BIOMETRICS INSTITUTE

Two decades of biometrics

A story of responsible use

October 2021

Contents

1. Introduction

The purpose of this report is to mark the 20-year anniversary of the Biometrics Institute on the 11 October 2021. More importantly, however, this report celebrates the work of the Biometrics Institute over the past twenty years, which together with the support of its members, has provided a platform for a balanced discussion promoting the responsible and ethical use of biometrics and a deeper understanding of the biometrics industry.

Biometrics Institute and its member community

We are a global, independent, multi-stakeholder community representing government, practitioners, suppliers and academics whose achievements in the areas of privacy and policy; technology innovation and research and development have led to the successful launch of products and services creating jobs and opportunities, as well as leading to breakthroughs in science and technology applications.

By highlighting the many success stories of more than thirty members, this report demonstrates how biometrics products and services have made a positive impact in society: combining high security with convenient access; delivering fraud reduction solutions; providing biometric search algorithms for disaster victim identification, and law enforcement through fingerprinting and DNA profiling.

Now, more than ever, the biometrics community needs to find its voice

Concerns over data security and privacy and not attending to cultural, social, and legal considerations have led to misinformation and debate on how different use cases can pose risks as well as opportunities.
By providing a range of thought leadership and guidance materials, facilitating knowledge transfer, and acting as a connector to the biometrics community, the Institute and its members are working towards good practices to ensure the responsible and ethical implementation of biometrics.

2. Chairman

From humble beginnings in 2001, the Biometrics Institute has developed into a key global forum for the exchange of information relating to biometrics. Starting with a reputation for providing quality events that bring thought leaders and practitioners together, the Institute has moved also to being a policy and procedural leader for governments, private sector and community organisations seeking to use biometrics to meet a range of their business and day-to-day activities. These days, the Institute is positioned on the global stage, its members representing all regions of the world and its Board reflecting the shared engagement of governments, business and academia in furthering the responsible and ethical use of biometrics. For those of us working in organisations that use biometrics, it has been a great help over the years when faced with a business challenge to be able to reach into the Institute and find peers across the world faced with similar challenges and able to offer ideas for their solution. The next 20 years promises to be as successful.

Andrew Rice
Chairman and Director, Biometrics Institute
director@biometricsinstitute.org

3. CEO

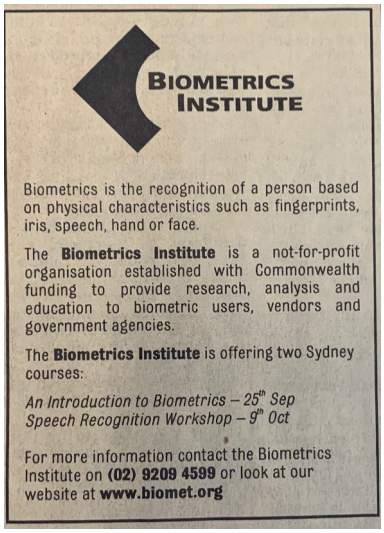
What did we know about biometrics in 2001?

When I applied for my first position at the Biometrics Institute in April 2002, of course I wanted to prepare myself for the interview, so I searched the internet for the term "biometrics". There were very few results and the few articles I found focused on law enforcement use of fingerprints and DNA. I also learnt that the Biometrics Institute was established to promote the responsible use of biometrics, a mission that has remained unchanged ever since its foundation and has become a widely accepted term. It's founding members included the Australian Department of Home Affairs, Department of Foreign Affairs & Trade, Australian Taxation Office and Australian Federal Police.

Australia had started to look at biometric technology pre-9/11 to help facilitate passenger flows into Sydney airport. During early consultations about the Institute's role, it became apparent that what the industry needed most was an independent body which provided information sharing opportunities and to address user concerns such as privacy.

Then the sad events of 9/11 took place and placed biometrics centre stage as a tool that could help thwart the terrorists desire to hide. By chance on the very date of 11 September 2001, *The Australian* newspaper published an advert announcing the establishment of the Biometrics Institute.

Our mission: Promoting the responsible use of biometrics since 2001 as a user group


BIOMETRICS INSTITUTE

Biometrics is the recognition of a person based on physical characteristics such as fingerprints, iris, speech, hand or face.

The **Biometrics Institute** is a not-for-profit organisation established with Commonwealth funding to provide research, analysis and education to biometric users, vendors and government agencies.

The **Biometrics Institute** is offering two Sydney courses:

An Introduction to Biometrics – 25th Sep
Speech Recognition Workshop – 9th Oct

For more information contact the Biometrics Institute on **(02) 9209 4599** or look at our website at **www.biomet.org**

The Biometrics Institute was formally established on the 11 October 2001 as a user group giving organisations using the technology more power to set the strategic direction for the organisation. Through its independence and by being self-funded through membership and events, it was able to attract key government organisations to join. Today we are proud to represent 79 government/public organisations from 22 countries. But the real value of the Institute lies in the diversity of its stakeholder community including government members, suppliers, academia, aviation and financial sectors, privacy experts and as observers several international organisations including United Nations agencies, EU institutions and regulators.

Addressing Big Brother concerns in 2006

In the early years of my time at the Institute we started seeing media headlines which often focused on fears of "Is Big Brother watching you? " The Australian Privacy Act at the time dated back to 1977 and the then Privacy Commissioner encouraged the Institute to write the voluntary ***Biometrics Institute Privacy Code*** under Australian privacy law to address the responsible use of biometrics through a set of guiding principles. For the first time the Institute addressed a gap in legislation by acting in consultation with its members to manage potential risks around biometrics. When the Australian Privacy Act was revised in 2012, the Code was deregistered as it was no longer required, having biometrics addressed in the new legislation. By then the Institute had a global membership and once again in consultation with its members decided to launch its ***Privacy Guidelines***. It was a first major milestone for us that put privacy and biometrics at front of mind of all future discussions.

The year 2008 - What about spoofing and liveness?

Performance and accuracy testing by then were well established, but spoofing was a topic that was not something the industry was that keen to talk about. However, in 2008, we secured government funding to develop a methodology that would help assess how easy or hard it is to spoof a biometric system. It created a lot of attention and caused some concern how secure biometric systems really are. Rather than setting up a testing facility we decided that we needed to raise awareness about this topic globally and develop standards and stress the importance of testing to manage the risk. In 2010, we formed the ***Biometrics Vulnerability Assessment Expert Group (BVAEG)*** including 16 members.

Today we have ISO standards (ISO/IEC30107) and companies conducting vulnerability testing.

Going global in 2011 with offices in Sydney and London

Ten years into our existence, we were servicing 111 organisations from Australia and New Zealand and had member organisations in Europe and the USA. The Board of Directors and I agreed that we should go on a discovery journey to test whether we could expand our outreach into Northern hemisphere more proactively. I relocated to London, closer to my home turf Germany and the Australian High Commission hosted our Launch Reception in October 2011 at the beautiful Australia House, the first Australian overseas mission. There could not have been a better venue.

Engaging with the biometrics community in Europe and creating a network for the biometrics industry, we ran several networking events and a first UK Showcase was held in 2012, with a second in 2013 hosted by RBS.

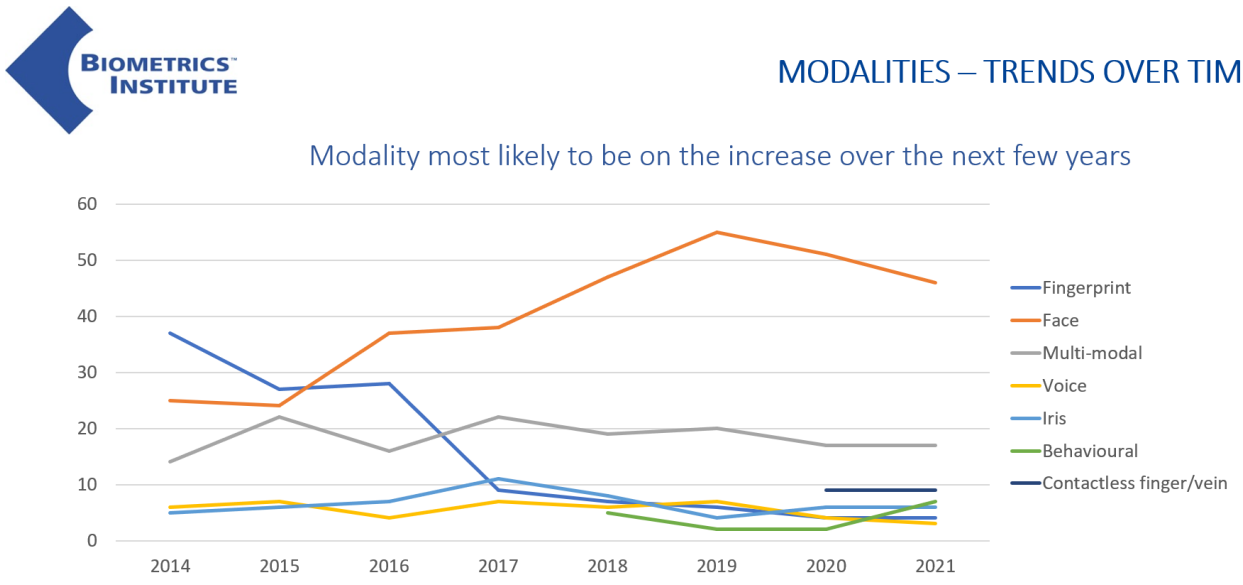
In October 2013, we launched our continental European event, the ***ID@Borders Conference*** and in March 2014 once again, the Australian High Commissioner hosted a Launch Reception but this time in Washington DC followed by our first US conference in March 2017.

In 2014, we entered a productive partnership with the Elsevier publishing firm to organise the programme for what was then the *Biometrics 2014 Conference and Exhibition*. Three years later, Elsevier withdrew from the biometrics market and offered us to launch the ***Biometrics Institute Congress*** in 2017 which has now become the global event for biometrics providing balanced discussions of different stakeholders under the Chatham House Rule which drives our agenda.

Our member register now lists 220 membership organisations from 34 countries plus 10 Observers representing United Nations agencies, IGOs and European Union institutions. We now have 7,006 followers on Twitter and 2,746 followers on LinkedIn.

Looking at trends over the last 20 years, there is a general overview that privacy and data protection have always been a market restraint and that perceived developments used to be about borders and are now about digital identity.

We started capturing market data in our ***Industry Survey*** from 2014, surveying our members with a good geographical spread in UK and Europe, the Americas, ANZ and others including Asia, and consisting of both suppliers and users, particularly in the public sector. We can see in 2014 that fingerprint was the dominant modality peaking at just under 40%, although this is now in decline, with contactless finger/vein at just under 10% in 2020-21 compensating a little. However, the dominant modality in 2021, at a high of 55% in 2019, is face.



Biometrics Institute Industry Surveys BASE: all respondents (274/302/181/218/288/432/326/362)

Taking biometrics to the consumer market in 2014

When the Apple iPhone 5S was released in June 2014 the big news within days was that the *Chaos Computer Club* had managed to hack the TouchID fingerprint. Our very active BVAEG released a statement a few days after pointing out that there are technologies that can detect such attacks and that spoofing a biometric requires a level of effort that makes such attacks difficult. The arrival of the iPhone 5S certainly brought awareness of biometrics to consumers who were now using it on their mobile phone and no longer perceiving fingerprinting as something scary but convenient. Chaos Computer Club joined the Biometrics Conference that year and engaged in dialogue with our member and experts. We provided a trusted and balanced discussion in a truly independent environment and started to have a voice. Now it was time to be heard more widely.

Championing good practice recommendations with the United Nations in 2018

I had first approached the United Nations in 2014 to engage with developing nations through the UN, a strategy the Board had agreed earlier that year. It took several years to find the best contact within the UN and build the relationship. In 2017, I met with the UN Counter-Terrorism Directorate (UNCTED) in New York, and they presented us with a proposal to help develop recommended practices for their use in counter-terrorism. As an independent and international multi-stakeholder community that has been promoting responsible use of biometrics, they considered us the perfect partner for this task. The UN resolution 2322 (2016) was passed in December 2016 followed by 2396 in December 2018 when we started the work of the ***UN Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter Terrorism*** and completed it within six months for its launch at the UN headquarters in June 2018.

The next Compendium project phase was looking at delivering awareness workshops teaching the content of the Compendium, but COVID-19 delayed this phase. In the interim, we decided to proceed with the development of our good practice tool kit and once again in consultation with our members and key stakeholders produced the ***Good Practice Framework***, a structured pathway through the factors that may influence or constrain a biometric application. The Framework was launched to members in July 2020. Hundreds of years of experience with biometrics have merged into this document and it is now our next task to help members put the Framework into operational use.

Having a voice and being heard – the road ahead

Our members have highlighted how the industry has changed over the past 20 years by improving security, convenience, and privacy with for example e-gates travel through an airport, biometric authentication for banking apps, and biometric solutions such as facial recognition for law enforcement; by responding to technology with research into new standards and testing regimes; and together with the Biometrics Institute helping to inform and shape privacy and ethics legislation by promoting responsible and ethical biometrics.

We have run over 60 conferences

31 in Sydney, 16 in Canberra, eight Congresses in London, five in Washington DC, nine ID@Borders in continental Europe, 119 Workshops and 245 Member Meetings

I believe the Institute has truly arrived on the world stage however there is still a lot more work to be done, partly because the world is a big place but also because our industry continues to change and evolve. Biometrics have become pervasive and if you search the internet now for the term biometrics, you get overwhelmed by information. It is nearly impossible to know what is true and false and the complexities of different use cases of biometrics are not easy to understand. I think this is where the Institute can have a significant impact on both public and private sector thinking: The nuances and complexities of deploying a biometric system in a responsible and ethical manner need to be examined carefully at the planning stages and not at a later stage in front of regulators/courts. We need to continue and extend our education offer to members and other interested parties to help them counter potentially serious reputational damage and substantial fines focusing as always on the aim to implement biometrics responsibly and ethically.

Isabelle Moeller
Chief Executive, Biometrics Institute
manager@biometricsinstitute.org

4. Accenture: Moratorium on biometrics – What to do?

Over the past twenty years we've seen rapid growth in the biometrics market – personal, commercial, and governmental use cases all on the rise. The greatest spike in the usage of biometrics was seen with the release of the iPhone 5 which added millions of biometric sensors and an awareness of the benefits of usability and security that automated recognition has to offer. In the same period, we have seen a rapid increase in biometrics used to automate border clearance, increase inclusion for the undocumented, and add security to financial transactions. There are scores more examples where automated recognition systems facilitate and secure our public and private interactions.

As these systems have become more part of our daily lives we have also heard of, and perhaps experienced, some of the downsides of automated recognition systems. Perhaps because of the success of biometric systems they are receiving more scrutiny – are they accurate enough? Do they discriminate? In response to this some jurisdictions have banned the use of biometric systems outright and some have put moratoria in effect.

The relative performance of biometric recognition systems is extremely use case dependant, so it is difficult to understand outright bans that don't delineate factors such as:

- Is the system overt or covert?
- Is the system performing authentication or identification?
- Does the system require informed consent of the data subject?
- Under which privacy regulations does the system operate?
- Under which performance requirements does the system operate?
- To which security requirements does the system conform?

We know that all biometric systems have Type I and Type II errors (False Rejects and False Accepts) and we know that these error rates can be influenced by factors such as quality and age of the biometric data and the sex, age, and ethnicity of the data subjects.

Given the rapid adoption and utility of biometric systems in the public, private, and humanitarian sectors, one would think that effective regulation would follow suit – it has not – and outright bans and moratoria with no corresponding action plan does not resolve this issue.

If the perceived, or actual, problem with a biometric system for the intended use case is that it is not accurate enough or that its performance is impacted by demographic differentials then bans should be replaced with performance requirements and moratoria with regulations that require certification to specified conformance criteria for the intended use case. The sharing, retaining, and protecting of personal data, including biometric information are all fundamental data privacy provisions as are portability, accuracy, redress, and breach alerts that must have corresponding regulation and enforcement– and liability.

There is an understanding gap that should be reconciled with education – regulators need to understand how biometric systems work in their many and varied applications and legislate accordingly as they did with Health Information, Vehicle Emissions, Food Safety, etc. With proper education, legislation, and certification biometric systems can continue to facilitate and secure our lives – while preserving our privacy and human dignity – for the next twenty years and beyond.

Accenture
Daniel Bachenheimer
Daniel.bachenheimer@accenture.com
Director, Biometrics Institute

5. Terry Aulich: Thoughts as Chair of the Biometrics Privacy Experts Group, on the 20-year anniversary of the Institute

As Chair of the Biometrics Institute's Privacy Experts Group, I have been amazed at the development of the biometrics technology and industry over the last twenty years. Initially, biometrics had a public image of sci-fi semi-reality, and few understood what would come to pass. Now, more than thirty-five countries issue biometrically enabled passports, mobile phones and doors are secured by biometrics, refugee medicines and food are distributed with biometrics ensuring security and fairness in the process, social media uses biometrics and biometrics have a significant role to play in areas as diverse as marketing and military uses.

At the centre of this rapid development has been the Biometrics Institute. As a strategic advisor to the Board in those days, I watched three very important decisions being made. The first was the decision to ensure that the Institute was independent and a respected organisation. This was done in several ways: the most important was to ensure that constitutional control had to be in the hands of the users; the Institute had to be the source of credible information and ethical practice.

The second was to ensure that privacy was front and centre of everything the Institute did. In practical terms this meant the creation of Privacy Guidelines which are updated every two years in line with social, technical, and commercial challenges.

The third has been the expert committees, conferences and training programmes which have ensured that the Institute is the source of credible trusted expert advice and information.

All three of those developments could not have been possible without the thousands of hours of volunteer experts, a seriously good succession of Board members from many sectors and countries and, most important of all, the long-term guidance and drive of the Institute's CEO, Isabelle Moeller.

Isabelle especially understood how events needed to be managed and has had the golden touch that turns an international organisation into the biometric family where sharing ideas and knowledge and, in many cases friendships, has become the norm.

The Institute has also worked together with many international organisations such as the UN, INTERPOL, and leading universities. Much work has been on technical matters, anti-crime and anti-terrorism policy, human rights, privacy, and immigration.

Like all new technologies, biometrics can be abused for reasons of greed, authoritarianism, or plain stupidity. This is why the Institute's work has been so heavily concentrated on ethical considerations, where the human comes before machines. This approach has been richly rewarded as more and more organisations around the world have joined the Institute.

From humble beginnings in Sydney Australia, the Institute has grown with the industry and become multinational, finally basing itself in London but retaining its office in Sydney. It has been one of the great unsung stories of the modern IT era and we look forward to many more years and more organisations realising that fact and taking advantage of all that the Institute offers.

Aulich & Co.
Terry Aulich
+61 407 106 836
aulichterry8@gmail.com
Head of the Privacy Expert Group, Biometrics Institute

6. Australian Department of Foreign Affairs and Trade: The Australian Passport Office: Helping shape the future of biometrics

What's in a name? Nothing, compared to the value of a face, or other biometric indicator, when it comes to securing your identity.

More than a century ago, the Australian Government recognised the value of biometric information well before 'biometrics' was even a term.

The first photos appeared in an Australian passport in 1915, when passports became compulsory as a temporary measure during World War I for all departing males of military age.

Back then, a passport included some personal details and a simple black and white photo. This image served as an important security feature, allowing authorities to confirm a person's identity.

As technology evolved, so did the Australian passport. Since then, there have been a further 20 iterations of Australia's passport over the years, but the inclusion of an image to recognise someone's facial biometrics has always been there.

In 2005, the Australian Passport Office (APO), which is part of Australia's Department of Foreign Affairs and Trade (DFAT), launched its first biometric passport—one of the first countries to do so—by embedding an electronic chip containing biometric information. This small silicon chip helps authenticate the identity of the passport holder in over 140 countries.

Few Australians appreciate how advanced and secure their passports really are.

The APO's pioneering work on face biometrics is a big part of that story. Since the introduction of the biometric passport, facial recognition checks have been a standard part of the APO's processing.

Every time a customer applies for a passport, be it first time applicant or a renewal, APO staff check the photo against the entire database of facial images to ensure the person does not exist in any other identity. Currently holding over 29 million passport photos, this database is one of Australia's largest facial biometric banks.

These checks are still amongst the world's most thorough. APO staff are highly trained to pick up discrepancies as part of the facial recognition check. In fact, DFAT was one of the first organisations anywhere to test the aptitude of staff performing facial comparison tasks.

