the UK's National Cyber Security Centre found that 23.2 million victim accounts worldwide had used 123456 as a password[6] – and the prevalence of people duplicating these weak passwords across sites and accounts, only increases the risk to our online security.

For businesses, relying on passwords can be extremely costly. Data breaches afflicted 88% of UK companies from September 2018 to 2019, according to Carbon Black[7]. There is also the cost incurred when passwords are reset, a process that on the surface is simple but when added up across a large business becomes a major outlay.

Growth of finger vein ID

Initially, the drive to replace passwords with biometrics spurred the development of fingerprint systems. And as biometric checks became increasingly prevalent in consumer electronics, businesses started to explore their applicability. For example, statistics from CyberArk suggest that by 2018, nearly one in five office IT security teams had started to use biometric security techniques[1].

Now, the less well-known alternative biometric of finger vein technology has emerged to offer businesses a potentially superior solution. First developed and patented by Hitachi in 2005, finger vein authentication is increasingly being used across a range of sectors, from banking to retail. This form of verification uses unique finger vein patterns to verify an individual, and works through a process of image capture, verification and authentication.

Finger vein devices use infrared light to penetrate the skin, which when absorbed by the haemoglobin in the blood, reflects the image of the finger vein pattern to the device. This image is captured by an in-device camera, and image processing constructs a finger vein pattern from this image. When a user sets up their finger vein authentication, after the first image is compressed and digitised, this can then be used as either a template or a digitised image. Whenever the device is used, it will grant access when these multiple finger patterns are matched.

Apple's game-changing adoption of biometrics for authentication has significantly helped in opening up the market to finger vein, as people are increasingly accustomed to using biometrics for verification. Finger vein tech itself has been around for almost 20 years, but its relatively recent adaptation in laptop and mobile cameras, alongside developments in the technology itself, has opened the market up and turned finger vein into a huge opportunity for the biometrics market. But the question many might ask is: what is the difference between finger vein and fingerprint authentication, and what makes veins better?

Vein vs print

There has long been market demand for a more accurate technology than fingerprinting. It has taken longer for finger vein technology to come to fruition in the market simply because of the relative complexity of making finger vein scan-

ners – it is easy and cheap to make fingerprint scanners. However, people are increasingly realising the drawbacks of using cheaper fingerprint applications, and the numerous benefits instead of using finger vein. These include:

• Physical contact. Fingerprint recognition requires physical contact with a scanning device, making the technology vulnerable to prints being lifted from finger smears left behind. In the Covid-19 era, touchless technologies are also seen as safer. Alongside collecting individual prints, 'Masterprints' can also be generated using machine learning to match with many fingerprints.

In addition, the accuracy of fingerprints is questionable – not just because fingerprints can be faked, but because the surface of skin changes over time. For users, this can mean repeated failures to access the device. Finger vein scanners don't require physical contact with the scanner, removing the risk of spoofing or failed authentications due to change over time.

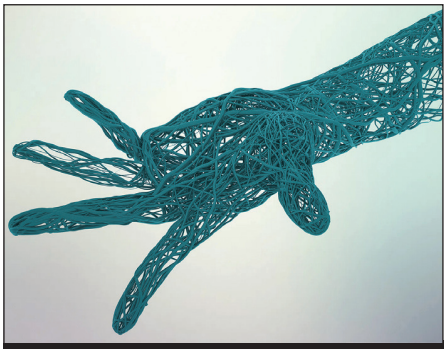
• Data storage. Fingerprint scanning holds information on the device rather than centrally – if you lose your phone or tablet, your fingerprint is of no use to you, as you can't use it to access your details on another device. Finger vein applications can be stored centrally, making it easier to operate across multiple devices.

• Cost. Previously, the cost of finger vein technology has been a key prohibiting factor in it becoming mainstream, despite its obvious benefits over face and fingerprint. But with the shift to using standard cameras in various applications of the technology, and moving away from specialist hardware, we can now see that start to change.

For example, in applications that utilise a user's own camera, the outlay for deploying finger vein becomes that of a simple software licence – reducing the cost of deployment by around 20% compared to previously. This helps to make finger vein technology a highly secure and robust mode of biometric now available to everyone.

• Ease of use. Finger vein technology can work seamlessly with existing technology, without the need to add a physical scanner or use tokens. Finger vein-based applications have now been developed for use on a PC or laptop – the in-built camera just has to be upgraded using software to scan finger veins. Utilising existing technology makes it far easier for a large business to install this technology at scale.

