State of Biometrics Report

October 2021

Table of contents

Introduction

Dear member

Our third *State of Biometrics Report* comes at a time of flux. Many businesses are opening up, new opportunities are appearing, big changes are happening all around us, and some big challenges still remain. While some organisations are thriving, many others cannot see a clear path to getting back to business, and fear that the future is still very uncertain.

In the last 12 months, much of the world of biometrics has seen a pause in activity. With no face-to-face interaction, the focus is on survival, and this has inhibited the rollout of many planned pilots and new projects. However, we are also beginning to see some new investment moves in places, and we anticipate a wave of business activity as the effects of vaccination programmes are realised. Collaboration – including between standards bodies, government and private sector – has proven to be the most important activity for progress.

COVID-19 has brought an observable degree of rules uniformity across private sector organisations that did not exist before, for example in the use of QR codes for contact tracing and to prove health status, the mandating of social distancing rules, capacity limits and mask wearing. We saw a big move to a less cash-dependent society and reliance on the mobile phone to access services and prove identity, and the digitalisation of health credentials has proliferated.

New operators are appearing in the world of biometrics and this poses new risks where sensitive biometric and health information is potentially being collected and accessed with little control. The level of understanding and oversight that newcomers have of their responsibilities and compliance to regulatory frameworks such as GDPR could influence public opinion and generate further regulatory change.

Face recognition has dominated as the world has focused on remote identification, contactless processing, and the need for the biometric to be captured by devices people have at home. There has been a realisation of the need for digitised services, remote onboarding, and the requirement for identity assurance and liveness verification in those scenarios.

In the borders and travel world, one area where governments, the public and industry agree is that once travel is again underway, it must be safe – with delays and disruptions kept to a minimum. Long queues and mixing of passengers arriving from different countries is not conducive to safety, while physical contact with staff and public surfaces should be kept to a minimum. Some digital health solutions are actively using biometrics or are linked to biometric identity data, and these will contribute to the smooth and timely transit of passengers through terminals.

As we look beyond COVID-19's current grasp on society, what legacy do we want biometrics to have after this recovery programme? And how can biometrics be used for a more resilient future?

The Biometrics Institute celebrates 20 years independently promoting the responsible and ethical use of biometrics this year. We relish the task ahead of bringing together the growing number of organisations using biometrics to share experiences and develop industry-wide good practice.

This third *State of Biometrics Report* provides insights from our diverse and expert membership into the likely impacts on the industry in the coming months.

Isabelle Moeller

Chief Executive, Biometrics Institute

The state of biometrics

Our Future Direction Group has identified five key development areas in biometrics from the last 12 months. The group, which includes government, regulatory and industry experts, has also looked at how these areas will grow further in the coming months.

1 COVID-19 recovery

When we wrote the *State of Biometrics Report* last year, the hope for the world opening up centred on a vaccine being developed. A year on and the prevailing barrier to travel, business and community life is the ability to prove vaccination and testing status, quickly and reliably.

Looking back twenty years, we saw a similar period of disruption as enhanced security screening was implemented post 9/11, creating additional processes, inconvenience and delays for many important aspects of life. Although in recent months we've seen some innovation put into practice[1] to ease administration and queues, overall the challenge of proving COVID-19 status – whether that be to gain access to an event, to board a plane or cross a border – is again resulting in layered processes and delays, hindering business and community recovery.

Borders and travel

COVID-19 has had a particularly devastating impact on the international travel and tourism industry. As of June 2021, International Air Transport Association (IATA) data showed air passenger traffic globally was growing, but still stood at 60% lower than pre-pandemic levels of June 2019.

While individual countries around the world are constantly adjusting entry requirements, the impact of COVID-19 on travel is less seamlessness and more manual processing, coupled with very high uncertainty. New requirements and new systems also introduce new policy and data protection challenges.

The current response to coronavirus is to make use of health certificates to aid the safe reopening of society and borders. Many of the credentials used currently pose significant counterfeiting concerns. Security and integrity of these credentials, whether physical or digital, could be enhanced through identity binding with the use of biometrics. The challenge in the coming months will be to ensure the sensitive application of biometrics in this area in a reliable, sound and ethical way.

The crisis has massively accelerated the digital transformation agenda for government and non-government organisations, and we have seen unprecedented levels of cooperation and collaboration between stakeholders across the spectrum focusing on safely restarting international and domestic travel. Airports and airlines are moving towards more contactless self-service solutions for safety and efficiency, as well as for savings, as they plan commercial recovery.

Contactless and digital identity for travel

Coronavirus has heightened awareness of physical contact and proximity with strangers in confined spaces. Touchless biometric technologies have proven their ability to meet this challenge. The use of face biometrics within the US Customs and Border Protection (CBP) biometric border systems continue to demonstrate the value of biometrics to border processing, while also promoting the safety aspects of touchless processing for entry into the US under the Simplified Arrival scheme[2], for example.