Of course, it's not possible for APO staff alone to compare an image against a database of that magnitude. So that's where the use of cutting-edge algorithms comes in.

Face comparison algorithms can spot anomalies humans would miss. The programs the APO uses to run these algorithms are industry-leading and are upgraded regularly to introduce further performance improvements to our systems.

Investing in facial recognition systems also delivers wider benefits for passport customers—using their face to confirm their identity through the Government's face-matching service. For example, the APO facilitated access to its passport face-matching service so Services Australia could fast-track financial assistance to those affected by last year's bushfires.

The APO's facial recognition system is also central to the Government's digital transformation agenda by supporting customers to create secure, trusted digital identity credentials.

Digital identities for the digital world are the future.

Customers no longer want paper-based products. The service environment is electronic, self-serve and almost instantaneous (think online shopping). Environmental events like COVID-19, where people are unable to meet in person, also push us closer to a digital future.

So how does a passport – a physical document with important biometric data and over 100 security features woven into the seams – meet these digital expectations? It evolves.

What this will look like will be interesting to watch, but two things are certain:

- Biometrics will be essential to both securing your identity and the integrity of any future Australian passport, and
- Any future success will require the continued work and collaboration of the APO and the Biometrics Institute.

APO is proud to be a founding member of the Biometrics Institute. We have benefitted immensely from the Institute's insights, and the close working relationships it has helped us forge with key agencies in the biometrics field.

We want to acknowledge the Biometrics Institute's tremendous contributions over the past 20 years and congratulate it on reaching this important anniversary. The APO looks forward to working closely with you for the next 20 years!

Australian Department of Foreign Affairs and Trade (DFAT)
Shashi Samprathi
Head of the Borders User Group, Biometrics Institute
DFAT were a Founding Member in Australia

7. Australian Department of Home Affairs: Biometrics: Use of the Face Verification Service to assist Australians in need

The Face Verification Service (FVS) is a secure online service that helps people to verify their identity in a way that is fast, secure and private, without having to present documents in person, making it easier to access government services.

The FVS enables Australian government agencies to check a person's photo against a government-issued photo identity document record. This is called a 'one-to-one' check and helps to confirm the identity of a known person. A small number of Australian government agencies have commenced trialling use of the Face Verification Service, with consent from the individuals involved and in circumstances where this is permitted by current laws.

The FVS helps to protect people from identity crime, which is a key concern for many Australians.

- 1 in 10 Australians are impacted by identity crime each year.
- The total economic impact of identity crime in Australia is approximately $3.1 billion per year. This includes $2.1 billion in direct costs and a further $1 billion in costs associated with lost outputs, prevention and response costs incurred by government, business and individuals.
  (*Australian Institute of Criminology Report "Counting the costs of identity crime and misuse in Australia, 2018-19").*

The FVS also helps victims of identity crime reclaim their identity faster, and helps in other cases where people can't access their identity documents, such as natural disaster victims.

The FVS builds on the success of the Document Verification Service (DVS), which has been available to Australian government agencies for more than 10 years, and to the private sector since 2014.

The DVS is a national online system that enables organisations to compare a customer's identity information, such as name and date of birth, with government records and is currently used by more than 160 Australian Commonwealth, state and territory agencies and almost 2000 private sector organisations.

During the 2019-20 summer, Australia was experiencing catastrophic bushfires. Services Australia responded to the emergency with an FVS pilot to reduce the burden on people seeking disaster relief payments. The pilot was focused on helping people to prove who they are in the absence of physical documents.

Twelve Service Centres across New South Wales and Victoria trialled the use of the FVS for the emergency payments for bushfires. During this period, more than 700 customers confirmed their identity using the FVS, including people unable to retrieve identity documents due to the continued fire threat.

In accordance with FVS requirements, individuals were asked if they consented to their identity being biometrically verified. Images of their faces were captured via a camera attachment (similar to a webcam) that was positioned on service officers' computer monitors, and compared online to government identity records to confirm a match.

Using the FVS supported individuals and families by saving them from sourcing additional identity documents, such as an Australian Birth Certificate or Australian Citizenship Certificate, avoiding the need for customers to return to a

Service Centre with their identity documents and reducing administrative burdens at a distressing time in their lives, thus reducing the emotional toll.

Here are just two of the success stories from this pilot:

- *A 91 year old customer attended a Service Centre to provide identity documents for an Australian Government Disaster Recovery Payment claim. The customer's husband, also claiming, was in the car. He was unable to walk into the office as he did not have his walker with him. The couple had been evacuated from their home due to the bushfires and were staying in a motel. Both customers had a current passport but did not have the passports with them. With customer consent, the Services Australia team used the FVS Portal for customer number one. The team then walked out to the car and spoke with customer number two. With his consent, they captured his image while he sat in the car and successfully matched it through the FVS Portal.*
  Without the FVS, the customer would have been required to come back at a later date with physical identity documents. This was a great outcome for them and for Services Australia.

- *A customer in his 90's attended a Service Centre in early January. He had been evacuated from his home, leaving all his belongings (including all identity documents) thinking he would return when it was safe. Unfortunately, his home and property were destroyed by bushfire. The Services Australia team was able to grant an emergency payment for the customer on the spot and without identity documents by using an image of his face in the FVS portal to verify his identity with the government's records.*

The majority of customers responded positively to the technology and its use, saying they felt their identity was being protected by the Agency. Many customers reflected on how easy the service was to use and the amount of time it saved them from trying to locate a physical document and come back to a Service Centre with that document. Less than 5% of participants asked did not consent to use the technology.

The FVS offers immediate, contactless identity verification to assist with disaster recovery activities, such as the timely provision of relief payments, or re-issuance of lost or stolen identity credentials.

Outcomes from the pilot demonstrated that the use of the FVS can more confidently provide vulnerable customers with the payments and services they need, when they need them, as seamlessly as possible.

Australian Department of Home Affairs
Matt Huntington
+ 61 (02) 5127 7301
Matt.Huntington@homeaffairs.gov.au
Department of Home Affairs were a Founding Member in Australia

8. Australian Digital Transformation Agency: Australia and Digital Identity

The world is changing quickly, it's becoming smaller and bigger at the same time, with the importance of safe, simple and secure digital services never more important.

Using biometrics as a default means to access services would have been unthinkable only a few years ago but with technological advances and social adoption, it is now second nature to verify a transaction with a tap of a finger.

People are engaging online at unprecedented rates, accelerated by the COVID-19 pandemic—even for activities like telehealth and remote employee onboarding. At the heart of these traditional in-person services is identity, needing a way to securely prove who you are online.

The shift to online has brought communities closer together while opening up a whole new world of risk and reward for us to navigate. Including privacy concerns, the need for businesses to keep up, as well as new opportunities engage, transact, and grow our economy.

Governments and the private sector need to focus on how identity is perceived, it's critical to build trust in the technology, ensure consumers are protected, and have strong policies that set the foundation for change.

Digital Identity underpins the Australian government's Digital Economy Strategy that will allow Australian businesses, and in particular small business, to capitalise on the opportunities that digital technologies are creating, enabling them to grow and create jobs as part of Australia's economic recovery following the COVID-19 Pandemic.

Following an inquiry into the financial sector in 2014, the Australian Government took the first steps towards a national approach to digital identity to support our country's economic growth.

The objective was to develop a national federated Digital Identity Framework, which would guide the development of a world class solution that could improve digital transactions across Government and the broader economy. To achieve this, we looked at international best practise and consulted extensively on the policy underpinning the Australian Government's Digital Identity System (the System).

Our guiding principles are privacy by design, putting the user first and taking an iterative approach in everything we do to make sure Digital Identity not only meets but exceeds community expectations.

Putting people first, we also need to consider and ensure that in-person services remain for those in our community who can't or don't have access to engage online. Inclusive system design is crucial to support as many people as possible to access online services with a digital identity.

Central to our System is the Trusted Digital Identity Framework or TDIF. It sets the standards, rules and guidelines for usability, accessibility, privacy protection, security, risk management, fraud control for Digital Identity providers. Anyone who participates in the System must meet these strict requirements.

The high standards set out in the TDIF allow for a true whole-of-economy digital identity system where people can have complete trust that their security and privacy is protected when using the System to access services.

This is especially crucial when they're asked for their biometric information.

When we talk about biometrics in the context of our System, we refer to the method of access and face verification for remote onboarding. "Biometrics" refers to a full breadth of measures to verify someone's identity and it can be a confronting concept. It's important to understand that with Digital Identity we're simply verifying that the photo taken by a person on the end of the phone (or device) matches their photo ID. In the future, this may extend to other biometrics to suit the appropriate use case.

Face verification is only required for people to access higher risk or higher value transactions—like those that currently require you to prove your identity in person at a government shopfront or service centre.

The key privacy features we've implemented for Digital Identity face verification and use of biometrics are express consent, one-to-one matching only, no central data base for storing images, and images are not shared across the System.

This means that any data that is required to prove your identity will need your express consent before it's shared. This is a principle that applies to the whole System.

Face verification is only used for 'one-to-one' matching. This means the System matches a photo you take of yourself with a photo you have provided as part of your identity verification. This very important security and privacy principle ensures the System only collects the information needed to establish and maintain a digital identity.

This is an important distinction from 'one-to-many' matching which matches a person's face against many images stored in an identity database and then adds that photo to the database.

And there is no central database where data will be stored for the System. Once a person's photo has been used for its consented purposes—including where you've consented to it being used for quality assurance testing and fraud detection—it will be deleted.

It's important that we ensure this system is secure and as robust as possible. We're working to enshrine these principles, the TDIF requirements, and strict security and privacy standards including protections around the use of biometrics in legislation, giving the Australians trust and confidence in Digital Identity.

Privacy is important to Australians, and to us, and we need a digital identity system that Australians can trust. A consent-based, regulated system will support people to do their business, big and small, online without compromising their security or their privacy.

Australia already performs well in government service delivery relative to other countries—ranking second for E-Government in the IMD's 2019 Digital Competitiveness and fifth in the UN's 2020 E-Government Survey. But there is more to do. Our goal is to provide safe, secure and convenient government services online. The Australian Government Digital Identity System will change the way that Australians and Australian businesses engage with the government services they need, and with each other, online.

Australian Digital Transformation Agency
Jonathon Thorpe
Jonathon.thorpe@dta.gov.au
Director, Biometrics Institute

9. Cognitec: Two decades of innovation for safer, swifter, self-service border checks

On a cherished day in 2002, shortly after the business launch in Dresden, Germany, our founders find themselves signing the company's first major contract in far-away Australia to help develop the SmartGate program, the very first eGate implementation in the world. The system at Sydney International Airport becomes a forerunner for worldwide adoption of self-service border control at airports and other checkpoints.

We extend our connection to Australia by joining the Biometrics Institute in March 2003 as the third European member, and lend our voice to the early conversations about feasible use cases for biometric technologies, their advantages and risks, and their impact on society.

The first eGate applications and their error rates also raise many questions about the feasibility and necessity of such systems. But most countries push forward with establishing biometric passports and automating border procedures. And statistics are easy to collect and present, showing very soon that the use of biometrics positively curbs identity fraud, outperforms ID validation by agents, and speeds up the immigration process.

In 2013, we respond to the growing demand for automated border control by introducing a new product—this time also providing the hardware for live facial image acquisition of the traveler. The device features new concepts for lighting, user guidance and camera control.

Following a contract award by the German Border Police to a German technology consortium, our device and verification software is integrated in eGates at all major German airports. Soon travelers embrace the speedy procedure that allows them to "cross the border" in 14 seconds or less, all on their own.
We continually optimize the device to boost usability for travelers while it captures best-quality images that guarantee high verification accuracy. Ongoing development work also enhances the performance of the proprietary sensor that distinguishes between human faces and artifacts like printed images and masks, thus preventing presentation attacks.

In the meantime, biometric algorithms gain in accuracy, and we participate in the "face recognition revolution" with regular releases of new matching engines. Every new version contributes to raising the reliability of now more than 400 eGates with our device in Europe and Asia. Billions of verifications later, the analysis of false rejections or faulty authentications in eGates with our technology shows extremely low error rates.
The innovative journey resumes in 2021, prompted by countries adding biometric entry/exit schemes to their immigration routines. Various tenders are now asking for equipment to quickly take biometric photos at the border. We react to very special installation requirements on German border control booths, and develop a slim, lightweight device that can hang on the glass front of booths in any design.

The German Federal Police awards the contract in July 2021. The project initially spans four years and includes the delivery of more than 1700 devices, followed by installation and maintenance at all international border checkpoints in Germany. Other countries are in the process of also choosing our device to fulfil entry/exit requirements. With slightly different immigration setups in each country, product development needs to stay flexible and retrofit the device to work well for every scenario.

And the journey continues. Our teams are already drawing new designs for a device that combines image capture, presentation attack detection and verification procedures. Managing Director Alfredo Herrera: "Our profound technical expertise, combined with the experience in working on government projects in the past 20 years, fuel continuous innovations for border control processes. We hope they contribute to ever safer and easier travels!"

Cognitec Systems
Elke Oberg
+49-351-862-9214
oberg@cognitec.com

10. Collins Aerospace: Biometrics: Changing the way we travel… and it's all for the better

The travel industry, like all others, has experienced dramatic changes resulting from the influx and adoption of new technologies. As has happened so many times before, today we are poised on the cusp of another massive change in the way we travel, thanks to another innovative solution: biometrics. Biometric technology gives us the ability to accurately identify individuals and to empower them based on that positive ID.

To some, the word "biometrics" conjures fear and skepticism. Chief among the concerns are fears about privacy of personal information — if individuals allow their biometrics to be used for one purpose, that information could then be used for some other purpose without their consent. Others fear a "Big Brother" plot, where the government uses a large biometric database to track and control people.

These worries stem from a lack of understanding of biometric solutions, how they are used, and what kinds of controls are in place to manage the data they gather. Further, the value of biometrics — and how they can dramatically improve both aviation/airport operations as well as the travel experience for the passenger — is underappreciated.

Biometrics simply means to measure ("metrics") the body ("bio"). Every individual has a unique set of measurements — whether it's the distance between their irises, the width of the space between their eyebrows or the length from their hairline to their chin — that can be used for identification.

This idea is not new — it actually dates back to the 19th Century. A young records clerk with the Paris Police Department named Alphonse Bertillon determined that a system based on precise measurement of certain body parts — circumference of the head, length of the middle finger, size of the ears, etc., in addition to standardized photographs of the individual — would provide a way to identify people that relied on fixed, unchanging attributes or characteristics, regardless of whether they changed their appearance.

Fast forward to the Digital Age, where we have morphed from the physical measurement of body parts to the digital measurement of body parts, which is transforming industries that require accurate identification of individuals.

A game-changer for air travel

Chief among those industries is air travel. Airports and airlines must be able to accurately identify who's traveling where, ensure the right passengers are on the right plane, verify passports and visas for international transfers, and match baggage to the right individuals. Essentially, every part of the commercial aviation infrastructure depends on the proper identification of people.

And it's the human-to-human exchange of identification documents and personal interactions that add friction to the flow of people through airport and airline travel procedures. The back-ups and queues that form because of these interactions also detract from a positive passenger experience.

Removing friction from the process

Biometric ID technology removes that friction. It makes the identification process faster, easier and far more accurate. With one facial scan upon entering the airport, for instance, your face becomes your ID throughout your journey.

You can check your bags, move through security operations and enter the jetway—all with minimal stopping, showing documents and waiting for verification. Your face provides all of the information required.
The technology also enables passengers to make their way through their journey with less support. Fewer security personnel are needed to ask questions and check documents. Airline personnel are no longer required at key stations — such as baggage areas and airline gate entrances — and can be deployed elsewhere.

In a post-pandemic world, biometrics will also reduce a major concern associated with air travel: the fear of contracting disease by touching public surfaces or interacting with people who are ill. We already have "curb-to-curb" biometric solutions that enable a passenger to move from the point of origin to the destination airport without touching anything other than his or her own items. A face and a smart phone are all that's required.

Biometric systems can also be equipped with health diagnostics that can help identify individuals who have a high temperature or other symptoms so they can be evaluated by medical personnel. In combination with virus testing, this system could mean moving closer to disease-free flights and enable the reopening of borders now under COVID-19 restrictions.

Biometric technologies make air travel safer in other ways, too. Think about how much more secure your smart phone or laptop or bank account is when your face or fingerprint is required to unlock it rather than a password. Now think about how much more secure air travel will be when that same technology is fully embedded into commercial flights. With the added accuracy of biometric identification, airlines will know exactly who is on each flight.

By reducing passenger concerns about illness and safety, we can increase the number of people willing to fly as well as the frequency of trips. Less fear leads to increased passenger volume.

All of these improvements amount to a vastly more efficient air travel ecosystem that can accommodate significant increases in capacity.

The Biometrics Boon Is Building

Biometric identification technologies have been in use in airports throughout the world for several years, primarily for immigration and border control. But momentum is building for wider application of the technology throughout commercial aviation as airlines, airports, passengers and other stakeholders begin to see the enormous value this technology can offer.

Biometric IDs will make quick work of matching facial images to ensure people are who they say they are—and give them the freedom of movement that comes with that identification. It's a simple, efficient, low-risk solution that will bring countless improvements to the way we travel.

Without question, the biometrics boon is coming. And it will transform, refresh and enhance the travel landscape for decades to come.

Collins Aerospace
airports@collins.com

11. Paul Cross: Thoughts as the former Head of the Border User Group, on the 20-year anniversary of the Institute

Congratulations to the Biometrics Institute for 20 years of providing leadership and advice to all stakeholders associated with biometric technology.

For 20 years the Institute has provided access to global expertise on biometrics from the technical, academic, privacy and user perspectives, as well as unparalleled networking opportunities for professionals who are involved with this technology.

For me this is an opportunity to reflect on what I have gained from my association with the Institute over 10 years. In my time with the Institute, I have been a member of the Border User Group and of the Future Directions Group, I have acted as a Director from 2011-2015 and from September 2020, have presented at 25 events, and attended some 95 different Institute events!

Imagine what you learn from attending 95 industry events on biometrics, and from all the many papers, presentations and discussions the Institute has organised, that have involved the very best experts and authorities on biometric technology from around the world.

It's important to also acknowledge the value we all get from the Expert and Sector Groups that the Institute maintains. Much of that value is hard to quantify. These groups produce papers and products for members that explain important concepts and that help us to maximise the benefits and manage the risks that accompany the use of this technology. They are also invaluable information sharing opportunities, where members with similar interests get to talk about their challenges and their successes, and inevitably, members continue to interact offline to focus further on areas of common interest.

I remember when we started the Border User Group (or BUG), in July 2015. It was at a time when many countries were planning or developing major biometric capabilities and programs to better manage their borders, and all were facing similar challenges. From 13 members in June 2016, the BUG grew to 27 members in June 2017 representing different agencies from a range of countries, and it formed a professional biometrics international network that still thrives today.

The Future Directions Group (FDG) was formed in June 2019, as a group of dedicated industry-watchers with different backgrounds and a shared interest in monitoring developments that will shape our future. This group works hard to produce various thought leadership products, including the annual State of Biometrics Report covering the important events and developments each year, explaining their impacts and predicting where we are headed next. My favourite part of FDG meetings is a roundtable discussion on *'what's new, what's different?'* where we each share insights into the latest developments, explore what is behind them and what implications they have for all of us.

The Biometrics Institute has certainly been a huge success and I wish the Institute the very best for the next 20 years as well.

Paul Cross
Director, Biometrics Institute and former Head of the Borders User Group
+61 (2) 9911 7551
paul.cross@sita.aero
SITA were a Founding Member in Europe

Privacy and policy, technology innovation, research and development, applications and use cases

12. Ted Dunstone: The past, the present and what's next for biometrics and the Biometrics Institute - the Institute's Chief Executive in conversation with its Founder

To celebrate the Institute's 20-year anniversary, I caught up with Ted Dunstone, the founder of the Institute to have a chat about the early days, where we are now and what are the things we need to tackle going forward. Ted was sitting in his home office in Singapore while I was having a coffee in my office in London which in itself describes the Institute so well: a global community of people with a passion for the responsible use of biometrics.

Isabelle: Ted, tell me about how it all started back in 2001 and why you founded the Institute.