The process of software installation on a laptop is also typically quite fast. It generally takes around five minutes, and applications can take less than two seconds to authenticate a user. For the user, identifying themselves through this finger vein technology is also a straightforward process. Known as 'hand gesture' technology, the unique finger vein pattern of the user can be identified by the computer or laptop's camera with a simple raising of the hand. It's easy and fast, and it offers a long-term solution that doesn't need to be constantly updated.



As biometric checks become increasingly prevalent among consumers, the less well-known alternative of finger vein technology has emerged.

Sectors switching to finger vein

For a long time, finger vein technology was seen as suitable in areas like high-end banking applications, rather than the mass market. But this has started to change. Finger vein tech is certainly useful for individuals who simply don't want to have to remember a plethora of passwords. But for a range of businesses, there is value to be found by using this technology in their operations. These include:

• Banking. There is naturally a strong impetus for banks to turn to a more secure method of authentication. In Japan, for example, finger vein technology was first deployed at ATMs in 1997. In Europe, the entry of biometrics into this sector was given the official nod in June 2019, when the European Banking Authority clarified that all biometric techniques, including methods such as finger vein recognition, were acceptable. This also has benefits for consumers, as it reduces the risk of fraud. Goode Intelligence estimates that by the end of 2020, 1.9 billion banking customers will be using biometrics for banking services[2]. Barclays Bank recently deployed finger vein identification for corporate customers and found it has reduced the number of errors and instances of fraud. Customers have also found it enabled them to process payments much faster and more efficiently.

With finger vein, people identify themselves through a simple raising of the hand. It's easy and fast, and offers a long-term solution.

• Payments. The increasing use of finger vein in the banking sector has naturally started to extend to wider payment uses, with finger vein technology appearing in a variety of retail applications. A bar in Manchester, UK last year became the first to start using finger vein technology, enabling customers to pay for orders with a simple swipe of their finger. Launched in partnership with Fingopay, this followed successful pilots across other venues across the UK[3].

• E-commerce. Online businesses are also increasingly turning to biometrics. E-commerce is an area where we can expect to see finger vein technology increasingly being used. There are of course the natural security considerations, but also a business-case perspective – one in three online shoppers in the US have abandoned a transaction rather than re-enter payment details[4].

Conclusion

Studies are finding that, for consumers, security is increasingly starting to outweigh convenience – perhaps finally signalling a turning tide for the era of passwords. Importantly, we are also moving into an age where people are increasingly happy to use biometrics: an IBM survey in 2018 found that, globally, 87% of adults said they would be comfortable with these technologies in the near future[5].

The result is that biometrics are increasingly becoming the preferred verification method for both consumers and corporates. As a relatively new biometric technology, this is therefore an exciting time for finger vein technology. With its proven security advantages over alternative modes of authentication, including both facial recognition and fingerprint scanning, finger vein is set to emerge as one of the easiest and most secure methods of biometric authentication.

About the author

Andy Milton is head of channels at Hitachi Security Business Group. He has worked on finger vein technology for Hitachi since 2018, helping to raise the technology's profile as a more cost-effective and efficient authentication method. Hitachi is an industry leader in digital security, helping customers to move away from passwords and towards the future of biometric authentication. Before working at Hitachi, Andy worked in digital security for several information technology and services companies, including T-Systems.

References

1. David Higgins. 'Biometric Authentication – Our "Unique Human Identities" Under Attack'. CyberArk, 30 April 2019. Accessed May 2020. https://

www.cyberark.com/blog/biometric-authentication-our-unique-human-identities-under-attack/.
2. 'Biometrics for Banking; Market & Technology Analysis, Adoption Strategies & Forecasts 2018-2023'. Goode Intelligence, 19 September 2018. Accessed May 2020. https://www.goodeintelligence.com/report/biometrics-for-banking-market-technology-analysis-adoption-strategies-forecasts-2018-2023/.
3. 'Fintech Disruptor Chooses Manchester for Global Launch'. Invest in Manchester, 1 April 2019. Accessed May 2020. https://www.investinmanchester.com/latest-news/2019/4/1/fintech-disruptor-chooses-manchester-for-global-launch-a2682.
4. Carly Minsky. 'Ecommerce turns to biometrics to validate shoppers'. Financial Times, 20 November 2019. Accessed May 2020. https://www.ft.com/content/5d8100b6-ca6e-11e9-af46-b09e8bfe60c0.
5. 'IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape'. IBM, 29 January 2018. Accessed May 2020. https://www-03.ibm.com/press/us/en/pressrelease/53646.wss.
6. 'Most hacked passwords revealed as UK cyber survey exposes gaps in online security'. National Cyber Security Centre, 21 April 2019. Accessed May 2020. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security.
7. 'Global Threat Report'. Carbon Black, October 2019. Accessed May 2020. https://www.carbonblack.com/global-threat-report-defender-power-on-the-rise/.