Governments globally are now issuing digital health certificates linked to national identity or health schemes, and are beginning to accept health certificates issued by other countries to assist with international travel. Vaccine pass apps are being piloted by airlines[3] to demonstrate proof of negative test results or vaccination status, with some underpinned by biometric identity assurance measures.

Some governments have taken steps to link the vaccine credential to the individual's biometrically assured identity document. For businesses and governments that require strong proofing behind a health pass, the use of biometrics to anchor identity, and then link the health record and health assertion provides confidence. Without this assurance, the impact of fraudsters who get through the system could be devastating for businesses (who have to shut down as the result of positive cases), the healthcare systems (which may not be resilient to huge strain in many tourist destinations), and the governments that have to manage new outbreaks.

Digital identity schemes are also being promoted to facilitate travel, at a domestic and international level. The International Civil Aviation Organisation (ICAO) has released initial standards for its digital travel credential[4] which includes key information from the ePassport chip, and for the Visible Digital Seal (VDS)[5]. The VDS has been proposed for use in proving health status of travellers and leverages existing ICAO public key cryptographic infrastructure for certificate assurance.

Global trust frameworks

As governments have stepped up their plans to keep borders secure and their people safe, organisations have looked to digital solutions to facilitate checks and manage risks. There has been no shortage of innovation in this area, although policy is having to play catch up at times. We all recognise that the current health challenge is unprecedented in its breadth, taking in every country and principality in the world, but the risks of managing sensitive and personal data are also real. The related policies and methodologies must align with appropriate laws, controls, and oversight mechanisms for every jurisdiction.

The Biometrics Institute's *Three Laws of Biometrics*

At this point, the extent of variables and differences between countries globally precludes the possibility of a universal solution to manage health. The ongoing direction of the pandemic remains fluid and whatever systems are implemented today must adopt an agile and flexible framework that can adapt to the rise and fall of the threat or risk. The key then, is to adopt an integrated and flexible global framework of solutions that can deliver trust. The Biometrics Institute's *Three Laws of Biometrics*[6] and its *Good Practice Framework*[7] provide best practice principles and guidance for organisations considering the use of sensitive personal data .

Verification for large events

Verification of identity and vaccination or testing status at large events brings with it factors not present in the more rigid atmosphere of the airport. Sports and entertainment events alike seeing thousands of excited people converging on an entry point at the same time, needing to prove their ID and health status on perhaps a poorly lit or damaged screen. What are the impacts of a biometric solution replacing that lengthy wait? Biometric modalities could have a valid use to increase the efficiency of practical COVID-19 checks at large events, as well as facilitate contact tracing.

People-counting technology using face biometrics could ensure COVID-19 capacity of venues like pavilions and conferences are not exceeded. A biometrics system could exclude employees and exhibitors, not count the same person twice and efficiently take into account exits and entries.

There may be organisations who are now considering the significant value that a biometric solution can offer for their COVID-19-safe challenges, and who also need to ensure they have the right processes in place to manage the risks of using the technology.

2 Digital identity

The 2021 Biometrics Institute *Industry Survey*

In this year's Biometrics Institute *Industry Survey*[8], the majority of respondents said they believed digital identity to be the main area of significant biometric development over the next five years. More than 90% of industry professionals agreed that biometrics will be the key enabler for anchoring digital identity and that there will continue to be significant growth in mobile remote identity verification systems and remote onboarding technology.

The pandemic has been a driving impetus for digital transformation. We have seen increasing interest and usage of digital identity across government, private sector organisations, and citizens, particularly in attaching health credentials as part of a so-called vaccination passport.

National identity frameworks

A trend last year, supporting the renewed focus on remote services, has been the growth and impact of national digital identity frameworks. Many relevant authorities, such as those in Australia, Singapore and the EU, have made significant progress in developing and rolling out these identity frameworks recently, aiming to drive economy-wide benefits from digital identity usage.

In the UK, a recent consultation[9] asked for views on how a digital identity system should operate. It requested input on how to allow certain organisations to make digital checks against government-held data, how to establish trusted, legally valid digital identities in place of passports or bank statements as identity documents, and included proposals for a governing body to keep organisations in line with the government's rules.

Earlier this year, the UK government published a draft of the *UK Digital Identity and Attributes Trust Framework*[10]. This set out what rules and standards are needed to protect people's sensitive identity data when used digitally. The Australian government published version 1.2 of its *Trusted Digital Identity Framework*[11], and several digital identity providers are accredited under that framework. Key aspects of these frameworks are around ensuring trust in both the digital apps and the processes underlying any service requiring tight identity binding using biometrics.