Ted: Isabelle, do you remember our first Member Meeting in Canberra in 2002? This was pre-GPS and we kept going round the roundabouts at Parliament House trying to find the exit to the Department of Foreign Affairs and Trade. We knew where we needed to be, but we had to work out how best to get there. This is similar to how the Institute started.

Early on it was apparent there was something special about what we were creating. To this day, I haven't come across an organisation quite like the Institute, having its users at its heart, but also embracing the important contribution from suppliers and other members of the community. We found a way to nurture all of those different aspirations and requirements. That's a difficult act to get right and it is a credit to all the people that have been involved with the Institute. In addition to yourself, I'd particularly like to call out John Peacock, an association consultant, who really helped shape the early thinking about creating a user group, and Geoff Poulton who took over from me as the Institute Chair.

The first real users of biometrics were government agencies, who were early adopters of large-scale biometrics. As I was already established in the industry, I had existing relationships to help bring together the right people early on.

Isabelle: So why did so many government departments become members? What attracted them to the Institute?

Ted: They joined because they could see the power of community of practice, where they were not only the passengers going on a journey but the actual drivers. They could use the Institute to help further their goals rather than just receive a sales pitch.

A core common goal was the mission of the Institute to promote the responsible use of biometrics. Getting the mission statement right at the start was a fundamental component of the success of the Institute. I had started the Institute as I could see how this technology could turn out to be misused, and that if you didn't have a way to educate people about how it should be used, the whole industry would be imperilled and then the public would react badly. Most unfortunately, time has borne some of that out.

Isabelle: And here we are 20 years on still facing that very challenge of creating public trust in biometrics. So, what do you see as some of the key advancements the Institute has supported through its very existence?

Ted: I think we've had a lot of firsts in Australia where the Institute was founded. A lot of interesting biometric projects have gone on to deliver long lasting value within the passport system, e-gates, and government services. And most of these have been very successful projects that have not generated any negative publicity or problems.

The Institute has enabled its members to have the knowledge and the understanding and to feel comfortable and more confident about adopting biometric technology, because it comes with new risks and challenges. As a result, I believe the Institute has been a catalyst for allowing the industry to grow responsibly.

From its beginnings the Institute has pushed the privacy agenda and emphasised why that has to be considered upfront. In 2006, for example, we released the very first Biometric Privacy Code.

Another example is the vulnerability work that we've done. There was a recognition early on by the Institute, that this was an area that needed more development and more understanding by members. We brought together the international experts for the first time in 2010 and in the outcomes of those first meetings were the seeds of what we see today - in terms of standardisation, testing and awareness. People have asked whether these changes would have happened regardless. I think they would have eventually. But I think that the Institute - again - acted as a catalyst to make these things happen faster.

There's another aspect. When we started with the Institute in 2001, biometrics was still very niche. It was in some passports and some people had seen it in movies, but most people had no understanding that it wasn't science fiction. Now, 20 years later, it's everywhere: on our phones, used in government services and it would be fair to say that a good percentage of the world's population has encountered biometrics in one form or another. The Institute has been there for much of that journey, in all sorts of ways, working with development agencies like the UN agencies and law enforcement as well as big corporates and social media.
The work we did in 2018 with the United Nations Counter Terrorism Executive Directorate (UNCTED) and the Office of Counter Terrorism (UNOCT) in delivering the Compendium for Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-terrorism was a major milestone for the Institute. We were advised that there is no other organisation that represents such a multi-stakeholder community from around the world and that we are best placed to be the penholder for the Compendium as we deliver diverse but balanced viewpoints on biometrics. Our independence is a critical part of who we are.
The Institute has provided the one place to meet where those new to biometrics could connect with a knowledgeable community and learn from others and seek information. It is important for those seeking information on biometrics to know they are not alone. There are so many amazing and passionate people that I have worked with at the Institute - starting with the various Board Directors and Committee Members – but also the membership overall who attended so many of our events.

Isabelle: I agree, Ted, it is all about the people. I will never forget how we convinced Geoff Poulton from Commonwealth Scientific and Industrial Research Organisation in Australia to be our first government Director and then Chairman from 2002, followed by John Secker from New Zealand Customs in 2005 who helped us take the Institute to New Zealand. In 2011 there was Paul Kirkbride from the Australian Federal Police who strongly supported the plan to set up an office in London in 2011 and now Andrew Rice, so far, our longest serving Director since 2016.

So, what do you think is next for the Institute and our community?

Ted: Our community has matured. There are such experienced people involved. New people can learn from the other members.
We have built these amazing foundations, and the Institute has accomplished so much in its 20 years. But in reality, I believe we are only just at the beginning of this journey with the significant transformations that biometrics and identity are bringing to the world.
To date, biometrics has been a largely unregulated space but that is changing as it is becoming much more mainstream. New legal frameworks are being discussed, biometric commissioners are being setup, and the EU GDPR and other legislation that addresses biometrics is being introduced. The value of a place like the Institute is to assist those who write the regulations to get them right, wherever they are in the world. It is important that all regulation everywhere is developed appropriately. The Institute can help these changes by providing the guidance and information to those regulators to ensure that biometrics will be used responsibly and ethically.
There is a lot of work ahead. I am looking forward to the challenge.

Isabelle: Thank you Ted, I have certainly enjoyed the past 19 years that I have worked with you and the Institute, and I am not yet ready to retire.

Ted: It's hard to believe its 19 years. When we first met, I think you were expecting someone older, and now I actually am! I honestly can't imagine anyone better to be at the helm of the Institute for the last 19 years and to see it into its future. For all the fun times, and some hard ones, it's also been a real pleasure working with you on this incredible journey.

Ted Dunstone
Founder, Biometrics Institute
+61 419 990 968
ted@biometix.com
Biometix were a Founding Member in Australia

13. FacePhi: Humanising technology: Biometrics as part of our daily lives

When was the last time we thought about how new technologies were integrated into our lives? In recent years, we have rapidly adopted devices and tools that have digitised much of our daily lives. Smartphones have become an essential instrument for relaying and accessing information about our environment in an immediate manner. On the other hand, the IoT has allowed, in addition to sensorising our homes and turning them into smart homes, to develop a wide range of application possibilities on a larger scale, for example, more and more cities allow us to access public transport and mobility services through simple applications and the reading of codes on our mobile devices.

Accepting a greater presence for technology in our environment has been a natural process, which in these advances has encountered a way to simplify daily tasks and improve our quality of life. For years, both experts and market developments have pointed to biometrics playing a leading role in the digitisation of our society, which is an important responsibility for development companies. The creators of identity verification technology are driving its adoption with great success, but perhaps the same effort is not being put into spreading knowledge about biometrics. It is a technology so tied into people, and thus should be perceived as a practical, safe and non-invasive tool by society, and now the time has come to take that step and connect with people in their dual role as users and citizens.

We have seen our identity verification solutions go from being a tool almost exclusively requested by banks and financial groups to entering various sectors and achieving a much broader positive social impact. During the health crisis due to Covid-19, digital onboarding and authentication technology reached the health sector, for example in the Kangbuk Samsung Hospital in Seoul, helping patients to carry out procedures without using cards, paper documentation or in-person interactions. Months later, biometrics would allow the collection of pensions in Argentina by introducing a biometric recognition system for retirees to provide 'proof of existence' with a simple mobile application from the safety of their homes. This success story in the silver economy has recently been emulated in Nigeria, where biometric technology is helping the public to collect their benefits through 100% digital identification.

These projects have had the common characteristics of showing that biometrics is more than a tool to improve the customer experience, highlighting its ability to be inclusive with all types of users -an aspect that our company considers essential. It is important that algorithms avoid discriminatory behaviour towards certain groups due to biases related to sex, race and age; all this complemented with the contribution of accessible, safe and useful digital environments in their day to day lives. Biometrics need to generate great confidence in the end user, who authorises the use of identity identification technology in a conscious way. This concept of 'ethical biometrics' is what allows us to bring technology closer to users and put to rest concerns about practices such as mass video surveillance or unwanted image capturing; This is the way in which we can make biometrics be accepted with the same naturalness as smartphones or voice assistants in our homes.

The next few years will be decisive for the incorporation of digital identity verification systems into relations between citizens, companies and public administrations. For this reason, we must become more than technology developers: We must be disseminators, transferring to public opinion the advantages and opportunities that biometrics offer. The time is now, at a moment in which digital identity verification systems begin to be introduced as an alternative to documentation at airports, as a means of payment in shops and as a form of access to various public services. We are at a true turning point with respect to the normalisation of biometrics, as we have seen after our entry into projects for the travel and transport sector, or the development of smart cities such as the one that the Korean government will promote on the island of Jeju.

Being able to show the positive impact of biometrics, avoiding misinformation and clearing up the doubts of citizens and public administrations is a part of technological development that we cannot ignore. Biometric technology is on the way to becoming part of the daily lives of millions of people, and this reality not only presents us with a great economic opportunity, but also with the challenge of humanising it.

FacePhi
Javier Mira, CEO and Founder
Joined in 2018

14. Implementation Capacity Building Working Group (ICBWG), ICAO: Extending the benefits of ePassports

The establishment of the Biometrics Institute twenty years ago reflected a broader need to understand a world in which digital technology was playing an increasingly influential role in daily life. At about the same time in 2003, the International Civil Aviation Organization (ICAO) adopted specifications for electronic machine-readable travel documents (eMRTD or ePassport) that are digitally enhanced documents that contain an embedded chip, which holds both biographic information and a photo. The ICAO guidance material and specifications found in Doc. 9303 laid the foundation on which an extensive system of infrastructure could build. Beginning with Belgium in 2004, successive governments began issuing ICAO-compliant ePassports. By 2013, over 100 countries issued ePassports and nearly 400 million were in circulation worldwide.[1] As of 2020, 145 countries issue ePassports and there are roughly 1 billion in circulation

In the post-9/11 world, the ability to confirm the identity of incoming travelers has increased in importance. ICAO's specifications allow states to encode the documents they issue with a biometric to serve this objective. The capability to add biometric information to a document, combined with the option to authenticate data stored in an ePassport via ICAO's Public Key Directory[2] (PKD), positions travelers to biometrically substantiate their claim to an identity in a secure manner. Moreover, electronic ePassport verification has enabled border authorities to streamline border processing by employing Automated Border Controls (ABCs). ABCs are "self-service" passport control points for arriving or departing travellers. In most cases ABCs will read and authenticate the ePassport and compare the holder to the ePassport facial biometric to verify identity. ABCs can thus be an important tool to expedite traveller process and identity verification, along with enabling border officers to focus on higher-risk scenarios.

The benefits of ABCs and the digital biometric data included in the ePassport can only be effectively leveraged if ePassports can be successfully read and if receiving states are consistently authenticating these travel documents. Compliance with Doc 9303 specifications will ensure that ePassports can be successfully processed at borders; however, it is important that receiving border entities carry out the full ePassport authentication process outlined in Doc 9303. Lack of adherence to these technical specifications can negatively impact the security, facilitation, and ID management benefits of the ePassport. Similarly, compliance with ICAO travel document issuance standards and recommended practices will help to ensure that presented ePassports can be trusted by receiving states. At the crux of trust lay the evidence of identity (EOI) principles of document issuance (i.e., a claimed identity is genuine, the presenter is linked to the identity, etc.).[3] In other words, states have assurance that data on ePassports are input only after issuing authorities exercise robust due diligence. The ICAO Implementation and Capacity Building Working Group (ICBWG), in which the Biometric Institute has been a valued participant, supports states in developing this capacity and has published a number of guidance materials and supporting documents for issuers and verifying entities.

As a reliable source of both digital identity and biometric information, the ePassport (or its derivative forms) is likely to be used to support facilitation and economic recovery – including as a tool to support low-touch processes in the new COVID-19 context. The profound impact of COVID-19 on the travel and tourism sectors cannot be overstated. As a recent Airports Council International analysis highlights, the airport industry anticipated a -64.2% reduction in traveller volumes and a reduction of over 6 billion travellers in 2020 compared to 2019.[4] ICAO has played a critical role in supporting states recover from the unprecedented crises through the establishment of the Council Aviation Recovery Task Force (CART). Among its many principles is the need to accelerate the use of contactless processing of travellers to reduce potential transmission. While governments and air industry sought to leverage biometrics and contactless processes well before the pandemic, COVID-19 has accelerated this trend.

As industries worldwide grapple with how best to exit COVID, there has been a proliferation of apps and solutions that support digital identity, and other inputs to cross-border travel, like vaccination credentials and testing results. The ecosystem is indeed fragmented. However, in the same way ICAO has played a significant role throughout the pandemic, so too has it continued to advance work on the Digital Travel Credential (DTC)—in its simplest form, the

[1] Government of Canada, "History of the ePassport: Backgrounder," (Ottawa: May, 2014) Accessed 25 August 2021.
[2] ICAO PKD Background: https://www.icao.int/Security/FAL/PKD/Pages/default.aspx
[3] ICAO, "TRIP Guide on Evidence of Identity," Version 5.4 (May 2018).
[4] Airport Council International – World (ACI), "The Future of Travel and Digital Identity at Airports," (Montreal: May 2021), 5.

DTC is a digital replica of the data on the ePassport. The DTC presents a new opportunity to process travellers before their arrival. With the DTC, border entities can carry out most of the border inspection process before a traveller's arrival, leveraging the embedded digital biometric to bolster pre-arrival screening. Upon arrival, the traveller would be linked to their pre-screened digital biometric and enjoy an increasingly streamlined and touchless arrival process. Now, perhaps more than ever, the existing infrastructure that supports ICAO-compliant ePassports is fundamental, as a strong base in ePassport issuance and processing is required to support the use of the DTC, along with the expanded use of digital identity and, by extension, the recovery of travel. The ePassport offers as much potential now as it did almost two decades ago.

Extending the benefits of ePassports will serve a variety of purposes. For example, leveraging existing ePassport infrastructure will reconcile privacy concerns by protecting the identity of individuals through well-established and trusted cryptologic practices. Additionally, bringing awareness to the ability for the ePassports to act like a record from an issuer's database, but in the hands of travellers, strengthens the notion and principles of individual digital sovereignty. The DTC, as a digital replica of the ePassport, contains the same electronic and security features as an ePassport and contains a biometric that adheres to passport issuing processes. This can be electronically verified for signs of tampering and authenticity.

Although many private-led initiatives comply with privacy by design (PbD) principles, the ePassport remains one of the most reliable documents in circulation worldwide. That ePassports are issued according to global standards on travel document issuance underscores their global interoperability and trust. Further, no other entity has the same access to the PKD/PKI like government authorities do, which further supports the use of a DTC, the PKI's cryptography, and a decentralized validation structure in the future.

As we approach the twenty-year anniversary of the ePassport, how can we ensure that the benefits of ePassports are maximized? What other use cases may benefit from leveraging biometrics and the backend infrastructure that support ePassports? ICAO has expressed interest to provide non-state actors access to the PKD for limited commercial purposes on a trial basis. This is welcomed news for many, particularly in the air industry. Accordingly, the PKD Board recently solicited interest from private entities to determine whether leveraging the PKD for limited commercial purposes may have utility beyond aviation. In this way, the benefits of ePassports may well extend into the private sector in the future and apply to a variety of areas in which digital identities are required.

For further information on the ICBWG please email ICBWG@icao.int.

Implementation Capacity Building Working Group (ICBWG), ICAO

15. IDEMIA: Smart borders – A technological and democratic achievement & Future-Proof Access: Flexible and Frictionless

How policy, process and technology were combined to achieve the European shared Biometric Matching System

The European shared Biometric Matching System (sBMS) was founded on a political agenda that was converted into legislation. This legislation was then translated into large biometric IT systems. This process created the foundation of trustworthy biometric technologies – a development that required expertise in order to be achieved.

The policy

To comprehend how the sBMS came to fruition, it is important to understand the history of the Schengen Area. It started on 14 June 1985, with five European countries signing the Schengen Agreement, a treaty that led these now 26 countries toward the eradication of their national borders, to build a Europe without frontiers.

The process

In 2013, the Smart Border regulation proposal was received from the European Commission (EC). The proposal focused on the Entry/Exit System (EES) and the Registered Traveler Program (RTP). The following year studies were carried out to ask the leaders in biometrics if such a system was feasible. The question being debated was: could technology efficiently manage a multi-biometric database that contained millions of records? Keeping in mind that the database had the crucial role of ensuring the utmost accuracy and security of the biometric data, while respecting a stringent response time at border crossing points.

After completing the study on the capacity of the back-end system, it was necessary to test the impact of this idea on the ground, at border crossing points. All Member States implemented pilots to test their technical capacity to efficiently capture traveler biometric data at land, air and sea border crossing points. ICAO recommended capturing three biometrics: face, fingerprints and iris. In order to push the testing capabilities, it was important to capture a combination of biometric configurations (four fingers, eight fingers, ten fingers and face and iris recognition) in varied situations and climates.

While the testing was happening, the world was witnessing many international security threats and incidents that made the Smart Borders initiative an urgent need for Europe. The borders of the Schengen Area needed to be protected and all third country nationals (TCN) needed to be thoroughly checked in order to ensure the security of local citizens and bona fide visitors. The EC issued a new regulation proposal integrating the outcome of the studies and the pilot tests. The proposal was to capture and store biometric data of four fingers of TCN and their faces in the EES database. The aim was to be absolutely proportional and time efficient at border crossing points.
In quick succession over three years, the EES regulation, the ETIAS regulation and the Interoperability regulation respectively came into play, completing the technological environment needed to provide liberty, security and justice to the European Union.

The successful implementation of the sBMS necessitated the involvement of all European stakeholders: the Commission, the Council, the European Parliament and notably the LIBE Committee, the Member States, the various agencies involved and industry. Industry was greatly involved in carrying out studies and pilot programs.

Conclusion

Biometrics for Smart Borders was built in an open process involving industry, politicians and the general public. Each decision to implement biometrics should take the local context into consideration, be it national, regional or international, and adapt accordingly. By working together and by listening to the needs of all stakeholders, trust in biometrics will be achieved.

Future-proof access: Flexible and frictionless

Society is migrating to access control models that are more flexible yet remain secure, and the adoption of contactless access using biometrics has been expedited by the Covid-19 pandemic. Consequently, biometric technology has emerged as a focus for both governments and private companies as it becomes part of everyday life for citizens worldwide. From smart phone access to border control screening, the goal is to find better ways to provide secure, trusted, and frictionless access points that enable daily activities while keeping people safe.

Experts in biometrics have made this possible with more advances coming every day.

Things that were once physical—key cards, car keys, IDs, credit cards—are being dematerialized into our smartphones. This digital shift introduces unprecedented convenience, seamless connectivity, and security whether by opening a door, verifying identity, or paying for goods and services.

Technology has made it so that what required a physical key and laminated ID 20 years ago, now takes a simple wave and a touchless sensor. These devices can deliver a reliable fingerprint match in mere seconds, boosting accuracy and security. Smart cards and multi-service cards now combine payment and civic use cases resulting in greater financial inclusion. Mobile ID solutions benefit both states and consumers, giving citizens control over identity authentication and creating a more secure and convenient way for agencies to provide refund payments or benefits digitally and remotely. Logical access control and IT security rely on biometrics, too; requiring fingerprints and multi-factor authentication to grant employees remote access to operating systems, and application-based logical access is used to control strategic points of user identities, protecting access to resources for single sign-on or to digitally sign sensitive documents.

Experts know that this progress and power requires stability. Thankfully, 5G technology deployment has begun, delivering the power needed and dramatically improving network connectivity with faster, more reliable connections that meet the demands of ultra-high-definition broadcast, smart devices, and vehicle-to-everything communications.

As the pressure on networks grows, the secure authentication of devices is even more critical. SIM cards protect user credentials by leveraging tamper-resistant hardware; and with properly configured 5G SIM cards, mobile network operators can seamlessly connect mobile devices and IoT connected objects ensuring subscribers gain immediate access to 5G services.

There is no doubt that biometric technology will continue to get even stronger. Privacy and security experts, governments, and industry are tasked with a critical mission to bring the future of identity to the citizen, but they must do so *together*—ensuring all parties realize the extreme responsibility that comes with it and to continue putting the safety and security of citizens worldwide at the forefront.