Covid-19: why selfies are in the spotlight for proving ID

Zac Cohen

Zac Cohen, Trulioo

Beyond its threat to life, the impact of the Covid-19 virus on business is going to be felt for some time. No industry is immune and while vaccines, social distancing and testing apps might prove to be enough to help protect citizens and consumers, the same can't be said for companies.

One of the biggest lessons from the Covid-19 pandemic is how important it is to stay ahead of the digital transformation curve. Indeed, one of the major changes we have seen in recent months is remote working, as offices have closed and where possible people have been tasked with operating virtually. Whether it is in reaction to the virus or just an acceleration of the cultural shift the world was starting to see anyway, returning to offices *en masse* is not something we're going to see any time soon. And, while the world's workforce has largely tried to continue to maintain levels of productivity, this major shift in working practices is not just 'business as usual' and for it to work in the long term, proper provisions will be required.

With the workforce now far more remote, organisations in almost all sectors need to be adequately equipped to deal with the rigours that virtual access and working from satellite locations bring. This means that major business continuity issues around security and access (or lack of it) to the requisite materials, will be a priority. For organisations like banks that are reliant on manual document checks for their KYC (know your customer) and AML (anti-money laundering) processes, this presents a major challenge. These banks and other financial institutions – along with others affected by money laundering regulations (MLRs), such as lawyers, accountants and estate agents – all need to shift to digital to continue performing these checks.

Biometrics boom

It goes without saying that the changing consumer behaviour has contributed to verification strategies and technologies evolving rapidly. In a dynamic online environment like the one we currently live in, identity verification needs to work quickly and seamlessly across multiple channels and fit in with a world-class digital experience.

For that reason, biometric authentication – uniquely identifying a person by evaluating one or more distinguishing biological traits – is becoming a critical element of identity verification, particularly driven by the staggering adoption rates of smartphones that support and enable biometric technology. Data from Statista[1] suggests that there are 3.2 billion smartphone users worldwide, which puts global smartphone penetration at around 41.5%.

Although we are still in the early stages of biometric-based identity proofing and authentication, its development will serve as an important fraud indicator for the growing epidemic. Businesses will increasingly look to incorporate biometrics as part of an holistic approach to identity verification.

Organisations will want to ensure they have access to the broadest possible identity network, which in turn gives them access to the most appropriate identity data points, based on the level of risk associated with the transaction or activity. These will include personal identification information, IP address, mobile data, behavioural data, fingerprint, selfie, retina scan, document verification, bank data, fraud data, and much more. This breadth and depth of data points within a trusted and secure identity network will become the holy grail for organisations as they optimise their identity assurance.

These new technologies are playing an increasing role when businesses verify the identity of new customers during the online account creation process. Security and user experience have to go hand in hand. In fact, consumers are increasingly intolerant of poor online account opening processes[2] and organisations that don't do it right will risk losing customers and revenue. However, if they can deliver smooth, seamless and secure account creation, then it sets them up for long and fruitful relationships with customers.

Little wonder then that the selfie is coming to the fore as a simple and quick way for consumers to be able to verify the authenticity of the identity documents they have submit-

ted. Taking selfies has become second nature to us – in fact, it is predicted that the average millennial will take 25,000 selfies during their lifetime[3]. As more and more people unlock their phone with their face, it's paving the way for facial recognition systems due to the fact that people are more familiar and confident with this experience first-hand. According to new research[4], 74% of global consumers are more confident that physical biometrics will protect their information over passwords, up from 43%.

Adoption by businesses

The acceleration of selfies as means of ID verification has been one of the immediate impacts of the Covid-19 pandemic. For example, the UK Financial Conduct Authority (FCA) recently announced that financial firms can ask customers for a selfie to check their identity – in an effort to ease the burdens on staff having to work from home during the coronavirus lockdown. But this is just part of a much broader trend, not just a short-term solution to location and access issues.