Interoperability and re-use

As digital identities are used by more people in more contexts, a critical new question is are all these different digital identities necessary? In this context many organisations are looking into ways to avoid expanding the set of digital identities a consumer needs to hold, at least in part to reduce the burden on individuals of digital identity management.

This is leading to a number of concepts being explored by digital identity users:

1. Re-use, where an existing digital identity is able to be used in a new context
2. Interoperability, where two (or more) different types of digital identity are able to be used interchangeably

Re-use is becoming clearer as a mechanism for especially private sector organisations to effectively outsource digital identity management – perhaps using an existing digital identity mechanism supplied by another organisation to onboard customers. Interoperability, while perhaps less advanced, seems to be of greater significance between digital identity mechanisms such as nation-to-nation. In that context, national identity schemes are exploring whether they can use the identities of other nations – and, if so, any limits around that re-use.

Re-use and interoperability both lead to a range of biometric-related issues, such as:

- Can all parties agree on mechanisms for identity proofing? For example biometric vs non-biometric and which mode or modes of biometric to be used
- If there isn't agreement on mechanisms for identity proofing, how can parties compare the standard of the identity proofing performed? Can appropriate standards be created to underpin this?
- Is consistent testing of biometric identity proofing mechanisms available for parties to trust in assessing digital identities created by others?
- Are there privacy risks in connecting together different digital identities[12]?
- How can these complex issues be communicated to consumers, especially considering the other complex elements of digital identity and re-use?

The continuing development of especially national digital identity frameworks is expected to increasingly include re-use and interoperability as material components. Whether national in nature or private-sector-driven, ultimately the aim is to allow an app or services certified for use in one context or national identity framework to be recognised as certified in another context or framework, whilst preserving the integrity and trust of the original scheme.

We believe there is substantial work to be done to bring this to fruition, and the Biometric Institute's global network allows us to facilitate discussion to explore these issues across all stakeholders.

Self-sovereign digital identities

Greater consumer control over digital identity still looms as a theme, although advancements in this field have been relatively slow. Perhaps the most significant movements to date have been recognition by both centralisation-focused and self-sovereignty-focused parties of the merits and utility of the views of their counterparts at the other end of the spectrum. Some self-sovereignty stakeholders have taken steps towards recognising the value in anchoring identities to a centrally held record system. Some centralised identities provide increased user control over what kinds of information they expose when presenting elements of a digital identity.

A related subject gathering increasing attention is distributed ledger technology such as blockchain. The immutable nature of distributed ledger intersects with fundamental aspects of identity and with biometrics, and the extent to which self-sovereign identity might rely upon, or at least be entwined with, such ledger systems is a developing field. It is yet to be seen whether distributed ledger underpinning biometrics and digital identity at scale in either government or private sector is achievable. The extent to which biometrics might be used in the opposite context is also unclear, for example a use case like supporting certain types of anonymous digital currency holdings that are nonetheless usable by the owning party.

Ramifications in the real world

As biometric-powered digital identity intersecting with digital COVID-19 health status increases in scope and consumer engagement, a range of real-world impacts and consequences are becoming apparent across the lifecycle of digital identities.

While counter-terrorism has taken something of a backseat while the COVID-19 storm has raged, these concerns may also creep back up the agenda in many countries as terrorist organisations become emboldened and adopt new emerging technologies to inflict atrocities.

As digital onboarding has dramatically grown in usage over the last year, so has usage of various biometric technologies to support this. Chiefly this is around the use of biometrics and document authentication services to prove linkage to a trusted real-world identity, otherwise known as proofing. This usually uses facial recognition to compare the new customer's selfie against a trusted, often government-issued, document. To support this, the use of liveness detection to protect against various spoofing attacks has also greatly increased. We expect this usage of biometrics to continue to grow even after the COVID-19-driven necessity for remote onboarding recedes.

With digital identity creation at a national level, two key groupings appear: those who already have a national identity scheme, and those who do not. This split affects biometrics and digital identity in many different, sometimes subtle ways. For instance, nations with national identity schemes have an existing structure on which to build consumer awareness and indeed the identities themselves. However, those nations without such schemes have perhaps greater flexibility to align the objectives, implementation and consumer engagement with digital identity with today's issues and challenges in mind, rather than being associated with earlier identity models.

Biometric authentication of digital identities, once a fairly stable field related to customer service delivery, continues to evolve in several directions. Passive and behavioural biometrics to perform ongoing authentication are increasingly important, in part to drive down consumer friction and increase the convenience of engaging with and paying for products and services. From a technical perspective multi-factor biometrics seem likely to increase in importance, largely to drive up the difficulty of mounting certain types of attacks on digital identity authentication mechanisms.