IDEMIA
Leana Hersch & Maggie McClain
maggie.mcclain@hkstrategies.com
IDEMIA were a Founding Member in Australia and Europe as Sagem Morpho

16. ID Transnational Consulting & INTERPOL: 2004 Southeast Asian Tsunami – victim Identification in Thailand

Introduction

On the 26th December 2004 a massive 9.1 magnitude earthquake struck off the north coast of the Indonesian island of Sumatra. This resulted in one of the largest tsunamis ever recorded spreading across the Indian Ocean and striking the coasts of many Southeast Asian and East African countries. More than 230,000 people were subsequently killed. The operation to identify the deceased in Thailand was centred in Phuket. It was jointly led by the Royal Thai Police and the Australian Federal Police with Interpol supplying and operating the AFIS and DNA biometric search systems. Other countries, whose nationals were missing in the disaster, supplied Disaster Victim Identification (DVI) teams of police and forensic science personnel to aid in the identification of the deceased, regardless of their respective nationalities.

Disaster Victim Identification (DVI) is a protocol employed by law enforcement agencies around the world to identify the deceased in mass casualty events such as natural disasters, aviation incidents and terrorist attacks. The three primary identifiers used in DVI are:

- Fingerprints: In cases where a putative identity has been established, post-mortem fingerprint impressions are taken from the victim and compared 1:1 with ante-mortem finger marks that may have been developed, for example, on personal items such as household contents, diaries etc. or official fingerprints (if held). In cases where there is no indication as to the identity of the deceased then an Automatic Fingerprint Identification System (AFIS) is usually employed to conduct a biometric search of the post-mortem fingerprints against a database containing the ante-mortem finger marks.
- DNA: Similarly, DNA profiles generated from samples obtained from the deceased can be compared 1:1 with ante-mortem DNA profiles taken from personal items such as tooth or hair brushes or DNA profiles of surviving close family members (familial/kinship matching). DNA Databases can be used in the same way as an AFIS to search the victim's DNA profile against the profiles produced from all the victims' personal items. Additionally, links may be established between the DNA profiles of victims from the same family. This only applies to biological relatives.
- Forensic Odontology: A comparison of the victim's teeth with ante-mortem dental records, X-rays and charts. A search capability of dental records is usually not possible because of the decentralised record systems used in most countries.

Challenges and critical success factors

Fingerprints

The immersion of the deceased in salt water for long periods resulted, in many cases, in the detachment of the epidermal layer of skin from the hands in the form of a 'glove.' It is this layer that contains the papillary ridges of the fingers and palms that make up a person's 'fingerprints.' The dermal skin layer beneath contains the 'anchoring' ridges that hold the epidermal ridges in place. There are two dermal ridges for each epidermal ridge and therefore this made impressions obtained from the dermal layer of skin largely incompatible with AFIS search systems i.e. attempting to match double ridge formations with single ridge formations of the same person. Any epidermal 'gloves' recovered with a body was examined by experts to determine whether or not the 'glove' had turned inside out when detaching from the hand. If the skin had turned inside out then the fingerprint impression taken from the glove would be in reverse direction, when recorded, and therefore would not be found during an AFIS search.

Of special note was the action taken in respect of the Myanmar workers who had lived in huts on the beaches of Phuket. It was originally assumed that because they had no possessions or property left after the destruction of the beaches that they would remain unidentified. However, it transpired that all Myanmar immigrants had been fingerprinted (two fingers recorded on cards) on entry to Thailand. These fingerprints were loaded into the Interpol AFIS and searches of the victims' post-mortem fingerprints revealed a significant number of matches.

DNA

The prolonged exposure of the victims to the intense heat and humidity of the Thai climate meant that many of the 'normal' post-mortem samples obtained from the deceased were 'denatured' and no usable DNA profiles could be generated. DNA from bone marrow was found to be suitable but the extraction of DNA from bones was a highly specialised process in 2004/5 and very few laboratories could undertake the process, especially in bulk. However, eventually the samples were sent to the International Commission on Missing Persons (ICMP) facility in Sarajevo. Their considerable expertise in identifying numerous skeletal remains from the 1990s conflict in the former Yugoslavia proved invaluable. The DNA profiles were sent to the Interpol DNA Database in Phuket for search and many victims were successfully identified and, where appropriate, repatriated, including family groups linked by their DNA.

Forensic odontology

In most countries, dental records had to be collected from the individual dental surgeries of the missing persons. In Scandinavia, however, the dental records of several countries are collated in a centralised database. This allowed all the required records, charts and x-ray sheets to be accessed, collated and dispatched to Phuket within a very short time after the tsunami. Consequently, many Scandinavian victims were identified and repatriated in the first few months of 2005. Other countries took much longer to obtain dental records, on an individual basis, and use them in the Thai reconciliation process to establish identity.

Outcome & developments

More than 5000 people died and nearly 3000 were missing after the tsunami hit the coast of Thailand. In the two years after the event over 3600 of the deceased had been positively identified by the DVI process using one or more of the primary biometric identifiers.

In the 17 years since this disaster there have been significant developments not only in terms of scientific advancements e.g. DNA extraction and profiling technologies but also in the processing power and accuracy of the biometric search algorithms that are available to DVI specialists today.

ID Transnational Consulting
Roger Baldwin
Member of the Advisory Council, Biometrics Institute
idtransnational@gmail.com

INTERPOL
Mark Branchflower
m.branchflower@interpol.int

17. IQSEC, S.A. de C.V.: Validación de identidad en la era digital - Biometry as a key factor to avoid identity theft

The digital transformation that has taken place in recent years has led different states and organizations to implement a strategy to recognize a secure and immutable digital identity in the digital environment.

In this sense, in the Digital Identity Guide of the International Financial Action Task Force (FATF) published in March 2020, the digital identity system is mentioned as a reliable solution to: (i) verify the identity of people; (ii) facilitate customer verification; (iii) support due diligence; (iv) help transaction monitoring, and (v) manage risks.
This Digital Identity Guide also notes that digital identification systems may soon be available on a large scale, this as a consequence of the use of biometric technology, internet ubiquity, mobile phones, digital device identifiers, life testing, artificial intelligence.

The need for secure identity validation mechanisms in the digital environment arises from the increase in the crime of identity theft, without undermining the economic losses that this represents for organizations and citizens.

Having a digital identity, linked to biometric data such as fingerprint or facial, are solutions that have been successful in specific use cases. At the international level, biometric data is used to implement authentication mechanisms or biometric systems for airport boarding processes, without the need to continuously present passports and boarding passes, as in the Narita International Airport Corporation, in which passengers are registered in a biometric kiosk where the facial image of the passenger is captured and verified with their passport.

In this context, data from the United States Federal Trade Commission (FTC) indicated around 1.4 million complaints of identity theft received by the said Commission in 2020. In this sense, imagining that a reproduction of the face through deepfakes can supplant identity, or be victims of bank fraud due to not having a robust identity validation mechanism, begin to be part of the risks that society faces.

To avoid identity theft, various Mexican authorities have issued regulations regarding biometric identification, as is the case of the National Banking and Securities Commission of Mexico, that since 2017 strengthened the identity verification procedures and mechanisms applied by credit institutions, with the help of a fingerprint. Biometrics has also been an ally to reduce inequality gaps and guarantee access to services, as is the case with the Aadhaar application in India.

We must keep in mind that in any database, registry, register or procedure where biometric data is handled, it will always be essential to have measures that allow, with reasonable certainty to maintain integrity, confidentiality and availability of such information, that is to say, in order to minimize unauthorized access risks, information leaks or cyber attacks risks.

Likewise, the digital transformation and the new distancing needs caused by COVID-19, have led to the implementation of non-face-to-face authentication mechanisms, known as Digital Onboarding, which have represented improvements to processes and savings for the parties involved.

It should be noted that at the international level there are standards that allow avoiding the risk of identity theft through the treatment of biometric data, as is the case of the ISO / IEC 30107-3: 2017 Information technology - biometric presentation attack detection. This ISO is aimed at suppliers or testing laboratories seeking to carry out evaluations of Attack Presentation Testing mechanisms.

By using technological components that comply with the ISO / IEC 30107-3: 2017, las Technological solutions become reliable to avoid risks of identity theft attacks with artifacts (masks, high definition videos, 3D molds, 2D printing, 3D printing and more) or human characteristics (similar biometric characteristics, lifeless samples, alteration of biometric characteristics, among others).

It is also important to highlight facial validation with proof of life that allows determining if a biometric sample, in this case the face, is being taken from a person alive and present at the capture point, through the camera of a cell phone. Thus corroborating the identity of the users of a process and / or service, against reliable databases, with which you can be certain of the identity of a person.

As the biometric data is physical, physiological or personality traits attributable to a single person, they allow us to avoid impersonation by electronic means, as long as safe mechanisms are used, accredited with the best practices and international standards.

Whilst biometrics is a great ally to meet new identity validation needs, it is important to keep in mind that the use of biometric technology also represents important cybersecurity challenges, protection of personal data, encrypted database backup, confidentiality, availability and integrity, that as manufacturers, implementers and organizations we must not lose sight of.

IQSEC, S.A. de C.V.
Manuel Moreno, Security Sales Enablement Director
contacto@iqsec.com.mx

Joined in 2020

18. IrisGuard: The role of iris recognition in increasing financial inclusion and stretching funding further

Partnerships help deliver accountability, efficiency and preparedness

The Covid-19 pandemic pushed an additional 97 million people into extreme poverty in 2020, there are 1.1b people with no ID and 1.7b people already unbanked. Some of the challenges relating to delivering assistance include having a robust digital identity infrastructure to support the disbursement of assistance and services to large populations.

Distribution of cash aid is expected to increase by approximately 17% -20% per annum and proof-of-life is increasingly more in demand by donors who want to make sure that assistance is delivered to the right people.

This is where iris recognition technology adds value, providing a real-time verification of identities for the purpose of a faster, easier and targeted assistance or services to those who are entitled to it.

Implementation of that does pose a number of challenges including negotiating of service points, verified onboarding, data protection and security, resistance to disease and compatibility of different systems.

Private-public partnerships play a key role here because NGOs and Government agencies have the understanding of what's required to fulfil the task on the ground, whilst the private sector is able to innovate and quickly deliver solutions which are fit for that specific purpose or one that can be applied across a variety of use cases.

When it comes to digital identity, the value is clear in a number of sectors including healthcare, where a correct identification of a patient is paramount for the provision of the correct treatment, stopping insurance fraud, managing audit trail for payments and health screening programmes. It is crucial to remember that when using iris as the human identifier, which removes the need for any other ID credentials, the individuals themselves are in control of their information as it is protected by their iris because it is unique to them.

If we apply that to social welfare support for example, accurate proof-of-life will stop identity fraud and double-dipping, ensuring that funding value can be distributed accurately including pensions and other G2C services.

In the payments sector, building a verified onboarding process and replacing private keys, cards and PIN numbers with a robust biometric programme will secure the last mile in financial transactions, providing an additional security layer, and streamlining efficiencies.

Examples of most recent use cases:

- Iris recognition technology provided a lifeline during Covid-19 in locations restricted during lockdown. We enabled door-to-door deliveries of cash within refugee camps in Iraq.
- We enabled mobile ATMs built into CAB vans, which were then able to dispense aid cash to the community in locations restricted due to the lockdown.
- Fixed locations such as supermarkets within refugee camps as well as post offices providing cash payments and verification services remaining operational, thanks to the contact-free nature of the technology.
- Integrated with WFP's blockchain Building Blocks, we helped to authorise food deliveries to 2,500 refugees isolating due to Covid-19 with mobile devices held on socially, distancing sticks are helping refugees in Jordan pay for their groceries with a biometric iris scan, unaffected by face masks.

Iris recognition for KYC assurance

World remittance is not affordable for many vulnerable, displaced and poor populations and they are excluded from participating in the economy. Whether we are seeking a solution for an emergency or post emergency situation, there is a real need to rethink KYC criteria, with minimum information available to the unbanked people to open wallets and transact within the regulated financial eco-system.

This is directly linked to having a verified ID. By enabling digital inclusion, we will enable financial inclusion, increase international remittances and provision of salary assurance. Ultimately it would give the unbanked population an opportunity to build up a credit history, savings and pensions. They'll be able to contribute to the local community they reside in.

Although, whether the project is large or small, whether it's a one off or a long-term commitment or software, implementation includes hard costs such as licenses, hardware and servers. There is also the cost of on-going authentication, ensuring the integrity of KYC, handling complex beneficiary payment lists.

When we were founded in 2001, our technology was utilised at border security, and our systems at UAE airports across 3,273 days prevented over 650,000 offenders from entering. Now, we are very engaged in providing solutions to payments, blockchain and microfinance which help bring assistance to millions on a daily basis.

Empowering global financial inclusion and restoring dignity

There are 82.4 million displaced people globally and children make up an estimated 42% of that. The Clarkson University conducted a recent study on Biometrics, Behaviour, and Identity Science (Iris Recognition Performance in Children: A Longitudinal Study). This showed no evidence that irises age over time in children.

By providing a universal and portable UN identity to refugees and IDPs, beneficiaries are provided with mobility and freedom to move with a strong identity that is their eyes with no one depriving them of who they are.

Biometrics has enabled us to provide assistance to millions on a daily basis, who are now able to receive cash faster and contact-free from ATMs and mobile cash-out agents, buy their food in supermarkets and receive their regular pension payments using solely their eyes as a proof of life. This enables beneficiaries to receive their assistance with increased privacy, security and dignity.

IrisGuard UK Ltd
Eva Mowbray, Director of Marketing
emowbray@irisguard.com

Joined in 2021

19. Laxton: Beyond tomorrow. How biometrics is leading the way for revolutionary changes in travel, security, and the economy

What is the measurement (metrics) of life (bio)? Is it the impact on one or many? Perhaps, it is both. Biometrics has made a direct global impact - and over the past 20 years, it has indeed changed the world as we know. Whether it was an unthinkable act like 9/11 or an unimaginable time like during the COVID-19 pandemic, we have seen biometrics evolve and improve our lives. In a world that has shifted from a handshake to a smile behind plexiglass, we've learned to adapt. Biometrics can continue to help us acclimatize so we can fearlessly continue redefining our norm.

Evolution of border security – biometrics is not the exception

Border management is a hot topic. With upcoming changes for Europe's Entry-Exit-System, attention is being given to how passenger tracking is happening. Without biometrics, the evolution of border security would have stalled. The tools to secure borders have had a tremendous global impact.

The European Union Agency for the Operational Management of Large-Scale IT Systems, eu-LISA, addresses changes in migration and relooks at how a person's stay in a country is recorded to ensure databases are accurate.

Eu-LISA is set to play a crucial role in the technical implementation and development of interoperability of EU information systems, and will not result in the collection of more data, says the agency, but rather more intelligent ways of using existing data.[1]

Biometric technologies have evolved to become more user-friendly. Furthermore, on account of the improved accuracy of new systems, the potential for erroneous and potentially detrimental impacts on innocent users decreases. [2]

As biometrics cannot typically be lost or stolen, when combined with multi-biometric identification, it assists border management. Border control/security was ranked by the Biometric Institute[3] as in the top 5 top trends for the future of biometrics. This report also tells how *face* is the most expected modality in the next 5 years further supporting the importance of non-touch solutions

COVID-19 slowed the world and sped up changes in biometrics

Travel has changed. The ask for efficiency and safety has catapulted forward since the COVID-19 pandemic. For an unnerving period of time, travel came to a halt, but biometrics continued.

Recently, the focus of digitalization has shifted to security, data, and identity to further install trust. Before the pandemic, touchless biometrics were used, but demand has increased. Capturing biometrics can bring unwanted friction to a process. However, the prevalence of fingerprint and/or facial recognition used in personal smartphones has opened up acceptance to using an individual's biometrics for other use cases. Changes in user needs require "smarter" solutions for travel. Biometrics as a service, interoperability, and seamless integration with existing (and evolving) technology becomes more relevant.

Travelers want options, and many businesses have adopted their software offerings using biometrics in mainstream applications to meet changing demands.

These features, exclusive to biometrics technology, provide greater security measures for intellectual assets as well as workplace and individual information in comparison to common user authentication including passwords, user IDs, single sign-on and other traditional access management methods. [4]

Growth for people = growth for a nation

For millions of individuals in developing nations, having a reliable digital identity has opened up access to services, and supported the growth of their economies. Well-designed digital ID not only enables civic and social

empowerment, but also makes possible real and inclusive economic gains—a less well understood aspect of the technology.

Malawi needed a Digital Identity solution for its citizens. This project helped over 9 million Malawians obtain positive digital identities. The project was essential for the country and it was essential for the people of Malawi to access certain civil services, loans and grants. For the first time, when donors would give grants to specific individuals, they could now positively identify these people. When the system is reliable and consistent, the overall growth of an economy improves.

For example, digital ID could contribute to providing access to financial services for the 1.7 billion-plus individuals who are currently financially excluded, according to the World Bank, and could help save about 110 billion hours through streamlined e-government services, including social protection and direct benefit transfers. [5]
Biometrics used for digital identity brings forward opportunities. Malawi is an example of a developing nation positively impacted by biometrics. According to the McKinsey Global Institute by unlocking global economic value across our focus countries, digital ID could unlock the economic value equivalent of 3–13% of GDP in 2030.[6]
The implementation of biometric technologies by governments is happening. While there will always be challenges raised, we should also consider the good impact biometrics has. The more innovation, the more potential.

Where to from here?

What will we embark on in the next 20 years? Will biometrics continue to alter security, travel, and the global economy? Biometrics has earned a place in the safety, security, and growth of our world. Yet, we are still a long way from bringing this technology and its benefits to every person on earth.

Footnotes
[1] Biometric Update: EU eu-LISA industry roundtable to explore AI and biometric database interoperability, Aug 2021
[2] EU LISA REPORT: Biometrics in Large Scale IT, 2016
[3] Biometrics Institute Industry Survey 2020
[4] Cloud-based Identity and Authentication: BIOMETRICS-AS-A-SERVICE, Fujitsu-FrostSullivan, 2016
[5] McKinsey Global Institute: Digital identification: A key to inclusive growth, 2019
[6] McKinsey Global Institute: Digital identification: A key to inclusive growth, 2019

Laxton Ltd
Nick Perkins, President Europe, Middle East & Africa (EMEA)
nickp@laxtongroup.com
+31 702 505 600

Joined in 2021

20. Sandra Leaton Gray: Biometrics in schools – adoption and privacy concerns

21st century schools can be complex, difficult places to manage and attend, not least because schools have grown in size substantially over the last couple of generations, leading to the need for multiple systems of control and regulation. One of the primary issues for governing bodies and local education authorities is reconciling a need for bureaucratic efficiency whilst acting *in loco parentis* – ensuring that the children in their care are where they should be, engaged in appropriate activities at the right time, and being fed at appropriate intervals. Within this space, developers have sought to support schools (and monetise solutions to any number of management problems) through the provision of any number of digital products to streamline and enhance school processes, for example for attendance monitoring, assessment and accounting/audit. It is within this commercial framework that we find biometrics proliferating, and with it, associated privacy concerns.

Biometrics started to be adopted by mainstream schools around fifteen years ago, mainly in countries such as the US and UK, the Netherlands, Belgium and France, with products aimed at monitoring expenditure on school meals, as well as access to library books, or occasionally for building access control. Early adoption figures for these functions are hard to come by, but it is estimated that by 2014, at least 40% of the UK school population had been fingerprinted for such purposes, registered for palm vein readers or registered for facial recognition systems (Darroch, 2011, Big Brother Watch, 2014). Some countries and jurisdictions banned the use of biometrics in schools early on, for example states such as Arizona, Illinois, Iowa, Maryland, Michigan and Florida, as well as countries such as Germany. In other countries and regions there were protests, for example as early as 2005, the French 'Group Against Biometrics' went so far as to smash palm readers in schools. Therefore the adoption of biometrics in schools has always met with controversy (Andrejevic and Selwyn, 2020).

Privacy concerns are generally two fold. Basic systems used for school meals, library book loans and room access engender concerns centred around the misuse of personal data, the likelihood of mission creep in which data collected for one purpose end up being used for another, and the dangers of mosaic identification with databases being illicitly cross-referenced to identify individuals. This is technically possible, but difficult, as so few data points are collected for fingerprint or facial recognition purposes (although this has increased in recent years). The limited data points also represent a reason why biometric systems prove so unreliable in schools, with many children's accounts being confused, for example through meal credits/debits frequently applied to the wrong transactions, as a result of schools being poorly educated as to the important role setting the system's False Accept/Reject Rate properly to ensure fairness, and to avoid the same 10-20 children being regularly confused (much to their chagrin).