Ride-hailing firm Uber is bringing in real-time facial checks for drivers working on its platform. It is rolling out the additional ID check which will ask drivers to take selfies of themselves at random times when they log on to the app. It is hoped that the real-time ID check will verify that driver accounts aren't being used by anyone other than the licensed individuals.

In fact, using a selfie as a form of verification goes back to 2019, when the UK's NatWest became the first major retail bank to enable customers to open an account with a selfie. The move eliminated the need to go into a branch, put identity documents in the post, or wait a day or two for the account-opening process to be completed. Instead, the customer uploads a selfie and photo ID such as a passport to verify who they are. Fast forward to today and it's much more common. As an example, Monzo asks its customers to submit a short video of themselves saying "Hi, my name is [name], and I want a Monzo account". The RBC mobile app is the latest to announce plans to introduce selfie verification for customers opening new accounts. While this may seem a very simple verification mechanism, the crux of it is so much more than a click and smile.

Verification, then authentication

As with any major evolution to established processes, the increasing trend when it comes to selfie usage is not without challenges. There are some industry voices who have suggested that checking new client identities remotely amid the coronavirus lockdown makes financial firms more vulnerable to attempted money laundering. There are others who have gone much further, suggesting that regulatory guidance to accept selfies amounts to 'a fraudster's charter'.

On the surface, it's an easy critique to level but when considering biometric-based authentication methods for compliance or fraud prevention, it's vital to understand the various trade-offs between security, risk, accuracy, usability and cost. Achieving the level of security required for a particular use-case while delivering acceptable performance for the other parameters is now regularly attainable with the current state of technology. As with any risk-based approach, it's about determining the level of risk and matching system requirements that are appropriate to that level.

It's also important to note that authentication comes after enrolment and identity proofing; to authenticate someone, you must have previously verified the identity of that individual, to make sure you are dealing with a real person. There are three factors that can determine authentication which are all relatively common: something the customer knows (knowledge, such as a PIN or password), something the customer has (possession, such as an identity document or a smartphone) and something the customer is (inherence, such as biometrics).

Deploying multi-factor authentication (MFA), where two of the three factors are authenticated, is sufficient to meet the highest NIST security requirements. This criteria concurs with the EU standards for strong customer authentication (SCA). Of course, meeting these security standards presupposes that the factor has enough integrity and confidentiality to uniquely identify the user.

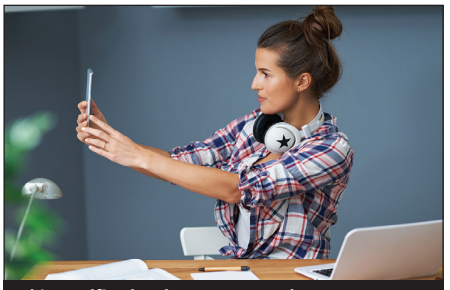
Balancing security and speed

It's imperative that any business has effective security measures to ensure that the real user of the account is performing the requested actions. However, this will demand the business evaluates what level of security is needed. The fact is that this approach becomes inoperable if businesses deploy systems that are onerous and time-consuming for users, or risk customer abandonment. There has to be a balance between risk and usability, speed and security.

This is why modern smartphones are a game-changer, as they have put powerful biometric technologies into the hands of billions of people. By combining possession of a smartphone (something the customer has) with a biometric (something the customer is), authentication has become scalable for general audience use-cases[5].

If a transaction needs authentication (such as with SCA), a bank can send a notification to a secure app on a customer's smartphone. If the notification is confirmed, that's strong confirmation that the customer has both the device and secure access to the app. While password access to the app would also pass the MFA requirement, logging in with a thumbprint or face scan is much quicker and easier for the customer. Seamless security is the goal, and biometric authentication delivers. However, it's crucial to ensure that the original identity is properly verified, matched against a wide range of robust identity data sources. After all, if a money launderer, fraudster or other bad actor already has an account, authentication provides no deterrent.

Continued on page 12...



Taking selfies has become second nature to us, and it's paving the way for facial recognition systems as people are more confident with this experience first-hand.

...Continued from page 11

In all walks of life, there are people who like having their photo taken much more than others. This same stance can be found in businesses that are (or not) adopting the selfie for ID verification.

Digital ID strategies

In all walks of life, there are people who like having their photo taken much more than others. The same stance can be found in businesses and industries that are (or not) adopting the selfie as a means of ID verification. It's not something that is right for every business, and there will always be early adopters of something that changes the *status quo* so drastically. For example, fintech business models especially are built for uncertain times. It should be little surprise that these businesses are preparing digital identity verification and fraud prevention strategies for stimulus fund disbursement, educating customers and preparing internally for pandemic-related scams, and aligning strategies for fraud, growth and innovation.