The Biometrics Institute's *Digital Onboarding and Biometrics* paper

Consumer concerns around digital identities are bubbling up too. The relationship with biometric technology and whether there are unintended consequences of using biometrics for digital identities – perhaps leading to unwanted joined-up surveillance both on-device and connected to real-world cameras – is a continuing issue in consumer minds. This is not helped by irresponsible actions of some, nor by some of the more sensationalist media coverage. Challenges around fraud and digital identity recovery and the responsibilities and liabilities of the various parties involved are also likely to come sharply into focus, especially as parties rely ever more on identities created and controlled by others.

We discuss these issues and more in our *Digital Onboarding and Biometrics* paper[13].

3 Governance

As biometric modalities continue to evolve and be explored, the need for robust governance, guidance and legislation is as important as ever to safeguard the rights and freedoms of individuals.

Legislation is naturally subject to change as governments come and go. It can also vary widely between jurisdictions and cultures, as can methods and capabilities related to enforcing legislation. However, the general public's expectations of governments or organisations which process its biometric data remains the same – respect for the personal privacy and general security of individuals. And while recognising the centrality of individual impacts, these governance frameworks should not inhibit innovation, but should provide appropriate support for the necessary and proportionate use of biometric technologies and the subsequent processing of biometric data.

In its January 2021 briefing note on ethical issues around public-private use of live facial recognition[14], the UK Biometrics and Forensics Ethics Group (BFEG), highlighted the need for independent oversight. Effective independent oversight and reporting mechanisms are an important component of governance at the national level, remaining outside of the political sphere while highlighting procedural and policy gaps.

As overall accountability sits with organisations themselves, the role of independent oversight should also be recognised and respected. Especially in relation to the processing of more sensitive categories of data, organisations who make decisions over how they use biometrics should be held accountable in a fair way by regulators, civil society groups and even the general public. Leading regulators in the field of data protection, biometrics and surveillance have an important role to play by upholding individuals rights, promoting governance and good practice, and taking action where organisations do not comply with particular legal obligations.

In terms of processing biometric data, the Biometric Institute's *Three Laws of Biometrics* (**Policy** first which drives **Process** accountability to enable responsible **Technology** implementation) encourage organisations to 'know their algorithm'. But organisations must also have a fundamental awareness of whether or not the data they are processing is in fact biometric in the first place, and have clearly identified the vulnerabilities, limitations and associated risks.

By taking a risk-based approach and a 'data protection by design and default' approach as established by the *General Data Protection Regulation* (GDPR), both large and small organisations can make informed and responsible decisions about whether the use of biometric technologies is necessary and proportionate in the circumstances. By understanding the nature of the data that is being processed, the internal governance arrangements can be adjusted accordingly to help mitigate any risks.

Legislation

Globally, there have been continued calls for formal bans or moratoria regarding the use of biometric technology in public spaces. On 21 June 2021 the European Data Protection Board (EDPB) spoke of the 'extremely high risks'[15] it saw posed by remote biometric identification of individuals in public places, stating that, along with the European Data Protection Supervisor, it calls for, 'A general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context.'

In the US, talk of bans and moratoria are showing no signs of abating. Portland, Oregon has added its name to the list of states and cities banning facial recognition technology. While bans exist in California and Massachusetts, including San Francisco and Boston, Portland is the first to preclude businesses from using the technology.

The American Civil Liberties Union (ACLU) of Michigan and the University of Michigan Law School have filed a lawsuit[16] to force the Detroit Police Department to change its policies on facial recognition. It comes after Robert Williams spent time in custody after a false match by the force's facial recognition technology.

Senator Jeff Merkley, one of the sponsors of the 2020 bill to pause the use of facial recognition, said we cannot wait for private companies to self-impose moratoria on the technology. The Facial Recognition and Biometric Technology Moratorium Act was reintroduced in June 2021[17].

On the industry side, Amazon and Microsoft have both paused selling facial recognition software to law enforcement[18], while IBM pulled out of the market altogether, calling for a 'national dialogue' on its use by police. Amazon and Microsoft say they are waiting for federal legislation to be put in place before revisiting this decision.

Even before such arguments gained momentum, the GDPR restricted the processing of biometric data to situations where a clear lawful basis is identified, and requires that such use is clearly documented alongside the data protection impact assessment it mandates for any type of processing which is likely to be high risk.

Where bans are not adopted, strong restrictions may still apply. As outlined in the UK Information Commissioner's published *Opinion on Live Facial Recognition in Public Spaces*[19], the commissioner provides certain recommendations to technology developers in light of data protection law including:

- Installing data protection by design and default into new technological developments
- Addressing and reducing the risks of bias and discrimination in systems and associated algorithms
- The adoption of common standards to assess statistical accuracy in systems

As solutions are rushed through to manage a pressing need, it is critical that biometric modalities are not implemented under the radar of information governance or under the guise of safeguarding public health but in reality for alternative purposes. As always, any implementation of biometric technology should be lawful, necessary and proportionate in the circumstances.