The second form that privacy concerns take is related to higher stakes applications where a failure of a biometric system is likely to have serious personal consequences, usually of the disciplinary type. This has been greatly amplified through the introduction of behavioural biometrics to educational settings in more recent years. An example of this is the introduction of virtual proctor software for the remote monitoring of pupils sitting exams at home, which came to attention during the COVID-19 pandemic. These systems track the most minute eye movements, amongst other things, and use a proprietary algorithm to diagnose 'cheating'. These systems, with their opaque analysis, trained on a limited population, are routinely perceived as oppressive and unfair by many examinees. Another example of high stakes biometrics is the introduction of 'emotional' biometrics for behaviour management purposes in the classroom, usually in an experimental capacity, as in the case of a system tested in a Chinese middle school by Hikvision Digital Technology. This latter system was designed to assess whether pupils were paying attention in class through assessing whether their facial expressions were happy, sad, angry, surprised or neutral. It brought resistance from parents and the system was quickly withdrawn. In the academic literature, the introduction of such technologies focused around the audit of the physical body has been described by Swauger (2020) as being representative of a 'punitive pedagogy', with power and control being at the centre of the product design, rather than, say, the growth of knowledge, or human flourishing.

In the light of recent developments, the biometrics industry now stands at something of a crossroads. It can continue to develop and test products on what is a captive population in schools, with minimal attention paid to the social consequences of their long-term use. Alternatively, it can decide to involve stakeholders much more closely in the development of products, through collaborative development approaches that involve significantly less commercial secrecy, so proper scrutiny can take place, and products can be revised and adapted as appropriate. By stakeholders, this should mean pupils, teachers and parents, rather than finance departments or senior management teams who

might be involved in high-level procurement. There also need to be more extensive training populations, in order to take into account diverse cultural and racial backgrounds, as well as any special educational needs. This builds on the Biometrics Institute's policy of appropriate use, providing for an ethical approach to technological tools which are having increasingly profound social consequences.

References

Andrejevic, M. and Selwyn, N. (2020) Facial recognition technology in schools: critical questions and concerns, Learning, Media and Technology, 45:2, 115-128, DOI: 10.1080/17439884.2020.1686014

Big Brother Watch (2014) *Biometrics in schools: the extent of biometrics in English secondary schools and academies* London: Big Brother Watch
https://bigbrotherwatch.org.uk/wp-content/uploads/2014/01/Biometrics-in-Schools.pdf

Darroch, A. (2011) Freedom and biometrics in UK schools *Biometric Technology Today* 2011 (7), 5-7

Swauger, S. (2020) Our bodies encoded: algorithmic test proctoring in higher education. Chapter 6 in Stommel, J. Friend, C. and Morris, S. (Eds) *Critical Digital Pedagogy* (Denver, Hybrid Pedagogy Inc)

University College London Institute of Education
Sandra Leaton Gray
Member of the Privacy Expert Group, Biometrics Institute
s.leaton-gray@ucl.ac.uk

21. Juliet Lodge: Towards an ethical and responsible biometric eco-system

Creating a biometrics eco-system to stimulate an ethical and responsible use of biometrics in all settings has been the hallmark of the Biometrics Institute's work over the past 20 years.

Many of the challenges originally identified by the biometrics community remain. Then, as now, it is important to ensure transparent and privacy-respecting use in order to generate trust in the reliability, security and dependability of the technology and of those private and public sector bodies using it either singly or in partnership for both commercial and more comprehensive public purposes.

The focus has changed over the years regarding the purpose of deploying biometrics for domestic, commercial purposes as well as for matters relating to physical border management at state boundaries, and to accessing public and commercial services in the geopolitical borderless spaces of the digital world. The convenience gain is irrefutable.

Playing catch-up

Managing physical borders using biometrics in passports was a first step that engaged the biometrics communities seeking to develop appropriate technical solutions to accelerate border controls and provide a degree of greater predictive certainty that there was a genuine correspondence between the person presenting themselves at a border gate and the identity in the travel document. The attendant vulnerabilities and security technologies evolved more swiftly than legislation.

It is still the case that technological applications of biometric technologies outpace legislative requirements and regulations. A guiding principle in using biometrics for diverse purposes has therefore been to advocate legitimate and ethical use to ensure clear, privacy respecting, proportionate, consensual, fair, secure, appropriate and responsible deployment of the applications.

This is encapsulated in the idea that just because it is possible to do something with biometrics does not justify their use if the overall effect is disproportionate to the original goal. For example, biometrics payments by children may be considered disproportionate when there are other means of paying that are less intrusive on their integrity as a young person.

Citizens or suspects

Concern persists over biometric applications treating children as 'suspects', linking that to all manner of educational, medical and social information – replete with errors – and over the potential for abuse of a system intended to reassure all using it that it was a credible and appropriate means to expedite otherwise slower and bureaucratic processes.

With opening your phone by iris recognition or fingerprint, voice biometrics for payments, hand or fingerprints to open doors, biometrics seems to have become accepted by a wider public.
However, as the Biometrics Institute has signalled over the years, with greater reach comes greater responsibility for the outcomes.

Beyond behavioural biometrics

In the early days of biometric enrolment and deployment primarily for financial or physical border control management, the Biometrics Institute stressed the need for clarity over both the definition of what constituted a biometric and the purpose of using biometrics. The need for privacy and guarding against function and mission creep have been entrenched in the EU's GDPR. It has become a model of good practice.

But mission creep is widespread and instead of a biometric being defined as a digital representation of an element of a person's physical characteristics (such as a fingerprint) it has become shorthand for everything they do.

Behavioural biometrics may be inferred from neurological as well as loose, social media-based information garnered anywhere, anytime.

As the EU now pushes ahead with realising a digital society, it is striking that once again many of the concerns raised by the Biometrics Institute's members over the years, have re-surfaced.

Biometrics for trustable digital society

As Members of the European Parliament now stress, biometric tools must be used mindfully to sustain public trust. They are particularly exercised now with the issue of biometric-enabled discrimination and mission creep – two issues that Biometrics Institute members stressed in early deliberations over the potentially privacy intrusive impact on the integrity of citizens' data that could arise.

But discrimination and differentiation lie at the heart of using biometrics for diverse purposes. The core question is now not simply whether biometrics should be used but whether the linkage of biometric data to other information about an individual is legitimate, proportionate, secure and beneficial to the individual and society.

In short, the ethical use of biometrics for strictly defined, specific purposes is crucial. Defining a biometric also remains problematic as neurological and medical inferences associable with biometrics may escape current guidelines and regulations.

Then as now, how access to biometrics may be skewed to privileging certain groups over others, often inadvertently, is a public issue. This is raised in the context of building an inclusive and responsive digital society and ensuring steps are in place to enable participation by the disadvantaged, disabled and marginalised.

Biometric bias

Whether biometrics should be required to unlock and link up information stored by commercial, financial and government bodies again requires reflection on the kind of biometric eco-system that evolves during this decade where artificial intelligence capabilities derive decisions from scanning biometrics – and other information – to build new 'pictures' of individuals on which further decisions are taken, again often without the intervention of human agency.

If the original algorithm is flawed, biased towards detecting certain biometrics or based on fake, misleading or false information, citizens face even greater problems getting it corrected. The onus for reliable, dependable, secure and trustable biometrics has never been greater on the creators of ever more precise potentially intrusive biometrics, such as those allegedly predicting and recognising emotional states and thought patterns.

The reliability and accuracy of systems such as iBorderControl has been challenged recently in court, and casual use of biometrics (or their scraping for unknown and unknowable purposes by unseen bots) alerts us to how readily public trust in biometrics can be eroded by careless use or misrepresentation.

MEPs are rightly concerned about the potential consequences of sensitive identifying personal data (including biometric information stored in crisis situations for instance) being misappropriated, compromised, re-spliced and sold. If biometric data collection is seen as enabling illegitimate surveillance public trust in the applications and both private and public authorities will suffer.

An ethical biometric eco-system fit-for-purpose

Biometric applications are neither value-free nor neutral in their impact. The challenge in refining the biometrics eco-system therefore lies with harnessing a deeper appreciation of the way in which biometric applications benefit society. Working together with policymakers and society in creating a digital society is therefore essential. The Biometrics Institute community has considered not just who provides the biometric but crucially who has access to it and for what purpose precisely. Meeting that challenge is as valid today as 20 years ago.

Juliet Lodge
Member of the Privacy Expert Group, Biometrics Institute
juliet@saher-uk.com

22. Robert Mocny: The United States implements the world's first biometrics border control program

This September the United States paid solemn tribute to the memories of close to the 3000 people who died twenty years ago on 9/11, 2001. Early that morning passenger planes commandeered by terrorists were flown into the twin towers of the World Trade Center in New York City, one into the Pentagon, and another forced to crash in an open field in Pennsylvania by heroic passengers who believed it was headed for the Capitol in Washington, DC. What led to those events was investigated by then President George Bush's Administration, the Congress, and many other public and private institutions.

One finding consistent with all these reviews was that the United States needed to strengthen its immigration and border policies and procedures. How did 19 terrorists slip through the visa and admission processes that had been in place for the past 50 years? In short, the United States needed to do a better job of sharing intelligence and identifying people with greater certainty. This all led to the creation of the Department of Homeland Security (DHS) and the United States Visitor and Immigrant Status Indicator Technology - or US-VISIT - program. I was fortunate enough to serve as the first deputy director and later director of US-VISIT and had the honor to lead a few hundred dedicated professionals to create the world's first biometric visa and border control program.

In 2003, when US-VISIT came into being through the leadership of DHS' first Secretary Tom Ridge, biometrics was not a term most people were familiar with. People understood fingerprinting for people who may be arrested or who may be applying for a teacher or bus driver job. But biometrics as part of applying for a visa to the United States? Biometrics taken from people arriving at our ports of entry? Unheard of.

This was the challenge we faced at US-VISIT: How to develop the policies, processes, and technologies to allow for the capture of biometrics, in our case two index fingerprints, from the millions of tourists who visit the United States every year and not cause huge delays at our embassies and consulates overseas or at our more than 300 ports of entry. As with any new process or technology we had to walk before we could run.

At US-VISIT we worked with the Departments of State and Justice, as well our sister agencies now part of DHS - Customs and Border Protection, United States Citizenship and Immigration Services, and Immigration and Customs Enforcement among others. On, or near day one, US-VISIT established one of DHS' first Chief Privacy Officers to ensure that whatever processes we put in place were clearly understood by the public as to why we were taking their biometrics; where we were storing their biometrics and; with whom we would share their biometrics.

We worked with technology companies to give them a clear understanding of what we required from them. How accurate and how fast the capture devices needed to be. A few years later, when we wanted to capture all ten fingerprints as opposed to just the two index fingers, we told them what size the devices needed to be and even what color the devices should emit (the original glowed red and was seen as off putting to many and we insisted on a more acceptable color which is now the green glow you see on most fingerprint capture devices).

And as our allies stood with us after 9/11, we at US-VISIT worked closely with Australia, Canada, New Zealand, and the United Kingdom to share our technologies and information. After a while, the five countries developed a compatible system to share critical fingerprint and identity information that helped protect not only the individual countries, but all of us collectively as terrorists and international criminals do not limit themselves to just one country.

And through all of this, we needed to keep the public informed as to what we were doing and why we were doing it. Why did we need their biometrics and what did we do with their biometrics? At US-VISIT we had a robust Office of Public Affairs which coordinated public speaking engagements, participation on panels at conferences, and joining organizations that not only allowed us to speak to the public, but which actively supported the ethical use of biometrics. One of the best forums we were able to be a part of was the Biometrics Institute. As the Institute turns 20 years old this year it reminds me of how critical it was for us to reach out internationally. Being a member of the Biometrics Institute gave us access to like-minded governments, technology companies, scientists and academics and discussion groups that gave us a platform to explain to the world what biometrics did to improve the security of the United States.

And during these past 20 years many others have adopted the use of biometrics and are exploring new modalities. The European Union developed Automated Border Control using facial recognition for EU citizens. The United States Customs and Border Protection have embraced facial recognition to ease entry for US citizens and are piloting its use for exit control. Apple lets you unlock your phone with your face. Amazon is using biometrics to expedite your shopping experience. The use of biometrics will continue to grow.

US-VISIT is now the Office of Biometrics and Identity Management (OBIM) and its senior leaders and many of the professional women and men of OBIM are active members of the Biometrics Institute. As the use of biometrics continues to evolve and new modalities and technologies are created it is my hope that the Biometrics Institute will also evolve and grow the services it offers to its members. From its association with the United Nations to the publication of the Three Laws of Biometrics and the Good Practice Framework I suspect that 20 years from now there will be someone in the biometrics field today or in the future who will want to offer a similar tribute to the Biometrics Institute.

Robert A Mocny
Former Director of the United States Visitor and Immigrant Status Indicator Technology Program (Retired)
Member of the Advisory Council, Biometrics Institute

Robert Mocny joined the Institute with the US Department of Homeland Security (DHS) in 2015

23. Reason360: Among us

In September 2001 I would reach into my pocket to take out a small folding leather case; another pocket contained a portable telephone for telephone calls, short messages, and Snake. In the leather case were about ten plastic cards – perhaps a little smaller than my palm – most containing magnetic coding. Having selected the appropriate card, I would insert it into a machine, enter a short numeric code known only to me and wait a few pregnant seconds for the machine to confirm its satisfaction with both card and code. Finally, I would remove the card and replace it in the case, and then the case in my pocket. All up this took perhaps 30 seconds, although sometimes – say when two different cards were needed to track my activity and pay for it – it might have taken as long as a minute.

In September 2021 my watch observed my pulse to determine whether it had stayed on my wrist since receiving input that morning of a numeric code known only to me. If it had, I could indicate approval for it to communicate with the next compatible reader it encountered by double-tapping a button, then presenting the wrist and watch to such a reader to complete a transaction. This took perhaps 10 seconds in all, including both removing and replacing hand in pocket if so desired.

For information requiring a greater area for presentation such as providing evidence of my licence to drive, the portable telephone had been replaced with a portable computer that recognised me by face and allowed me to present this information securely on screen upon demand. The leather case was consigned to the drawer for things never to be needed again.

Just like the rest of humanity's technological output, consumer adoption of biometrics has been led by convenience. And just like other recent technological advances that have out-convenienced the alternatives, vague notions of information trust have underpinned acceptance of biometrics in consumer devices. Simultaneously a different need for trust at a much larger scale – that between organisations, governments, and individuals – has combined with the inconvenience of the alternatives to drive usage of biometrics with explicitly centralised control over biometric information.

Many other examples of biometric-driven transition over the last 20 years can be cited. In some, like in my own field of customer service delivery at scale, biometric service delivery experiences are engineered with the utmost in simplicity and customer self-reliance in mind; in other fields such as border control, the continuous presence of real people in a physical area where movements are being controlled allows a high level of confidence from the combined biometric-human operation; in yet others, biometrics have been used to simplify everyday activities such as photography.

This two-decade rise in biometric usage has happened at the same time as another civilisation-wide transformation: the slow increase in artificial intelligence. While the intellect demonstrated artificially today is deficient in many ways, it is nearly certain that this will improve, and that we will end up with a new set of actors influencing the world around us. It is entirely possible (albeit by no means certain) that these artificial actors – 'the machines' if you like – will appear among us within the next 20 years.

Fundamentally this leaves us with a question: do we want these machines to be able to recognise us?

It also leaves us with the inverse question: what if the machines could *not* recognise us? Is it conceivable that they could even *exist*, absent the capacity for recognising us?

These big picture questions translate into hundreds of smaller points about individual biometric implementations, selections of use cases, data exchanges, security requirements, relationships between physical and digital identities, vulnerabilities to confusion, privacy, and many other subjects.

The first 20 years of the Biometrics Institute's existence have largely been spent helping the many types of engaged stakeholders to think carefully about these points, by connecting people and providing guidance. In that time the bigger picture questions have loomed over us, casting an indistinct image across our work. But that image is slowly coming into focus, and will I expect demand greater attention from both the Institute and society at large over the next 20 years as we shape this most important part of our future world.

In September 2041 I take the goods and commission the services I want when I want them; and any identity information or transactions required are automatically performed according to my chosen preferences – unless I instruct an ever-present artificial assistant otherwise. I spend time on exception cases when needed, not on typical daily occurrences; and the watch is worn for decoration, not function.

Hundreds of years of technological advancement have slowly brought benefits and convenience once only available to the wealthy down to the average citizen. And here we are contemplating no longer having to carry means of payment or information, a little like the Queen.

It could be argued that the price of great wealth is fame – that is, a lack of anonymity.

Hopefully that is not the price of convenience for all of us.

Reason360
Brett Feldon
Head of the Digital Identity Group, Biometrics Institute
+61 457 817 326
brett@reason360.com.au

24. Scottish Biometrics Commissioner: From World's End - to world leading: Biometrics within the National Policing Model for Scotland

The pre-digital age: A personal reflection

Biometric data such as fingerprints and photographs have been used in policing and criminal justice in Scotland as a means of verification, identification, and exclusion for more than 100 years.

In April 2021, I was appointed by Her Majesty the Queen on the nomination of the Scottish Parliament as the first Scottish Biometrics Commissioner. My own career as a police officer in Scotland, and my personal biometric journey had commenced 43 years earlier in Edinburgh, Scotland. Back in 1978, the police had only the most basic of technologies and it would be another 5 years before the launch of Microsoft Word. Fingerprints of persons arrested were taken manually with ink, and photographs were taken on the 'latest' Kodak camera complete with spool and reel. DNA profiling had not yet been established for criminal investigations, and there were no automated biometric databases.

Police forensics were similarly constrained requiring a blood stain the size of large coin to simply identify a blood type.[5] With limited science and technology, the pre-digital age of policing was beset with unsolved high-profile crimes. In 1978 Edinburgh, this included the 'World's End Murders' a colloquial name given to the murder of two girls Christine Eadie and Helen Scott, both aged 17 years, who were last seen alive after leaving The World's End pub in Edinburgh's Old Town in October 1977.

The digital era

Since the late 1980s, the advent of the forensic technique of DNA profiling has transformed the investigation of crime. It is used daily in the investigation of a wide range of offences to identify offenders from minuscule amounts of body fluids and tissues. In sexual offences, DNA profiling can untangle complex mixtures of body fluids, typically found in such cases, to provide evidence that was previously unavailable. Through the introduction of DNA24, Scottish Police Authority Forensic Services now provides Police Scotland with one of the most advanced DNA interpretation capabilities in world policing. The digital era also witnesses the introduction of automated fingerprint capture and recognition systems, automated facial search capability, and the introduction of ISO standards for forensic laboratory work and the independent accreditation and validation of the underpinning scientific techniques.

DNA time capsules

In 2014, one year after the creation of a single national police service for Scotland (Police Scotland) and a single forensic services provider (Scottish Police Authority Forensic Services) advances in DNA technology contributed directly to the conviction of Angus Sinclair for the 1977 'World's End Murders' concluding a 37-year long police investigation. Sinclair (now deceased) was given the longest sentence ever handed down by a Scottish Court.
Similarly, in May 2021 the mystery of the 1984 murder of Mary McLaughlin in Glasgow was solved after forensic experts extracted 35-year-old biological material from inside the knot of a ligature used on the victim.[6] Using Scotland's world leading DNA24, forensic scientists profiled 24 genomic sequence markers (the UK and Interpol policing standard is 17 DNA markers) establishing a DNA profile match against convicted sex offender Graham McGill. These cases, demonstrate just how far forensics and biometrics have advanced in the last two decades and how forensic techniques and biometric technologies have contributed positively to society. Such technologies do not of course establish innocence or guilt, but they do assist human investigators in ways which are often unquantifiable. Biometrics help fix identity, and will continue to enhance incriminatory, exculpatory, and deterrence value in the

[5] Forensics stop people getting away with murder, BBC, 13 August 2021: https://www.bbc.com/news/uk-scotland-58188079
[6] Mary McLaughlin Murder: Killer jailed after DNA solves 35-year mystery, BBC, 18 May 2021: https://www.bbc.com/news/uk-scotland-glasgow-west-56505250

future. By illuminating 'DNA Time Capsules' in cold case reviews, they also provide redress to the families of victims from earlier decades who had long given up any hope of justice.

Our biometric future

More recently there has been an exponential growth in a range of new biometrics in law enforcement, perhaps most controversially the use of public space facial recognition surveillance by the police in other jurisdictions. There has also been a proliferation of databases operating and exchanging biometric data over different legal and functional jurisdictions, including the application of artificial intelligence to those databases to develop algorithms for biometric matching.