But these are the trailblazers and they only underline why selfies are becoming so much more common for identity authentication. Selfies offer another layer of security and assurance that is unique to each individual and, when combined with other forms of ID, is immensely secure. If we think the power of the selfie has been demonstrated on platforms like Instagram, it's nothing to how influential it is going to be in the field of ID verification…but without the filters.

About the author

Zac Cohen is a business leader experienced in managing and scaling high-growth companies. He is a veteran of all facets of startup and tech operations, including strategic planning and execution, corporate management, and building high-performance teams. His expertise in risk and compliance software continues to drive innovative and effective solutions for businesses operating worldwide. Zac is chief operating officer at Trulioo, a high-growth Vancouver-based startup addressing global identity challenges associated with international regulatory compliance, fraud prevention, and trust and safety online. He focuses on fostering change-makers who want to make an impact and are engaged in building innovative solutions that address the world's most pressing problems.

References

1. 'Number of smartphone users worldwide from 2016 to 2021'. Statista, 28 February 2020. Accessed May 2020. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.
2. 'Trulioo Consumer Account Opening Report'. Trulioo, March 2020. Accessed May 2020. https://www.prweb.com/releases/consumers_say_online_account_creation_process_can_make_or_break_their_relationship_with_digital_services_but_less_than_half_are_satisfied/prweb17010738.htm.
3. Erica Tempesta. 'Researchers reveal millennials will take a whopping 25,000 photos of themselves in their lifetime'. Mail Online, 21 September 2015. Accessed May 2020. https://www.dailymail.co.uk/femail/article-3243646/Researchers-reveal-millennials-whopping-25-000-photos-lifetime.html.
4. '2020 Global Identity and Fraud Report'. Experian, February 2020. Accessed May 2020. https://www.experian.com/blogs/insights/2020/02/experians-2020-global-identity-fraud-report/.
5. ID Document Verification Reference Paper, Trulioo. Accessed May 2020. https://id.trulioo.com/Document-Verification-Reference-Paper.html.

COMMENT

Last month, South Korea's Suprema announced it has improved the security on its BioStar 2 biometric access control and time & attendance system.

This seemingly straightforward news story stands out because of the history: last autumn, Suprema suffered unwelcome headlines worldwide when ethical hackers at security firm vpnMentor discovered it had left BioStar 2's 1 million-plus fingerprint records and facial images exposed in an open online database.

The researchers hammered home the point that BioStar 2 is used by thousands of companies worldwide to protect highly secure sites, and integrates with the AEOS access control system that's used by major multinationals, governments, banks and even London's Met Police.

Yet Suprema had left BioStar's biometric data unencrypted and so highly vulnerable. "The unsecured manner in which BioStar 2 stores this information is worrying," vpnMentor said. "Instead of saving a hash of the fingerprint that can't be reverse-engineered, they are saving people's actual fingerprints that can be copied by criminals for varied illegal activities."

At the time, Suprema downplayed the problem, saying: "Some BioStar 2 customer data was accessed by researchers for a limited time. We launched an investigation and immediately closed the access point. No further access has occurred, and the scope of potentially affected users is significantly less than recent public speculation."

But many security experts pitched in to criticise Suprema, just as the superiority of biometric security over passwords was increasingly being taken for granted. Kaspersky principal security researcher David Emm said: "This incident raises the question of whether biometrics are a safe alternative to passwords." And Stuart Reed, a VP at security firm Nominet, called the breach "a huge blow for the biometrics industry".

Now, with the latest version 2.8 of BioStar 2, Suprema has struck a noticeably different tone. It emphasised that, on top of its existing encryption of personal authentication passwords, fingerprint and face templates, BioStar 2 now encrypts all available data that may potentially link to any individual. "This upscaled security will be not an option but a default feature," the company said. And just in case users still hadn't got the message, Suprema CEO Young S Moon added: "We place absolute top priority to strengthen security measures and reinforce our security framework. We will continue to strive to make sure our customers' personal data is protected."

Hopefully, this turnaround shows that biometric tech vendors have understood that, when their products are compared to passwords and other protection measures, they cannot assume security supremacy. The battle is not won. They have to work to earn users' trust.

Tim Ring