Public perception and ethics

The MIT Technology Review[20] estimated that in 2019, more than 26 million people had voluntarily submitted their DNA samples to a private company for genealogy tracing, predicting the number would rise to 100 million by 2021. So why is there such concern about the gathering of other biometric data like face recognition for retail and advertising? Perhaps at the core of this issue is the human sense of control. There is a great difference in the human mind between choosing to do something and being made to do that same thing. Where the purpose for the collection is not clear, or does not seem warranted or fair, problems arise.

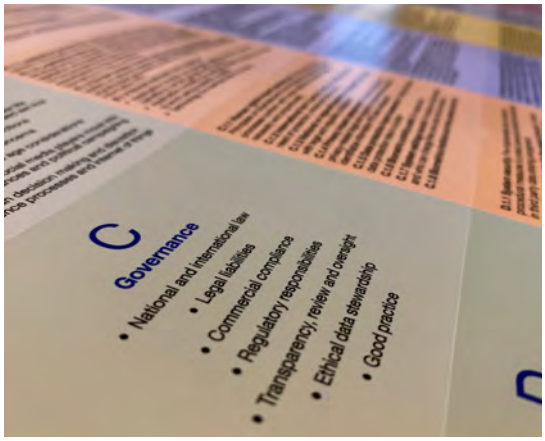
The Biometrics Institute's updated *Privacy Guidelines*

Public perception of biometrics is still a critical issue and the balance in the debate is still weighted more towards cost benefits and less towards benefits to society. As people see the benefit of using digital identities to establish their health credentials and quickly gain access to work, travel or entertainment, perhaps this balance will shift. That will only happen, however, if the expansion of use cases is accompanied by increased public understanding and growing level of trust for the reliability, fairness, and protection of the data in such systems.

Data ethics[21] is an important part of any discussion on implementing biometric technology. How is fairness assessed and who is ultimately responsible? This year we revised our *Privacy Guidelines*[22] to include two brand new principles. The first is around the need for a communications plan which explains the pros and cons of using a biometric to ensure maximum understanding among both the public and the organisation's own employees. The second is for law enforcement to ensure that even when there is an exemption under the law, actions are ethical and sensitive to community expectations and human rights. These guidelines are freely available to members and offer ethical and practical advice about obtaining a genuine balance between technology and human considerations.

Openness and honesty from those capturing, storing and sharing biometric data, and consent from those giving it will be critical to the expansion of programmes generated through outsourcing to the private sector or through joint partnerships between governments and the private sector. These currently include vast swaths of society like telecommunications, banking services, census collections, security, education services, transport, research, health provision and certification, pay-as-you-go taxation collections and energy services. As the exchange of personal information between sectors continues to advance, consumer awareness and consent should be front and central in developing or managing major projects.

Good practices are critical for users of biometric technology in this changing arena. Our good practice guidance includes The *Three Laws of Biometrics,* the *Good Practice Framework* and our *Privacy Guidelines.*



The Biometric Institute's *Good Practice Framework*

Accessibility and inclusion

The use and usefulness of the mobile phone has grown exponentially since the outbreak of COVID-19, as a contactless means to pay, as a means to check in to a venue, and to digitally onboard for services in the absence of face-to-face interaction. But in terms of the greater uptake of using personal smart phones in travel and border control or access to certain venues, there can be wider ethical considerations to mandating vaccination and the requirement to access health credentials within a mobile app.

Not everyone has the same level of access to personal technology, and could in theory be denied products and services because of this, especially if there are no alternatives in place. If a contactless biometric system that enables international travel or access to a large event is solely reliant on individuals possessing a smart device, this could be problematic to the initiative if individuals freely choose not to own one, or are not able to. Some jurisdictions are issuing physical documents such as QR code printed cards to provide just such an alternative, for example to seniors without smart phones.

Consideration has to be given to the rights and freedoms of individuals, and the impacts on these rights, based on the choices individuals make and the opportunities available to them. There is a potential risk of splitting society into different groups based on their ability to obtain personal technology, or to buy into a particular biometric or health initiative.

Standards and testing

There have continued to be positive developments in international standards at both the detailed technical level as well as at a framework level. In international standards the release of the updated Biometric Performance Testing and Reporting ISO 19795-1 2021[23] is a significant advance in aligning terminology and in terms of detail. In the area of open standards for biometric systems, the Secure Identity Alliance (OSIA)[24] initiative is gaining significant support and progress. OSIA aims to enable open API connectivity between all components of the identity management ecosystem – independent of technology, solution architecture or supplier.

Along similar lines, the Modular Open Source Identity Platform (MOSIP)[25] is building and deploying an open-source framework for foundational ID systems in low to middle income countries and has deployed several implementations – including the new Philippines identity system.

Also this year, ANSI/NIST published best practices recommendations to their fingerprint standards[26] to allow for the creation of contactless fingerprint transactions that are not readily ingestible by existing systems.