Such issues raise important questions for society, including how best to balance our need for public safety and security, with broader privacy, ethical, human-rights, and equalities considerations.

In 2020, The Biometrics Institute devised the '***Three Laws of Biometrics'*** to prompt its members to remember the fundamentals of using biometric technology responsibly and ethically:

1. **Policy – comes first:** Any use of biometrics is proportionate, with basic human rights, ethics, and privacy at its heart.
2. **Process – follows policy:** Safeguards are in place to ensure decisions are rigorously reviewed, operations are fair, and operators are accountable.
3. **Technology – guided by policy and process:** Know your algorithm, biometric system, data quality and operating environment and mitigate vulnerabilities, limitations, and risks.

In Scotland, the policy first approach has witnessed the creation of a single national police service, a single national forensic services provider, significant investment in advanced biometric technology, and the appointment of an independent Scottish Biometrics Commissioner answerable to the Scottish Parliament. Reflecting on the title of this article 'From Worlds End - to World Leading' I would posit that the approach to biometrics delivery and oversight for policing and criminal justice purposes in Scotland safeguards our biometric future by following the 'Three Laws of Biometrics' advocated by the Biometrics Institute. In jurisdictions where the use of biometric technologies has proved more controversial, these rules have sometimes been overlooked, and technology has not been adequately guided by policy and process.[7]

> ***'New technology is not good or evil in and of itself. It's all about how people choose to use it'***
> *(David Wong, podcast geeks guide to the galaxy, science-fiction podcast, episode 171. October 2015).*

Scottish Biometrics Commissioner
Brian Plastow
Brian.Plastow@biometricscommissioner.scot

Joined in 2021

[7] UK Court of Appeal, Case No C1/2019/2670, 11 August 2020 in review of case of Bridges vs Chief Constable of South Wales Police: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

Research and development

25. Secunet: Efficient and secure border control thanks to eIDs and biometrics

Electronic identity documents and the biometric data stored in them form the basis for automated border controls and convenient passenger processes, as we know them today. How did we actually get this far? On the occasion of the 20th anniversary of the Biometrics Institute, we take a look back at the developments of the last two decades – and congratulate the Biometrics Institute on this milestone!

The addition of the electronic component to the established optical security features made storing biometric information in chips of eIDs possible. At the same time, biometrics created a unique link between document and document holder. In addition to a significantly higher level of forgery protection, this simultaneously opened up the use of biometrics-based automated border control. Biometrics in eIDs and the associated convenience are now taken for granted worldwide. However, the path to success was certainly not always a straight line and many steps have been taken.

Real added value can only be achieved through interoperability

The addition of biometric data to eIDs alone does not add value. First, it must be ensured that eIDs will be accepted and can be processed at borders around the world. Second, the binding between eID and its holder through biometrics enables a higher level of security and, at the same time, new digital processes. Two aspects, however, highlight the importance of interoperability:

The dynamic market for biometric technologies:

- Many devices and manufacturers, short product life cycles.

The sheer mass of eIDs:

- 1 billion eIDs were issued from 150 states in 2019.

In numerous interoperability tests, we supported manufacturers of eIDs and inspection systems in optimizing components and making them fit for international use.

These tests have shown the importance of cooperation between states, sovereign authorities, and industry. With the growing potential for biometrics, independent organisations such as the Biometrics Institute were essential in the process - connecting all stakeholders and providing a platform to exchange innovative ideas as well as concerns.

Standardisation is the key

The essential parameters for the use of biometrics in eIDs and the quality and security requirements for their use in sovereign applications have been defined and further developed in international standards. They regulate a wide variety of aspects, one focus being the protection of biometric data over the entire lifecycle of sovereign eIDs, e.g., during document issuance, the security mechanisms and access rights during document verification as well as the responsible use, including appropriate and data protection-compliant handling.

One of the first important standards for automated border control was ICAO Doc 9303, which is still the gold standard for eIDs but also an important prerequisite leading to the widespread use of biometrics in public sector applications. A milestone for biometric data protection in sovereign eIDs was certainly the BSI TR-03110 of the German Federal Office for Information Security, which is still valid today, and we were involved in its development. BSI TR-03110 specifies, among others, Extended Access Control (EAC) for access to biometric data stored in eIDs and can be regarded as the foundation for all security protocols for sovereign eIDs - it also had a significant influence on ICAO Doc 9303 Parts 10,11.

Standards continue to be an important tool for all stakeholders to jointly implement a consistently high level of security for handling biometric data in eIDs, on the application as well as technology side. Especially for biometric systems, standard conformity on every level assures the accuracy, thus the reliable use of the system.
Just how did these standards evolve, and what does it take to develop them?

Experience through a valid database

A prerequisite for standardisation is data and experience - this is a lasting truth. For the use of biometrics in sovereign eIDs, this initially meant collecting a lot of data – a biometrics aficionado will certainly remember the BioP I and II projects.

Together with the German Federal Criminal Police Office, we conducted a large field test at Frankfurt Airport and compared biometric verification algorithms (face, finger, iris). The results formed the basis for the selection of biometric features of the electronic passport in Germany. Both studies marked the start of many subsequent projects to investigate and evaluate biometric procedures, from which the entire market profited in form of standards and technical guidelines.

These steps - data collection, standardisation, interoperability - were essential key factors for the widespread use of biometrics today. They ensure data is reliably usable in accordance with specifications in terms of quality, security and speed.

Secure eIDs in everyday life

Standards and the worldwide spread of biometric travel documents have opened up completely new possibilities: Increasing passenger numbers could now be addressed through automated border controls (ABC). Aside from the current COVID-related slowdown, the demand for biometrics in border control and passenger identification has been increasing worldwide.

In the German EasyPASS project, for example, ABC systems have increased from 70 ABC gates in operation at four airports in 2014 to more than 250 ABC gates at eight airports today with a total of 95 million users.
For biometrics-based automated border control, protection against circumvention attempts plays a major role. Current standardisation efforts and developments focus on continuously improving procedures to detect fraud attacks through, e.g., presentation attack detection (PAD) or morphing attack detection (MAD).

Summary and outlook

There are plenty of challenges for biometrics in public sector applications such as border control. Biometric data is a sensitive asset that must be protected. A multitude of standards are binding in terms of which data may be collected, used and stored, and in which quality. Security, usability and user convenience must always be balanced for the specific applications needs. Continuous development of corresponding standards is essential in order to meet current and future requirements for secure biometric procedures and to effectively prevent attempts to overcome them. New possibilities that arise, for example, through artificial intelligence (AI), will play a decisive role here – plenty of work for the Biometrics Institute, and other important players in the biometrics community.

Secunet Security Networks AG
Georg Hasse
info@secunet.com

Secunet were a Founding Member in Europe

26. Thales: How facial recognition revolutionised the future of access control

How facial recognition revolutionised the future of access control

It's undeniable that biometric technology has greatly enhanced many core aspects of our lives. Whether enabling access to highly secure areas or unlocking our smartphones in an intuitive yet secure way, biometrics have revolutionised the way we protect and access sensitive information or resources over the last 20 years.
The impact of biometric technology has been particularly powerful in modernising access control. In the case of facial recognition, biometrics have provided administrators of restricted areas, such as construction sites, airports or banks, with a new identification method unlike anything previously used. Let's delve deeper into how facial recognition has re-written the rules of access control.

The problem of physical credentials

Before the application of biometric technology, most administrators across secure sites around the world built their access control strategies around the issuance of physical credentials, such as personalised photo identity cards or non-personalised swipe cards. While this method of authentication isn't yet totally obsolete, the use of physical credentials is not without its issues.

The primary problem with physical credentials is the authentication process, which relies on accurate manual checking by staff at entry points. As well as being slow and labour intensive, it is difficult to consistently and reliably make a visual match between the ID card and its holder. And, in the case of non-personalised swipe cards, the accurate verification of card holders becomes even more unattainable.

Both these single-factor methods of authentication can be easily circumvented. Simple techniques, such as badge swapping or theft, can quickly allow unauthorised parties access to restricted sites. What's more, tactics such as 'tailgating', where an unauthorised person follows an authorised person into a secure environment, are also enabled by staff using physical credentials. Lastly, losing or forgetting physical credentials is a major pain point for users and another time-consuming challenge for management.

The power of facial recognition in access control

First pioneered in the 1960s, with the first semi-automated use coming in 1988, the use of facial recognition technology throughout our everyday lives has skyrocketed over the past 20 years. Perhaps unsurprisingly, access control operators have embraced the benefits of facial recognition.

One of the main reasons for this positive reception is the speed at which these systems operate, almost instantly matching a face captured by a camera to the reference digital facial template of the individual stored on a database. Compared to manual systems, the time taken to verify individuals using facial recognition is dramatically reduced, with the authentication process taking place in less than a second. At the same time, the accuracy and reliability of identification is significantly enhanced. As a result, facial recognition eliminates the need to make trade-offs between efficiency and security. Instead, the two can go hand-in-hand.

The other core benefit of facial recognition is the convenience it provides to the user and the administrator. In the case of the former, workers entering and exiting secure sites do not need to constantly have their physical credentials on their person, be it an ID card or electronic key-fob. What's more, with the removal of physical credentials, administrators can significantly reduce the risk of these items being stolen, cloned or lost, providing that additional level of privacy and security that administrators seek.

An added benefit of removing physical credentials is that it allows users to enter and access restricted sites without touching any surfaces. This is particularly important in a time where minimalising physical contact has become a priority. With facial recognition access control, what was once a system based on the exchange of physical credentials has now become a seamless, touchless experience, further underpinning the technology's benefits.

Looking forward: What's next for physical access control?

In the coming years, the use of facial recognition in access control is only set to increase, with predictions showing that the facial recognition market will grow to $8.5 billion by 2025. While the increased uptake in these systems will improve the security of access-controlled sites, the industry will see more sophisticated spoofing attacks from unauthorised parties. Whether it's increasingly life-like masks or realistic video sequences presented to scanners, the growing use of facial recognition could unearth a wide range of new presentation attack instruments (PAI).
But, while the attacks on facial recognition systems have advanced, so have the systems themselves. How, you ask? With the power of artificial intelligence (AI). By adding bespoke AI software, such as liveness detection algorithms, developers have been able to vastly improve the accuracy of these systems. Combining AI with increasingly sophisticated tests from bodies such as NIST, facial recognition systems are in the best position ever to tackle modern presentation attacks.

The need to stay ahead of hostile actors looking to gain access to restricted sites will remain the priority when it comes to access control. And, while physical credentials have their purposes, the game has fundamentally changed. This seismic shift is predominantly due to the increasingly sophisticated techniques used by these hostile actors attempting to enter controlled areas. But with rapid advancement over the past decade, facial recognition now offers operators of controlled access sites an answer to access control, while offering users a more convenient method of authentication.

Thales
Kadie-Ann Fyffe
+33 1 55 01 54 26
kadie-ann.fyffe@thalesgroup.com

27. UNHCR, The UN Refugee Agency: Supporting refugees and humanitarian service delivery using biometrics

By the end of 2020, 82.4 million individuals were forcibly displaced. This equates to more than one in every hundred people across the world, the largest number in modern history. UNHCR, the UN Refugee Agency, is a global organization dedicated to saving lives, protecting rights and building a better future for refugees, forcibly displaced communities and stateless people who have fled violence, persecution, war or disaster at home.

UNHCR has worked for more than 70 years to help people forced to flee across enormously varied environments. UNHCR's operations are highly dependent on the collection and use of personal data for humanitarian delivery. Understanding who a person is, is critical to being able to deliver life-saving support. The identities which UNHCR protects have been lifelines for people in need.

The first use of biometrics in UNHCR was in 2002. While initially collected without links to other biographic data in Pakistan from Afghan refugees returning home to facilitate the fair issuance of cash grants once to each family, UNHCR has since evolved its use of biometrics. Biometrics data is now considered an integral component of registration data and is processed in 79 country operations. Since the introduction of their use, biometrics have brought direct benefits to refugees, UNHCR and partners alike.

Refugee financial inclusion and self-reliance are key aims of the 2018 Global Compact on Refugees. As well as reliably establishing and preserving identities, improving operational efficiency and protecting refugees against fraud, the increased use of biometric data to support UNHCR's registration and identity management work has opened up new approaches and possibilities to support the Global Compact objectives.

Displaced people often face formidable regulatory barriers in accessing services, such as registering a SIM card in their own name or opening a bank account. These obstacles can inhibit not just the efficient delivery of humanitarian assistance but also a refugee's ability to keep in contact with family or to ably participate in a host state's economy. Many refugees do not hold identity documents from their country of origin or the refugee identity credentials they do possess are not fully recognized by the host-state authorities.

In Uganda UNHCR and the United Nations Capital Development Fund worked together with the telecommunications regulator and the Office of the Prime Minister as well as with mobile network operators, internet service providers and humanitarian agencies in an effort to extend connectivity to refugees and their hosting communities. As a result, a directive was issued from the Uganda Communications Commission UCC to all mobile network operators to open SIM Card registration to those with refugee identity cards or attestation letters.

A key enabler to the directive was access to the biometrics secured by UNHCR. The SIM registration process for Ugandan nationals using automated biometric and biographic KYC checks was extended to cover the refugee population checking against biometric data collected jointly by UNHCR and the Government of Uganda. With biometrics offering comparable levels of identity assurance and process integrity for refugees as was in place for Ugandan nationals, over 600,000 refugees were provided with a legal pathway to accessing cellular connections for the first time.

The strengthening of registration data with biometrics has also helped other states to support the Global Compact objectives and promote the financial inclusion of refugees. Following the introduction of biometrics to registration processes, jointly issued UNHCR-Government identity attestations in the Democratic Republic of Congo and in Malawi were recognized as providing sufficient assurance to meet KYC requirements for the first time for the opening of refugee bank accounts, and for SIM card issuance in Niger. States in these situations have allowed markets to grow and families to communicate with ease where separation in times of conflict had previously resulted in isolation.

In Somalia, when former refugees return from Kenya with UNHCR identity attestations, their identities can be verified by UNHCR and the Government of Somalia using UNHCR's biometrics system. Based on this verification alone, UNHCR and the Government can issue an official Proof of Return document which is sufficient even in the absence of any other official identity documents for the refugee returnees to immediately open bank accounts.

In today's world, where we witness more and more cuts to the food rations of refugees, making sure that the assistance provided to every refugee is maximized and does not fall into the wrong hands is not only important, but life-saving.

In Iraq, UNHCR reduced the onboarding time for new individuals opening an account with a financial service provider from over two months to under three seconds by forming a partnership between the financial institution and an iris-biometrics payment solutions company. The partnership strengthened protection against fraud and identity misrepresentation through iris authentication. More than 120,000 vulnerable families and approximately 30,000 refugees in Iraq received cash support via UNHCR, with the agency disbursing over $60 million USD through its partners in 2018 alone. Refugees have the option to cash-out using iris without any needing any other identification in addition to existing mechanisms. Since the launch of the project in 2019, over 90,000 transactions were performed in this way.

UNHCR has also introduced self-service processes in Jordan and other countries, empowering refugees to have more access and control over their data stored with UNHCR, enabling them to validate and update data previously collected during registration. Self-renewal has also proven time saving for refugees, cutting down sometimes long waiting times in registration centres and increasing accessibility.

In the longer term, UNHCR aims to enable refugees, with their consent, to update data remotely and have access to a unique, portable, trusted digital identity to promote inclusion in civil society and state systems. Enabling refugees to authenticate against the biometric data collected from them has ensured that UNHCR can deliver on its humanitarian mandate and interact with refugee families with a high degree of confidence. No one would deny that the collection and storage of biometric data by UNHCR comes with a huge responsibility to continuously assess how it is secured, used and ultimately destroyed. Alongside diligently managing the risks, UNHCR will continue to focus on how the responsible and ethical use of biometrics can improve the way it serves and benefits the lives of the people it seeks to protect.

UNHCR holds 'International Observer' status with the Biometrics Institute and has contributed to a number of Institute events and products over its history, including the recent Good Practice Framework.

UNHCR – The UN Refugee Agency
Sam Jefferies

Joined as International Observer in 2019

28. UK Information Commissioners Office: Biometrics: data protection by design and default

With any new biometric technology, building public trust and confidence is essential to ensuring that its benefits can be realised. Where more sensitive categories of personal data are processed, for example via Live Facial Recognition (LFR) for the purposes of unique identification, the public must have confidence that its use is lawful, fair, transparent and meets the other standards set out in data protection law.

Biometric data extracted from a facial image can be used to uniquely identify an individual in a range of different contexts. It can also be used to estimate or infer other characteristics, such as their age, sex, gender or ethnicity. The UK courts, in the case of R (Bridges) v Chief Constable of South Wales Police and Others, have concluded that "like fingerprints and DNA" [a facial biometric template] is information of an "intrinsically private" character."[8] LFR in particular can collect this data without any direct engagement with the individual. This means it has greater potential to be used in a privacy-intrusive way.

The UK GDPR requires controllers to take a data protection by design and default approach to help them comply with the UK GDPR's fundamental principles and requirements, and forms part of the focus on accountability. This approach is explored further below, and is particularly important in the context of LFR because many issues of fairness, necessity and proportionality need to be addressed during the planning and design stage of a system.

LFR: The Information Commissioner's opinion

The Information Commissioner previously published an Opinion on the use of LFR in a law enforcement context. It concluded that data protection law sets high standards for the use of LFR to be lawful when used in public places. The Information Commissioner's Office (ICO) has built on this work by assessing and investigating the use of LFR outside of law enforcement. This has covered controllers who are using the technology for a wider range of purposes and in many different settings.

This work has informed the ICO's view on how LFR is typically used today, the interests and objectives of controllers, the issues raised by the public and wider society, and the key data protection considerations. The Information Commissioner has published a separate Opinion to explain how data protection law applies to this complex and novel type of data processing.

Key requirements under data protection law

Any use of personal data must be lawful, fair, necessary and proportionate. These are key requirements set by data protection law. Where the personal data in question is particularly sensitive, such as biometric data, there are stronger legal protections. Where the processing is automatic and there is a lack of choice or control for the individual, again there are stronger protections. This means that when LFR is used in public places for the automatic and indiscriminate collection of biometric data, there is a high bar for its use to be lawful.

The Information Commissioner has identified a number of key data protection issues which can arise where LFR is used for the automatic collection of biometric data in public places. These have been identified through the ICO's investigations, our work reviewing data protection impact assessments (DPIAs) and wider research. These issues include:

- the governance of LFR systems, including why and how they are used;
- the automatic collection of biometric data at speed and scale without clear justification, including the necessity and proportionality of the processing;
- a lack of choice and control for individuals;
- transparency and data subjects' rights;
- the effectiveness and the statistical accuracy of LFR systems;
- the potential for bias and discrimination;
- the governance of watchlists and escalation processes;

[8] R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341, paragraph 59

- the processing of children's and vulnerable adults' data; and
- the potential for wider, unanticipated impacts for individuals and their communities.

For any use of biometric data, controllers must perform a DPIA for any processing that is likely to result in a high risk to individuals. This includes the broad spectrum of biometric characteristics that may be used to uniquely identify an individual, and monitoring publicly accessible places on a large scale.

Data protection by design and default

Data protection by design and default is about embedding data protection into everything controllers do, throughout all processing operations. They should therefore consider privacy and data protection when procuring, purchasing or developing any biometric systems. They should also ensure biometric products or services they adopt from vendors have been designed with appropriate data protection and privacy-preserving features built-in. Controllers, not technology vendors, are responsible for this under the law.

It is important that controllers do not deploy "off-the-shelf" solutions without adequate due diligence to understand the technical processing and associated privacy implications. Controllers also should consider whether a biometric system, such as LFR, is designed with data subjects' rights in mind. For example, they should have the capability to isolate and extract personal data in response to a subject access request, other individuals' rights or for disclosures to authorised third parties unless valid exemptions apply.

In the specific context of LFR, it is especially important that controllers set out clear processes and policies governing its use, including:

- The circumstances in which the controller may activate the LFR system;
- Clear criteria and governance for any watchlists;
- Well-defined procedures for intervention in the event of a match and clear escalation measures;
- How data subjects are informed, how controllers will handle complaints, and how they will fulfil the public's data protection rights; and
- Processes to continually monitor the impact of the LFR system and assess whether it continues to be fair, necessary and proportionate.