And several organisations have been focussing on the creation of digital vaccine certification standards to support the scalable growth of post-COVID travel including IATA Travel Pass, the EU Digital COVID Certificate (DCC) and the UK NHS COVID Pass.

As with most things this year, the pandemic has changed priorities with respect to testing. Over the last few years the focus of testing has moved from 1-N matching accuracy, through matching performance on age to demographic differences – all including facial features such as the eyes, nose, and mouth. As a result of the pandemic, performance in identifying and verifying individuals wearing face masks has been added to the list of imperatives.

How mask testing is conducted is also an emerging issue. There are no large volume 1-1 databases of people with and without masks. As a result testing organizations have been digitally applying face masks to existing photos. However, a digital mask applied to an image is not necessarily the same as a photograph of a person wearing a face mask - and accuracy results will not necessarily be the same because digital masks do not show the contours of features such as noses or cheekbones under the mask, nor conversely do they generate the plethora of printed patterns or different edges that may be on the mask itself.

In its first report on masks published in July 2020, NIST tested pre-pandemic algorithms[27] that had already been submitted. It found than even the best of the 89 commercial facial recognition algorithms tested had error rates of between 5% and 50% in matching digitally-applied face masks with photos of the same person without a mask.

The second update released in November 2020[28] found that all algorithms submitted after the start of the pandemic continued to give increased false non-match rates when the probes were masked. While this is not surprising due to the reduced facial surface area the algorithms have to work with, we anticipate strides forward in the ability of mask-aware algorithms in the coming months. NIST researchers noted that some algorithms submitted after March 2020 already showed significantly improved accuracy. We will be watching this area with interest.

4 Commercial use of biometrics

There has been a lot of focus in recent years on government use of biometrics. However, the technology is becoming more prevalent across all areas of society. Private businesses and private citizens now have access to biometric capabilities and large biometric datasets.

What should be done to prepare us for a world where anyone can take any footage from anywhere[29], and run it against massive databases to identify everyone? What does that mean for your social media profile, for attending a televised sporting event, and for being in a society where technology is everywhere, and everyone is carrying – or wearing – a camera?

Privacy as we know it may look very different in the future and the Institute will closely engage in discussions on this issue.

The benefits of biometrics in the private sector

Biometrics assist enormously with many of the current challenges faced by the private sector, and bring big benefits for businesses and consumers in relation to security, service, and savings. Businesses are looking to automated solutions to manage employees and customers. In-store cameras profile customers for the purpose of targeting sales, or detecting shoplifters, and in several jurisdictions we will need digital vaccination passports to get into venues or attend events.

Risks

In its report on public-private collaboration of live facial recognition (LFR) in privately owned spaces[30], the UK Biometrics and Forensics Ethics Group (BFEG) summarised, 'It was clear that the use of biometric recognition technologies (including LFR), in private-public collaborations… are likely to increase.' The BFEG report outlined risks and recommendations related to privacy and data sharing within these schemes, and also to processes related to the management and population of watchlists, where people could be added to watchlists by companies or by police in different circumstances.

In June the UK Information Commissioner's Office also published its opinion on the use of LFR in public places by private companies and public organisations, building on its previous opinion on LFR for law enforcement use[31]. In addition to outlining the need for data protection impact assessments, proportionality, risk mitigation, and process controls, it emphasised the need for accuracy in solutions.

There are situations where risks related to public safety may clearly justify private and public sector collaboration with biometrics, if adequate controls are in place. Robust frameworks to guide ethical use for public and private organisations are readily available, like the Institute's *Good Practice Framework.* However, while talk of bans and moratoria on government use of biometrics have attracted our attention, legislation covering private sector use is either absent or confusing at best. It is uncertain whether businesses, including small businesses, are aware of the risks and the necessary controls for using this technology and can put those controls in place. Do businesses know exactly how data is managed and whether biometrics are being used? If a business is seeking information about age or gender for targeted advertising, do they know exactly what is being collected, connected, disclosed, and retained? Do consumers know when their biometrics are being captured and what is being done with their image? If misuse occurs and if people are harmed, what sanctions and what private rights of action exist under law?

This year, media reporting on the storming of the US Congress in January 2021 highlighted the ability for not only law enforcement, but also private citizens to use online biometrics services to identify individuals using news media images[32]. Images of protestors were uploaded into websites which matched them to images scraped from the internet, allowing them to be identified publicly including to friends, relatives, and employers.

We also saw reporting on the rapidly evolving field of deepfakes, and convincing videos of a deepfake Tom Cruise. The Cruise deepfake creator himself said he wanted to show what would be possible with a simple Snapchat filter in a few years and advocated stronger legislation to prevent misuse[33]. Certainly another example of how rapidly evolving and increasingly available AI technology is challenging our society.

5 Future directions

Much of this year has been driven by technology that is responding to the COVID-19 pandemic. Due to everyone working or schooling from home during the pandemic, there has been a pressing need for remote identity verification. Remote identity software typically operates by taking a selfie photo or video of a person, and comparing it with a known identity document held by that person. The document is then checked to determine if it is genuine and the selfie face is matched to the ID photo image from the document. A liveness check is also typically performed. Certification programmes for these applications, like FIDO IDWG[34], are under development.

As outlined in this report, touchless recognition is getting a boost due to COVID-19. Of course, face recognition is naturally touchless and many systems are using face. For fingerprint recognition, non-contact fingerprint systems include those which involve a photograph of the fingers, taken with a mobile device. There are also systems which are a kiosk where an individual holds or waves their hand across a sensor. Continued standards development and expanded testing is underway as this technology matures.

In order to support remote biometric recognition, liveness (also known as presentation attack detection) has matured. Most systems now incorporate some form of liveness check and many of them have gone through independent testing. While the anti-spoofing landscape is much better than previous years, adversaries will likely increase the frequency and complexity of presentation attacks. Investments need to be made to improve our abilities to mitigate these attacks and detect and counter them faster and with greater confidence.

As digital identity capabilities mature and expand across government and private organisations, there will be new options in how policies and governance are planned and implemented as we advance interoperability and achieve improved responses. A centralised approach offers a strong central governance structure along with its associated protocols and standards. A de-centralised approach relies heavily on point-to-point agreements across independent, interdependent organisations. Hybrid organisations implement portions of centralised and de-centralised concepts. Further analyses, research, and development in this area should prove helpful to capability progression.

The use of technology exemplified by police and the general public to identify those who stormed the US Congress, and the incredibly believable deepfakes emerging online set the scene for the coming months and years when considering what next for the use of biometrics. Digital still photo image morphing and deepfake videos will continue to attack vectors in a world where remote enrolment for services becomes more and more prevalent. Deepfake attacks will be combatted by machine learning of their characteristics such as face representation vs its background, video blurriness, facial glitches, jerky movements and inconsistent lighting.

We also anticipate seeing a gap in understanding of what constitutes responsible and ethical use of biometrics, and reasons for usage, emerging between private and public sector use cases.

The Biometrics Institute serves as a membership organisation for any organisation using biometrics and we will work to bridge this gap and share our good practices where they are needed.

Likely this increased awareness of biometrics available to everyone and anyone will drive governments closer to regulation and implementing oversight mechanisms for private sector use of biometric technology.

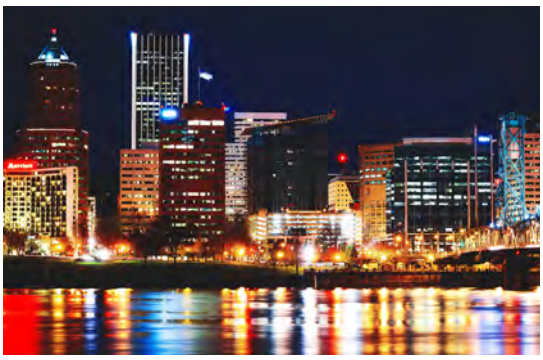
In the news, 2020-2021

AUG 2020

- Coded bias review: An eye-opening account of the dangers of AI

SEPT 2020

- Portland, Oregon bans face biometrics for businesses and local police



The US sees more facial recognition bans

OCT 2020

- NY researchers develop 3D finger vein biometric authentication
- Facewatch at the Co-op

NOV 2020

- Australian Government prepares digital identity service to enhance myGov platform

DEC 2020

- Regulating facial recognition - technology in the private sector

FEB 2021

- The UK government set out its vision for the rules governing the future use of digital identities
- How normal people deployed facial recognition on Capitol Hill protesters
- Northwestern sued over biometrics privacy in test proctoring software
- Europol warns fake negative COVID certificates being sold across Europe

Facial recognition is now freely available using a website called Pimeyes

Digital drivers' licence popular in New South Wales

MAR 2021

- UK Uber drivers claim company uses flawed facial recognition biometrics which prompted the former employees' firing
- FBI issues warning over deepfakes
- Disney trials face-based biometric entry system at Magic Kingdom