The Information Commissioner recommends that by integrating data protection considerations at the very start of any biometric processing, and documenting any decisions that are made in a DPIA, will help controllers comply with their legal obligations under data protection law. This will also enable controllers to adopt the data protection by design and default approach.

UK Information Commissioners Office
Steven Wright
Member of the Future Direction Group, Biometrics Institute

Joined in 2020

29. Department of Homeland Security, U.S. Customs and Border Protection: The Development of the Biometric Entry/Exit Program as a Key Recommendation in the 911 Commission Report

As we mark a key milestone – the 20th anniversary of the tragic events of September 11, 2001 – we remember where we were on that devastating day, think of the victims and their families, and remember the lasting impacts on our country. Following the terrorist attacks, the Department of Homeland Security (DHS) was created in 2003, through the integration of all or part of 22 different federal departments and agencies into a unified Department. The Entry/Exit mission, which included the development of an automated entry-exit system that would collect records on foreign travelers who arrived to and departed from the United States, was transferred to the newly created US-VISIT Program office at DHS.

Through several pieces of legislation that followed and as a key recommendation of the 911 Commission Report, the development of an Entry/Exit system would now include the collection of biometrics – two fingerprints and a photograph -- for foreign travelers on arrival and departure. US-VISIT successfully launched biometric entry in phases starting in 2004 – collecting two fingerprints and a photograph – of foreign travelers at airports and seaports and implemented a biometric entry process at all U.S. land borders at the end of 2005.

However, the implementation of a biometric exit process posed several challenges given the co-mingling of domestic and international travelers and the lack of infrastructure for exit processing at U.S. airports and land borders. Over the years, US-VISIT implemented a variety of biometric exit pilots, including testing some concepts in partnership with U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) to evaluate the optimal process to collect biometrics for departing travelers. Given the cost and amount of resources needed to build and staff a new biometric exit process, it became clear that DHS would need to come up with an innovative solution to successfully meet this security mandate.

When the Entry/Exit mission was transferred to CBP in 2013, we took the challenge head on by deploying new pilots and working closely with stakeholders in the air travel industry and biometrics industry to plan a path forward. The collaboration and partnership, combined with CBP's creative approach to the way we use our own data, resulted in real momentum, and led us to where we are today: the expansion of biometric exit fully, or partially, to 32 airports.

To advance the biometric exit mandate, we have partnered with the air travel industry to implement a secure, stand-alone system that can be seamlessly integrated into the boarding process. While the airlines and airports have purchased the facial biometric technology (camera) for biometric exit, we have built a facial biometric matching service that the airlines, airports, and TSA can access wherever traveler identity verification is required throughout the air travel journey such as check in, bag drop, security checkpoint, and boarding.

A camera can be installed at an airline departure gate without any necessary changes to existing airport infrastructure and is minimally disruptive to the flow of travel. We chose facial biometrics because of the photographs that are already in government holdings that CBP can compare against (e.g. passport, visa, and previous entries); it is an intuitive process as just about everyone knows how to take a photo; and it integrates seamlessly into the airport boarding process. When departing from select airports during international travel, passengers pause for a photo at the departure gate and in a matter of seconds, our biometric facial comparison service will compare that photo to images the traveler has already provided.

Currently, we have commitments from several airlines and airports to implement secure, touchless biometric boarding and enhance the departure process. To date, we have processed almost 20 million travelers using facial biometrics upon departure from the United States with a match rate above 98 percent.

To complement biometric boarding, we have implemented a similar process at entry at select airports known as Simplified Arrival, an enhanced international arrival process that uses facial biometrics to automate the manual document checks that are already required for admission into the United States. As the severity of the COVID-19 pandemic was becoming clear in the first half of 2020, we recognized the health and safety benefits of a touchless biometric identification service and accelerated the deployment schedule to ensure maximum utilization of Simplified Arrival. As a result, CBP is part of the travel recovery efforts to build passenger confidence in safer travel.

Currently, we have implemented biometric facial comparison technology partially or fully at entry into the United States at 198 airports, including Preclearance locations. As part of our land border innovation efforts and building upon the successful implementation of Simplified Arrival at the airports, we expanded the use of facial biometrics to the pedestrian lanes at U.S. land borders. Currently, Simplified Arrival has been deployed in varying degrees to 78 locations representing 46 Ports of Entry (21 on the Northern Border and 25 on the Southern Border). Each of these locations has a 1:1 biometric facial matching process, in which the traveler's live photo is compared to the document the traveler presents.

This month, we also began a Simplified Arrival pilot in select vehicle lanes at the Anzalduas International Bridge Port of Entry (POE) in Texas for travelers arriving in the United States. As part of this 120-day pilot, we will evaluate the system's ability to capture a quality facial image for each occupant in the vehicle, as well as the accuracy of the biometric matching to inform future biometric enhancements for vehicle entry processing.

In the sea environment, we have deployed biometric facial comparison technology into the debarkation process at eight seaports in the U.S., in partnership with nine cruise lines. In addition, we are expanding our data sharing agreements with cruise partners to enhance security. This effort will provide a more complete analysis of passengers in advance of travel and streamline inspections.

In collaboration with the Transportation Security Administration (TSA), we continue to explore how CBP and TSA can expand the use of facial biometrics in the curb to gate travel experience, leveraging CBP's facial biometric matching service. We have partnered with TSA on several multi-phased operational tests to assess the use of facial biometrics to further secure and enhance travel at the TSA checkpoint.

To date, CBP has processed over 100 million travelers using facial biometrics. Whether air, land, or sea innovation, the use of facial biometrics is secure, efficient, and touchless and enhances the customer experience. Biometric facial comparison technology has been proven to decrease aircraft boarding times. For example, airlines have reported that they have boarded travelers on A380 planes in 20 minutes through the biometric boarding process. Additionally, post-cruise satisfaction surveys by travelers have been exceedingly positive and highlight the ease and efficiency of facial biometrics in the debarkation process.

In addition to streamlining travel, the use of facial biometrics protects the identity of travelers and adds another layer of security. Since September 2018, we have used biometric facial comparison technology to identify over 950 impostors. Recently, CBP officers prevented an impostor from entry at the Laredo, Texas land border port of entry: https://www.cbp.gov/newsroom/local-media-release/laredo-cbp-officers-detect-impostor-through-facial-biometrics

As with the use of any new emerging technology, it's critical that accuracy and privacy concerns are appropriately addressed at the forefront to ensure the public's acceptance and use. At CBP, we use a high-quality facial comparison algorithm, which shows virtually no measurable differential performance in results based on demographic factors. We continually evaluate the performance of this algorithm and have partnered with the National Institute of Standards and Technology (NIST) to further enhance the biometric facial comparison process.

At CBP, we also take our privacy obligations very seriously and are dedicated to protecting the privacy of all travelers. We have published multiple Privacy Impact Assessments (PIA) that explain all aspects of CBP's biometric Entry/Exit program, to include policies and procedures for the collection, storage, analysis, use, dissemination, retention, and/or deletion of data. In addition, the Entry/Exit program includes four primary safeguards to secure passenger data, including encryption during data storage and transfer, irreversible biometric templates, brief retention periods, and secure storage.

Photos of U.S. citizens and select foreign travelers who are not statutorily required to provide biometrics are securely held in CBP systems and deleted within 12 hours. Photos of all other foreign travelers are stored in a secure DHS database. U.S. citizens are welcome to participate in the biometric facial comparison process; however, if they do not wish to do so, they can simply notify a CBP officer who will perform a manual document check. In addition, foreign travelers who prefer not to participate in the biometric boarding process upon departure from the U.S. can also request a manual document check.

In November 2020, we published a Notice of Proposed Rulemaking (NPRM), which proposes to amend CBP's Entry/Exit regulations by eliminating references to pilot programs and the port limitation to permit the collection of photographs or other biometrics from non-U.S. travelers departing from airports, land ports, seaports, or any other authorized point of departure. We have been analyzing all comments received and will respond in the Final Rule, including making any adjustments as necessary.

The September 11th anniversary continues to reinforce the critical importance of the biometric Entry/Exit mission each year, and we are proud of the progress we have made on this security mandate. Although the COVID-19 pandemic has severely impacted international travel in the air, land, and sea environments, there is also a significant opportunity to transform and enhance the future of touchless travel by expanding public-private partnerships and leveraging technology.

Department of Homeland Security, U.S. Customs and Border Protection
Kimberly Weissman
Kimberly.Weissman@cbp.dhs.gov

Technology innovation

30. Vision-Box: How biometrics are improving security, convenience & privacy for travellers in the post-pandemic era

Travel industry on path to recovery

The COVID-19 pandemic has precipitated a global collapse for the travel industry, made worse by a sharp downturn in the air transport sector and its supply chain. For much of the world, the extensive second wave of the coronavirus prevented a hoped-for revival.

Yet there is room for cautious optimism. With the successful distribution and deployment of vaccines by the latter part of this year, travel rates may rise substantially in 2022. In fact, IATA projects a return to 2019 levels by 2024, with the travel industry as a whole regaining strength in the years to come.

Big expectations from health, safety & privacy-conscious travellers

Issues of health, safety, and cleanliness have been brought to the fore by the physical protocols needed to deal with COVID-19 and the transition to its aftermath. People across the globe have become used to the concepts of social distancing, personal protective equipment, and minimal contact with surfaces.

This behaviour is extended to the travel industry. Travellers are increasingly demanding easy-to-use, seamless experiences which put their safety and data privacy at the centre. What's more, they wish to be in control of the personal information that is shared with stakeholders along the traveller journey.

Border agencies and ports and carriers alike need to adapt in this post-COVID world while giving full consideration to health, safety, privacy, and convenience. The key to do so, is through the simplification of processes and flows powered by automation and biometric technology.

How seamless, touchless biometric solutions can meet this demand

Simplification of traveller flows and enhanced experiences aren't new concepts. The demand for them already existed pre-Covid. The key issue is, and was, that of moving people around from A to B, smoothly and safely.

With the pandemic and the rise of the post-Covid traveller, airports, airlines, and border agencies have an increased desire and opportunity to overcome those challenges.

We help our customers provide safe and seamless travel experiences powered by state-of-the-art biometrics combined with a highly scalable identity management platform product which is the core enabler of realizing truly seamless experiences. A collaborative platform of real-time intelligence which is designed to accommodate large volumes of information on travellers' identity, people flow, connected devices and third-party systems, thus streamlining communication between all travel stakeholders.

Travellers are therefore winners as they benefit from better and safer user experiences and convenience while keeping control over their data privacy.

Furthermore, through touchless biometric technology, transmission of pathogens at airports can be mitigated. These solutions offer airports hygienic advantages through security, border control, and boarding. This is achieved by enrolling travel documents and facial images at airport check-in, or remotely using digital mobile ID apps.

As an example, our mobile identification software development kit allows various stakeholders to easily access different types of biometric services through an API integration, all tied to the biometric and biographic information provided by the traveller.

Our approach has equipped AirAsia with a Mobile ID SDK to capture high-quality facial recognition data, allowing them to verify users' documents quickly and accurately through e-passport and border technology. Our collaboration with AirAsia enabled the delivery of F.A.C.E.S (Fast Airport Clearance Experience System) – a touchless identification and contactless clearance platform designed for mobile check-in to enhance the guest experience at the airport, improve customer brand loyalty, and be an integral part of AirAsia's overall digital transformation.

Border Control Agencies also benefit from our approach. For Europe's first Smart Borders implementation at Helsinki Airport, we developed an avatar-based technology that interacts with the traveller and mimics their movements through an ABC eGate. With diversity and inclusion in mind, the customised avatar was a modified version of the Finnish Border Guard teddy bear emblem – which also contributes to a child-centred experience in one of the few countries that allows children to go through gates. There is no need for passengers to physically interact with human operators. Crucially, touchless biometric technology also helps border agencies process the growing number of international passengers, without expanding the physical footprint of immigration halls.

Moving forward into the digital transformation

For the travel ecosystem, the path to market recovery is characterised by an urgent need to focus on digital, seamless, and contactless traveller-centric innovation. The catalysts for that innovation to come about are multi-stakeholder collaboration, trusted identity data exchanges, interoperability, and privacy. We are uniquely positioned to enable all travel stakeholders on their path to recovery and well beyond with our expertise and solutions that guarantee effective communication and interaction and enable positive impacts on traveller flow optimisation. Travellers benefit from increased safety and privacy while using their biometric identity to simplify their lives.

Vision-Box
Paulo Godinho
Head of Marketing & Communications
paulo.godinho@vision-box.com

31. WorldReach, an Entrust company: Biometrics for the people: In defence of the responsible use of emerging identity technologies

On the 20-year birthday of the Biometrics Institute, we at Entrust are proud to be active members, joining with industry partners to promote the responsible use of biometrics for the public good. We believe that, with proper legal safeguards, whether we're accessing services at home or crossing international borders, biometrics will continue to improve all our lives as citizens.

A new paradigm

We are in the early stages of a new paradigm in the way citizen-consumers communicate with government and commercial service providers. Public expectations are shifting towards digital services and away from waiting rooms, paper forms, and valuable documents sent through the mail.

These changes are in part the result of rapid improvements in biometric technologies. For example, according to the Centre for Strategic and International Studies, "Facial recognition has improved dramatically in only a few years. As of April 2020, the best face identification algorithm has an error rate of just 0.08% compared to 4.1% for the leading algorithm in 2014, according to tests by the National Institute of Standards and Technology (NIST)[9]."

Public understanding of biometrics

The view taken by many across the industry is that facial recognition technology (FRT) has recently reached or surpassed the accuracy of other biometric modes such as fingerprints and iris, and that all these options are significantly better at identifying individuals than is the naked eye[10].

Despite this, biometrics generally - and FRT, in particular - have often taken a beating from the press, politicians and some academics. A notable example is the 2020 *New York Times* piece on the social media scraping activities of Clearview AI[11], now facing several lawsuits, and the anti-biometric campaign waged by the Toronto *Globe and Mail*[12]. Moreover, some municipalities, including San Francisco, have banned the use of FRT for some purposes[13].
Much of this critique is legitimate and well intentioned. It is arguable that technology is moving faster than legislation, leading to concerns about overreach, particularly in law enforcement use cases. But the critique is often guilty of conflating separate issues and oversimplifying issues on which the public would benefit from a more nuanced understanding. Here are two examples.

Much of the animus directed at FRT is focused on just one use case: police surveillance. Press articles often use 'facial recognition' and 'surveillance' interchangeably, never taking the trouble to distinguish between one-to-one, one-to-few and one-to-many use cases, or to explain the differences between face detection, face recognition and face verification. The evidence given by Chuck Romine of NIST to the US House Committee on Oversight and Reform in January 2020 is an object lesson in how to do so in a way that's easily understood.[14]

Secondly, concerns about the sometimes-differing performance of FRT across demographic groups have led to misleading headlines about 'bias', giving the impression that the makers or users of such technologies have racist or sexist intentions, without giving the whole story about the issues and how the industry is tackling them. That story is told in its most complete form in the 2019 NIST report on demographic effects.[15]

[9] https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter
[10] https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/
[11] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
[12] https://www.theglobeandmail.com/opinion/article-what-happens-when-our-faces-become-data/
[13] https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html
[14] https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0
[15] https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects

One of NIST's key conclusions was that the most accurate facial algorithms in fact show very little by way of differing accuracy across demographic groups. Another notable conclusion is that algorithms are only as good as the data sets on which they have been trained. Given the huge diversity of the real world, the most accurate algorithms are those which have been developed on the most diverse data sets.[16]

A good news story

Those of us in the identity industry are not naïve about the challenges ahead on the public acceptance of biometrics, but we often wish the good news about improvements to the lives of ordinary people was as prominent as the controversies about surveillance.

Here's one example that's close to the hearts of those of us in the Identity Verification team at Entrust. Following the UK's 2016 decision to the leave the EU, the Home Office was faced with a significant challenge: how to identify and register several million EU nationals living and working in the UK under freedom of movement provisions, in order to grant them a new settled status in UK law.

Since 2018, we have worked with the Home Office on the innovative EU Settlement Scheme, which allowed applicants for the new status to apply entirely remotely (if they chose to do so), augmenting the online application with an identity verification process performed on a smartphone in just a few minutes. This process uses market-leading facial matching and liveness capabilities (as well as an NFC document check) to confirm that the applicant is a real person and the owner of a genuine passport. This powerful data packet allows the Home Office to grant permanent settlement in the UK, without seeing applicants in person or receiving their passports in the mail, in most cases.

By the time the scheme came to an end in June 2021, more than 6 million people had applied, the overwhelming majority choosing to identify themselves through the digital route. According to Home Office figures, at the time of writing almost 5.5 million of those applicants have been granted settled status in the UK.[17]

Here is just one example of biometric technologies making life better. There is no surveillance in play here, and no agency overreach. Facial matching was used only on a one-to-one basis (to link the person securely to their own passport), the digital route was entirely voluntary, and the scheme adhered to both GDPR and UK government requirements for the handling of personal data, none of which is retained by Entrust.
The scheme was so successful that this approach to remote applicant identification is now being rolled out across several other UK immigration programs.

A way forward

Concerns about the responsible use of biometrics are well-founded. This is precisely why Biometrics Institute membership includes lawyers, privacy advocates and academics as well as technology providers.
But we need to elevate the public debate by accurately capturing different use cases and appropriate legal responses.

We at Entrust firmly believe that, when used responsibly, in ways that enhance individual privacy - whether we're traveling seamlessly across borders or securely accessing digital services - biometric technologies will continue to improve lives.

Entrust
Jon Payne, Director Strategic Alliances, Identity Verification
+1 703 883 7022
Jon.payne@entrust.com

[16] https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms
[17] https://www.gov.uk/government/collections/eu-settlement-scheme-statistics

32. Board of Directors and Expert Groups

Andrew	Rice	Department of Home Affairs, Australia	Chairman 2015
Darren	Bark	NSW Police Force	Deputy Chairman 2021
George	Rodrigues	Department of Internal Affairs, New Zealand	
Paul	Cross	SITA, Australia	
Dan	Bachenheimer	Accenture, USA	
Hans	De Moel	Ministry of Justice, the Netherlands	
Jakob	Glynstrup	Danish National ID Centre	
Stephanie	Schuckers	Center of Identification Technology Research (CITeR), USA	
Jonathon	Thorpe	Digital Transformation Agency, Australia	

Past Directors and Chairpeople

Name		Member organisation at the time of service	
Ted	Dunstone	Biometix	Chairman 2001
Geoff	Poulton	CSIRO Australia	Chairman 2002
Alistair	Tegart	Standards Australia	Chairman 2004
John	Secker	NZ Customs	Chairman 2005
Paul	Kirkbride	Australian Federal Police	Chairman 2009
Arron	Baker	Ministry of Business, Innovation and Employment New Zealand	Deputy Chairman 2012 and Chairman from 2013
Kevin	Darch	QLD Police, Australia	Deputy Chairman 2013
Roger	Baldwin	Metropolitan Police Service, UK	Deputy Chairman 2014
James A.	Loudermilk II	FBI	Deputy Chairman 2015
Andy	Foote	Wells Fargo Bank, USA	Deputy Chairman 2018
Raoul	Cooper	British Airways	Deputy Chairman 2020
John	Peacock	NFP Analysts, Australia	
Bruce	Lyman	Argus Solutions, Australia	
Trevor	Long	Qantas, Australia	
Terry	Hartmann	Unisys Australia	
Ian	Miller	Australian Federal Police	
Peter	Mottram	Australian Passport Office	
David	Philp	Department of Internal Affairs, New Zealand	
Tony	Burke	Australian Bankers' Association	
David	Lang	CrimTrac Agency, Australia	
Phillip	Youngman	Roads and Traffic Authority NSW, Australia	
Carlene	York	NSW Police Force, Australia	
Gregory	Henwood	UK Ministry of Justice	
Karen	Shirley	Australian Federal Police	
Cyril	Dujardin	Morpho, Australia	
Caroline	Hubbard	Department of Internal Affairs, New Zealand	
Leanne	Stevenson	Australia Post	
John	Kendall	Unisys Australia	
Charles	Ronaldson	Department of Internal Affairs, New Zealand	
Glen	Wimbury	UK Border Force	

Mandy	Smith	Kiwibank New Zealand
Juergen	Pampus	Cognitec Systems, Germany
Brett	Feldon	Salmat, Australia
Adam	Hergert	ANZ Bank, Australia
Richard	Agostinelli	Crossmatch, USA
Santiago	Uriel Arias	CECA Bank, Spain
Samantha	Hannah-Rankin	Department of Premier and Cabinet (VIC), Australia
Johanna	Morley	Metropolitan Police Service, UK
Art	Stewart	IDEX, USA
Tori	Lamb	Services Australia
Jill	Fitzroy	VicRoads, Australia
Mick	O'Connell	Interpol
Jason	Holmes	Heathrow Airport
Quek Sin	Kwok	GovTech Singapore

Expert Groups

Technical Committee: established November 2003 and merged into other groups

Privacy Expert Group (PEG): November 2007

Biometrics Vulnerability Assessment Expert Group (BVAEG, renamed BSIEG): October 2010

Borders User Group (BUG): July 2015

Advisory Council: November 2015

Academic Research and Innovation Group (ARIG): July 2017

Digital Identity Group (DIG): September 2016

Future Direction Group (FDG): June 2020

33. Testimonials

From humble beginnings in 2001, the Biometrics Institute has developed into a key global forum for the exchange of information relating to biometrics. Starting with a reputation for providing quality events that bring thought leaders and practitioners together, the Institute has moved also to being a policy and procedural leader for governments, private sector and community organisations seeking to use biometrics to meet a range of their business and day-to-day activities. These days, the Institute is positioned on the global stage, its members representing all regions of the world and its Board reflecting the shared engagement of governments, business and academia in furthering the responsible and ethical use of biometrics. For those of us working in organisations that use biometrics, it is been a great help over the years when faced with a business challenge to be able to reach into the Institute and find peers across the world faced with similar challenges and able to offer ideas for their solution. The next 20 years promises to be as successful.