APR 2021

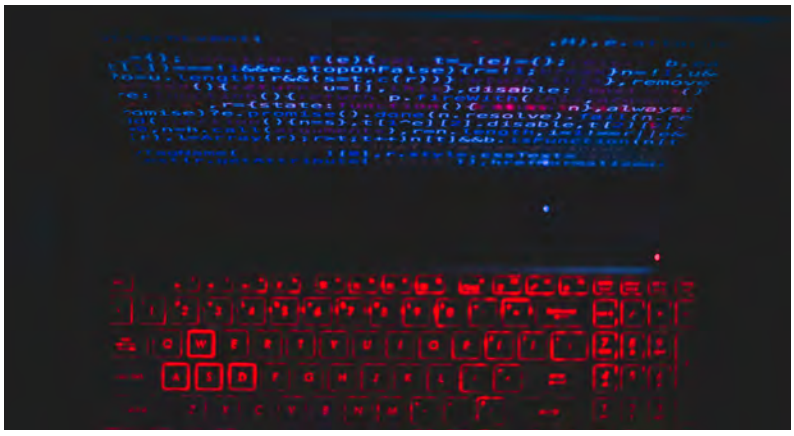
- Travel restrictions: Plans to digitally link UK travellers' COVID documents to passports to cut airport queues

MAY 2021

- Amazon extends moratorium on police use of facial recognition software
- More than half of NSW drivers have adopted a digital licence
- Over 180 musicians protest Spotify's speech monitoring patent in open letter over speech monitoring
- Cheese photo leads to Liverpool drug dealer's downfall - vein identification leads to arrest
- NIST kicks off public discussion about creating trust in AI
- Keeping a close eye on remote workers puts noses out of joint

JUN 2021

- NIST proposes approach for reducing risk of bias in artificial intelligence
- Brazil tests the world's first facial recognition shuttle service
- McDonald's AI drive-thru bot accused of breaking biometrics privacy law



NIST asks for help to reduce risk of bias in AI

About the Biometrics Institute

The Biometrics Institute is the independent and impartial international membership organisation for biometric users and other interested parties. It was established in 2001 to promote the responsible use of biometrics and has offices in London and Sydney.

With more than 800 members from 230 member organisations spread across 34 countries, it represents a global and diverse multi-stakeholder community. This includes banks, airlines, government agencies, biometric experts, privacy experts, suppliers and academics.

The Biometrics Institute connects the global biometrics community. It shares knowledge with its members and key stakeholders and most importantly, develops good-practices and thought leadership for the responsible and ethical use of biometrics.

References

1 https://inews.co.uk/news/travel-restrictions-uk-travellers-digital-link-covid-documents-test-form-passports-airport-queues-964190

2 https://www.cbp.gov/newsroom/local-media-release/cbp-expands-simplified-arrival-washington#:~:text=Simplified%20Arrival%20is%20an%20enhanced,admission%20into%20the%20United%20States

3 https://www.futuretravelexperience.com/2021/02/british-airways-to-trial-verifly-digital-health-passport/

4 https://unitingaviation.com/news/security-facilitation/replacing-a-conventional-passport-with-digital-travel-credentials/

5 https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf

6 https://www.biometricsinstitute.org/the-three-laws-of-biometrics/

7 https://www.biometricsinstitute.org/biometrics-institute-good-practice-framework/

8 https://www.biometricsinstitute.org/press-release-digital-identity-the-most-significant-development-in-the-use-of-biometrics-survey-finds/

9 https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation

10 https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework

11 https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework#:~:text=Trusted%20Digital%20Identity%20Framework%20The%20Trusted%20Digital%20Identity,templates%20to%20support%20providers%20to%20meet%20TDIF%20requirements.

12 https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

13 https://www.biometricsinstitute.org/press-release-new-guidance-on-digital-onboarding-with-biometrics/

14 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/953359/LFR_briefing_note_18.1.21.final.pdf

15 https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

16 https://www.aclu.org/press-releases/michigan-father-sues-detroit-police-department-wrongful-arrest-based-faulty-facial

17 https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology

18 https://www.reuters.com/article/us-microsoft-facial-recognition-idUSKBN23I2T6

19 https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

20 https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/

21 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/06/what-s-next-for-data-ethics/

22 https://www.biometricsinstitute.org/institute-joins-calls-to-make-privacy-a-priority-with-updated-universal-guidelines/

23 https://www.iso.org/standard/73515.html

24 https://secureidentityalliance.org/osia

25 https://www.mosip.io/index.php

26 https://www.nist.gov/publications/contactless-fingerprint-capture-and-data-interchange-best-practice-recommendation
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8307.pdf

27 https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-6a-face-recognition-accuracy-masks-using

28 https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-6b-face-recognition-accuracy-face-masks

29 https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/

30 Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology (accessible) - GOV.UK (www.gov.uk)

31 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

32 https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/

33 https://www.theguardian.com/technology/2021/mar/05/how-started-tom-cruise-deepfake-tiktok-videos

34 https://fidoalliance.org/identity-verification-binding/

Biometrics Institute

www.biometricsinstitute.org | manager@biometricsinstitute.org

Asia-Pacific PO Box 576 Crows Nest NSW 1585 Australia | Australian Business Number: 81 098 407 099

Europe 66 Prescot Street, London E1 8NN United Kingdom | UK Company Number: 7717293