Andrew Rice, Chairman & Director, Biometrics Institute and Regional Director, Pacific, Australian Department of Home Affairs

I have a strong commitment to sharing best practice usage and knowledge of biometrics technology to ensure its responsible and ethical use. The Biometrics Institute is the pre-eminent international forum which brings together users, suppliers, regulators, privacy experts and academics in the biometrics field. This melting pot of experts is a critical forum to ensure that biometrics are harnessed ethically and are used to benefit all, particularly minorities and vulnerable cohorts.

Having seen the benefits of biometric technology in the law enforcement, Justice, and community sectors, it is critical that forums such as the Biometrics Institute lead and guide biometric usage and implementation - something the Institute has been doing successfully for two decades.

The Institute continues to benefit the global community by driving critical thought and development in biometrics technology, particularly in privacy and policy, digital identity, security and integrity and research and innovation.

With such exciting developments, the Institute continues to be the most effective platform, with global reach, to further my social responsibility, and our social contract to foster-ethical innovation.

My vision is for the Biometrics Institute to continue to be the trusted voice on biometrics, especially in the setting of global standards and best practice. This will ensure better and more coordinated integration between industry and Government to enable more consistent application of responsible biometric principles.

Darren Bark, Deputy Chairman & Director, Biometrics Institute and Chief Executive Officer, NSW Jewish Board of Deputies, Australia

APO is proud to be a founding member of the Biometrics Institute. We have benefitted immensely from the Institute's insights, and the close working relationships it has helped us forge with key agencies in the biometrics field. We want to acknowledge the Biometrics Institute's tremendous contributions over the past 20 years and congratulate it on reaching this important anniversary. The APO looks forward to working closely with you for the next 20 years!

Australian Passport Office

I have been a member of the Biometrics Institute for 3 years and have had the opportunity to engage with other members on our joint mission to promote the responsible and ethical use of biometrics through thought-leadership and good-practice guidance.

The Institute brings together expertise from across the globe which has been extremely beneficial for the Australian Government's Digital Identity program. Sharing lessons around policy and application for various use cases helps us inform the implementation of biometrics in a local context as we deliver better experiences for Australians and businesses.

The Biometrics Institute offers valuable resources to anyone with an interest in biometrics as we continue to navigate new technologies and approaches to improve customer experience.

Jonathon Thorpe, Director, Biometrics Institute and General Manager Whole of Government Governance and Sourcing Division, Australian Digital Transformation Agency (DTA)

The Institute has enabled its members to have knowledge and understanding of biometrics to feel comfortable and more confident about adopting biometrics. As a result, I believe, the Institute has been a catalyst for allowing the industry to grow responsibly. When we started the Institute in 2001, biometrics was still very niche. It was in some passports and some people had seen it in movies, but most people had no idea that it wasn't science fiction.

Now, 20 years later, it's everywhere: on our phones, used in government services and it would be fair to say that a good percentage of the world's population has encountered biometrics in one form or another. The Institute has been there for much of that journey, in all sorts of ways, working with development agencies like the UN agencies and law enforcement as well as big corporates and social media.
Isabelle Moeller, Chief Executive, Biometrics Institute

The Institute has provided the one place to meet and if you're new to biometrics you could connect with a knowledgeable community where you could learn from others and receive information. You are not alone. There are so many amazing and passionate people that I have worked with at the Institute starting with the various Board Directors and Committee Members but also the membership overall who attended so many of our events. We have built these amazing foundations, and the Institute has accomplished so much in its 20 years. But in reality, I believe we are only just at the beginning of this journey with the significant transformations that biometrics and identity are bringing to the world. To date biometrics has been a largely unregulated space and that is changing as it is becoming much more mainstream. New legal frameworks are being discussed, biometric commissioners are being setup and the EU GDPR and other legislation that addresses biometrics introduced. The value of a place like the Institute can be to assist those who write these new rules to get them right, wherever they are in the world. Evenif onecountry gets it wrong itcancreate huge problems. The Institute canhelp these changes by providin g the guidance and information to those regulators writing the regulation to ensure that biometrics will be used responsibly and ethically.
Ted Dunstone, Founder, Biometrics Institute and Head, Biometrics Institute Security and Integrity Expert Group and Managing Director, Biometix

I would posit that the approach to biometrics delivery and oversight for policing and criminal justice purposes in Scotland safeguards our biometric future by following the 'Three Laws of Biometrics' advocated by the Biometrics Institute. In jurisdictions where the use of biometric technologies has proved more controversial, these rules have sometimes been overlooked, and technology has not been adequately guided by policy and process.
Brian Plastow, Scottish Biometrics Commissioner

The Institute plays a remarkable and invaluable role facilitating the ethical development and use of biometrics – not as an end in itself, but as a means to better public policy and industry outcomes. I'm proud that my organisation, as a founding member, has contributed to the Institute's work from the outset.
Stephen Gee, Australian Passport Office

On the 20-year birthday of the Biometrics Institute, we at Entrust are proud to be active members, joining with industry partners to promote the responsible use of biometrics for the public good. We believe that, with proper legal safeguards, whether we're accessing services at home or crossing international borders, biometrics will continue to improve all our lives as citizens.
Jon Payne, Director Strategic Alliances, Identity Verification, Entrust

Biometric applications are neither value-free nor neutral in their impact. The challenge in refining the biometrics eco-system therefore lies with harnessing a deeper appreciation of the way in which biometric applications benefit society. Working together with policymakers and society in creating a digital society is therefore essential. The Biometrics Institute community has considered not just who provides the biometric but crucially who has access to it and for what purpose precisely. Meeting that challenge is as valid today as 20 years ago.
Juliet Lodge, Member of the Privacy Expert Group, Biometrics Institute

From humble beginnings in Sydney Australia, the Institute has grown with the industry and become multinational, finally basing itself in London but retaining its office in Sydney. It has been one of the great unsung stories of the modern IT era and we look forward to many more years and more organisations realising that fact and taking advantage of all that the Institute offers.
Terry Aulich, Head of the Privacy Expert Group, Biometrics Institute

In the light of recent developments, the biometrics industry now stands at something of a crossroads. It can continue to develop and test products on what is a captive population in schools, with minimal attention paid to the social consequences of their long-term use. Alternatively, it can decide to involve stakeholders much more closely in the development of products, through collaborative development approaches that involve significantly less commercial

secrecy, so proper scrutiny can take place, and products can be revised and adapted as appropriate. By stakeholders, this should mean pupils, teachers and parents, rather than finance departments or senior management teams who might be involved in high-level procurement. There also need to be more extensive training populations, in order to take into account diverse cultural and racial backgrounds, as well as any special educational needs. This builds on the Biometrics Institute's policy of appropriate use, providing for an ethical approach to technological tools which are having increasingly profound social consequences.

Sandra Leaton Gray, Member of the Privacy Expert Group, Biometrics Institute and UCL Institute of Education

One of the best forums we were able to be a part of was the Biometrics Institute. As the Institute turns 20 years old this year it reminds me of how critical it was for us to reach out internationally. Being a member of the Biometrics Institute gave us access to like-minded governments, technology companies, scientists and academics and discussion groups that gave us a platform to explain to the world what biometrics did to improve the security of the United States.

US-VISIT is now the Office of Biometrics and Identity Management (OBIM) and its senior leaders and many of the professional women and men of OBIM are active members of the Biometrics Institute. As the use of biometrics continues to evolve and new modalities and technologies are created it is my hope that the Biometrics Institute will also evolve and grow the services it offers to its members. From its association with the United Nations to the publication of the Three Laws of Biometrics and the Good Practice Framework I suspect that 20 years from now there will be someone in the biometrics field today or in the future who will want to offer a similar tribute to the Biometrics Institute.

Robert A. Mocny, Former Director of the United States Visitor and Immigrant Status Indicator Technology Program (Retired) and Member of the Advisory Council, Biometrics Institute

For 20 years the Institute has provided access to global expertise on biometrics from the technical, academic, privacy and user perspectives, as well as unparalleled networking opportunities for professionals who are involved with this technology.

It's important to acknowledge the value we all get from the Expert and Sector Groups that the Institute maintains. Much of that value is hard to quantify. These groups produce papers and products for members that explain important concepts and that help us to maximise the benefits and manage the risks that accompany use of this technology. They are also invaluable information sharing opportunities, where members with similar interests get to talk about their challenges and their successes, and inevitably, members continue to interact offline to focus further on areas of common interest.

Paul Cross, Director, Biometrics Institute and Head of Border Management Sydney Practice, SITA

The Institute has done a remarkable job in providing thought leadership as to the effective, responsible use of biometrics to solve real world problems. Its content-rich events and communications have fostered an open and constructive dialogue among users and suppliers which has helped usher biometrics into the mainstream as an effective component of mission-critical security systems.

Rich Agostinelli, Member of the Advisory Council, Biometrics Institute

I have been impressed by the way that the Biometrics Institute has grown from an Australia-based organisation to extend to the European continent, North America and elsewhere and has established itself as an influential body advising such organisations as the UN. I very much support the principal focus on promoting the responsible use of biometric recognition rather than on the technology itself. This is vital for the protection of the users and for public acceptance. Awareness of some of the concerns has been highlighted in recent work by NIST and is also being reflected in current and developing international standards on biometric information protection, application security and security evaluation, privacy, and demographic bias.

Philip Statham, Biometrics Consultant

The establishment of the Biometrics Institute twenty years ago reflected a broader need to understand a world in which digital technology was playing an increasingly influential role in daily life. At about the same time in 2003, the International Civil Aviation Organization (ICAO) adopted specifications for electronic machine-readable travel documents (eMRTD or ePassport) that are digitally-enhanced documents that contain an embedded chip, which holds both biographic information and a photo. The ICAO guidance material and specifications found in Doc. 9303 laid the foundation on which an extensive system of infrastructure could build. Beginning with Belgium in 2004, successive governments began issuing ICAO-compliant ePassports. By 2013, over 100 countries issued ePassports

and nearly 400 million were in circulation worldwide.[18] As of 2020, 145 countries issue ePassports and there are roughly 1 billion in circulation.
Implementation Capacity Building Working Group (ICBWG), International Civil Aviation Organisation

Alongside diligently managing the risks, UNHCR will continue to explore how the responsible and ethical use of biometrics can improve the way it serves and benefits the lives of the people it seeks to protect. UNHCR holds 'International Observer' status with the Biometrics Institute and has contributed to a number of Institute events and products over its history, including the recent Good Practice Framework.
UNHCR The UN Refugee Agency

With the growing potential for biometrics, independent organisations such as the Biometrics Institute were essential in the process - connecting all stakeholders and providing a platform to exchange innovative ideas as well as concerns.
Georg Hasse, Head of International Sales, Secunet Security Networks AG

We should all be very proud with the Institute acting as a guardian for ethical use. It has played a significant part in forcing evolution through institutes like NIST and ISO to better functionality, performance, reduce bias, and create privacy by design – all leading to developing trust and confidence for the user community, framed with the beginnings of sensible policy frameworks.
Michael O'Connell, Member of the Advisory Council, Biometrics Institute and Managing Director, Critical Insights Consultancy Ltd

It is interesting to reflect over the last twenty years. I have been involved in liveness detection research and testing since 1998, writing one of the first academic papers in the area. At that time, many folks claimed that spoofing was not a problem and/or their systems were not vulnerable. I was told by a senior academic colleague that it was a "perception problem," which I took to mean, not an area of serious academic pursuit. However, the Biometrics Institute did take biometric vulnerabilities seriously, forming the Biometrics Vulnerability Assessment Expert Group (BVAEG) which started in 2010. There I met a small group of individuals who were committed to identifying and mitigating vulnerabilities and sharing best practices amongst ourselves, as well as the larger biometric community. I am happy to report that the landscape is a completely different story today. ISO has published standards on liveness, now called presentation attack detection (PAD), and multiple organizations have certification programs. Industry is actively competing on PAD performance and pursuing independent assessment and certification. Now there are many experts around the world who are continuing to move the field forward in a cat and mouse game with attackers, and this community is supported by the Biometrics Institute as well as many other organizations.
Stephanie Schuckers, Director, Biometrics Institute and Director, Center of Identification Technology Research (CITeR)

34. Timeline

2001	
8 June	The Australian Government awarded funding for the setup of the *Australian Biometric Testing Organisation,* which was renamed *Biometrics Institute Ltd*
11 September	Terrorist attacks in the US (9/11)
11 October	Biometrics Institute Ltd was officially established as a not-for-profit membership organisation in Australia
29 October	First Biometrics Institute *Supplier Briefing* held in Sydney
November	First Biometrics Institute *Government Briefing* held in Canberra
2002	
30 March	First *Biometrics Institute Conference* held in Sydney followed by two Member Meetings in August and November
10 May	Isabelle Moeller appointed as first employee of the Biometrics Institute
	20 members - Australia
2003	
February	The Biometrics Institute *Privacy Code* development was commissioned by the Australian Government
August	Recruitment of a Member Services Officer. Biometrics Institute has two staff
November	*Technical Committee* established
2004	
4 May	*Draft Privacy Code* submitted to Office of Federal Privacy Commissioner in Australia
	61 members - Australia, NZ, UK, USA, Germany
1 October	First *New Zealand Conference*
2005	
6 October	First *Showcase and Exhibition* in Canberra
2006	
2006	100 members
27 July	Privacy Code approved by the Australian Privacy Commissioner and came into operation in September 2006
December	Received funding from the Australian Government for a first *Biometric Vulnerability Assessment Project (Face)*. The project commenced in Feb 2007 and was completed on 31 Oct 2007
2007	
July	Biometrics Institute successfully completed a first Privacy Impact Assessment for Australian Health Management.
November	*Privacy Expert* Group (PEG) established
2008	
January	Received funding from the Australian Government for a second *Biometrics Vulnerability Assessment Project (Fingerprint and Voice)*. The project commenced in Feb 2008 and was completed in July 2009
Sept – Nov	Biometrics Institute successfully conducted a Privacy Impact Assessment for the NZ Department of Labour - Immigration
November	Biometrics Institute is a finalist for the Australian Privacy Awards for its work on the Privacy Code
2009	
November	The 4-day *Intensive Course: Applying Biometrics* was held for the first time in Canberra
2010	
May	Released *Privacy Awareness Checklist* to guide members on good privacy practice

May	Launched the Annual Industry Survey
May	Confirmed further funding from the Australian Government to extend the *Biometrics Vulnerability Assessment Framework* to include iris biometrics
June	Released an Information Sheet *Using Biometrics in Licensed Premises and Clubs – Are you protecting your patrons privacy and reducing risk of litigation?*
October	Established the *Biometric Vulnerability Assessment Expert Group (BVAEG)* with participation from the Biometrics Institute, UK Biometrics Working Group and German Federal Ministry of Information Security to focus on raising awareness about the importance of vulnerability assessments and that mitigation is available and help to develop standards
2011	
2011	Trademarked the Biometrics Institute logo in Australia and internationally
July	Opened office in London, UK
July	Inaugural Meeting held in Singapore attracting 50 delegates
October	Launch Reception held in London, UK, hosted by the Australian High Commission, attracting over 100 delegates
November	Biometrics Institute 10-year Anniversary Gala Dinner in Canberra
December	De-registered the *Privacy Code* in Australia and launched the Biometrics Institute Privacy Guidelines
2012	
27 June	First UK Conference
2013	
April	First *Biometric Vulnerability Assessment Workshop* held in London
	130 members
September	Apple launched first iPhone (5S) with biometric security – a fingerprint sensor
7 October	First *ID@Borders Conference* in Brussels
November	Received a first of nine Australian Government Export Market Development Grant
2014	
February	First *Introduction to Biometrics Short-course* held in London
March	Inaugural Reception in the USA, hosted by the Embassy of Australia in Washington DC, receiving record delegate registrations (100+)
October	Partnered with Elsevier for the first time to run the *Biometrics 2014* show in London, UK
2015	
Early 2015	Commenced work on proposed *Privacy Trust Mark* in close consultation with members and decided that it was very challenging to create certification around privacy
30 June	178 members
July	*Borders User Group (BUG)* established connecting over 15 border management agencies from across the globe
September	Supported the Canberra Institute of Technology in the development of a free Massive Open Online Course on biometric technologies
September	Developed the *Top 10 Vulnerability Questions Paper* and *Vulnerability Checklist*
November	*Advisory Council* established with Group Heads and former office holders advising the Board on strategy
2016	
28 January	Released *Privacy Guidelines Update* on World Privacy Day with the support of the *Privacy Expert Group*
May	First *Facial Recognition Performance Workshop* held with NIST
30 June	202 members
July	Established the *Digital Identity Group (DIG)*

September	Briefing to UK Parliament facilitated by Conservative Party Technical Forum
October	*BVAEG* developed and released a *How to address Biometric Vulnerabilities – a Baseline Assessment Guide*
11 October	15-year anniversary. 213 members
2017	
28 March	First *US Biometrics Institute Conference* held in Washington DC, USA
June	Reached over 5,000 followers on Twitter
30-Jun	222 members
July 2017	*Academic Research and Innovation Group* established to connect academic world with the user community
August	Released a series of *Viewpoint Papers on Border Management, Digital Identity and Biometric Vulnerabilities*
September	Biometrics Institute and International Organisation for Migration sign a Memorandum of Understanding to promote the responsible use of biometrics in response to challenges around security, safe transport for migrants and refugees and international cross border mobility
October	Chief Executive, Isabelle Moeller, wins the *Women in Biometrics Award*
1-2 November	First independent *Biometrics Institute Congress* held in London
30-Nov	First activity in South Africa "Introduction to Biometrics" event
2018	
June	United Nations released the *Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter Terrorism* with the Biometrics Institute at the UN Headquarters in New York City.
June	Recruited a Chief Operating Officer
2019	
February	Recruited a Communications Adviser. Biometrics Institute has a team of ten based in Sydney, Australia and London, UK
March	Launched *Ethical Principles for Biometrics* with a call to action for adoption
April	Partnered with Organization for Security and Co-operation in Europe at Biometrics Institute's *ID@Borders & Future Travel Conference* held in Vienna at the Hofburg
June	*Future Direction Group* established to monitor trends and the state of biometrics.
October	First *State of Biometrics Report* released with support of *the Future Direction Group*
2020	
March	COVID-19 declared a pandemic by WHO (World Health Organisation)
April	*Biometrics and Hygiene Paper* released
May	*COVID-19 Supplier Response Report* released
June	*Good Practice Framework* released
October	First online *Biometrics Institute Congress* followed by a series of online events
2021	
March	*Should We Ban Facial Recognition Viewpoint Paper* released
March	*Digital Onboarding and Biometrics Guiding Paper* released with the support of the *Digital Identity Group*
May	*Privacy Guidelines Update* released
June	Presentation to the 2nd UN High-level Conference on Counter-Terrorism
11 October	Biometrics Institute 20-year anniversary