# Just because we can, should we?

With a mission to promote the responsible and ethical use of biometrics, *Isabelle Moeller*, Chief Executive of the Biometrics Institute, questions whether the industry is waiting for one main player to discover how to manage biometrics at the border, and offers advice on how to get there quicker.

BIOMETRICS have changed the face of air travel. With passenger traffic expected to double in the next 20 years and existing infrastructure and resources being tested to their limits, the industry has high hopes for what biometrics can do for them. However, with the exponential growth of new biometric technology coupled with global terrorism challenges and privacy rising up the public agenda, it's never been more important for the industry to come together in order to move forward responsibly.

Biometric technology has the potential to play a big role in easing the pressures all stakeholders in the aviation industry face. Biometrics give airports the chance to accurately verify and move passengers more quickly through limited spaces. The potential of biometrics to calm pressure points of security and border control; maximising time spent in restaurants and shops, is very attractive.

Technology offers the opportunities to transition to an account-based model – rather than a transactional one. Greeting customers by name and automatically implementing preferences will generate satisfaction and loyalty. Authorities can feel secure knowing they are keeping everyone safe, with robust systems and positive IDs on who is entering and exiting. The passenger will find the end-to-end journey smoother and will be more likely to want to do it again.

## The wild west

Airlines tell us they need standardisation on how to connect all the components they need to make the seamless traveller vision work – standards and hardware for e-gates, kiosks and cameras (provided by one of five or six providers) – with their departure control and partner IT systems. One of our members described the current picture as the "wild west" when it comes to bringing together and understanding all the different considerations for a biometric process in the absence of common standards, changing community perceptions and adequate guidance.

U.S. Customs and Border Protection services now make the ID process slightly easier for airlines. Operating in the U.S., airlines and airports can send captured biometrics directly to the government for a thorough biometric identity verification against trusted information sources. The U.S. model takes the responsibility, and risk, of validating the passenger trying to board a flight to the required degree.

Airports who manage their own methods of identity verification take on the risk and consequences of getting it right. Border officers need to balance their responsibilities under the 2017 UN resolution 2396 mandate to share data to detect foreign terrorist fighters, with their responsibilities under privacy legislation.

## Biometrics in counter terrorism

Since 2017, all UN member states have been required to collect biometric data to combat terrorism. The Biometrics Institute was asked by the United Nations to collaborate on a compendium for recommended practices in the responsible use and sharing of biometric data in counter terrorism. Recently, we've been working with the UN to promote this compendium and raise awareness of its practical use to member states.

Governments have a big role to play in this changing landscape. There is huge potential for countries to cooperate with each other to create a safer world, using biometrics. One country's departure gate becomes another country's arrival gate. Biometric data can be checked against watchlists to enable countries to better manage risks away from their borders.

However, while many governments find it difficult to share information amongst their own agencies, sharing with others, including the private sector, is another challenge.

## Confidence and consent

SITA's 2019 passenger survey revealed the number of passengers opting for automated passport control has more than doubled, from 21 per cent in 2017 to 44 per cent in 2018. Overall, passengers using self service technology were found to be more satisfied with the self-service option at critical stages of the journey compared to those who weren't able to access self service.

But we know public confidence in companies who ask for and store their data has been damaged in the last few years. As far as facial recognition is concerned, every day seems to bring a new headline that creates confusion. People are no longer blindly welcoming of new technology: More effort now needs to be put into earning their trust. A tweet from traveller MacKenzie Fegan in April received 4,500 shares when she questioned whether she ever gave consent for facial recognition to be used on a flight out of the U.S. Fear, uncertainty and doubt over mass surveillance and the impact of the possible uses of that data will get in the way of progress if allowed to take root. People are uncomfortable sharing their most personal information if they are not advised about what it is being used for and how long it will be stored.

Awareness of privacy requirements has improved since the introduction of GDPR,

*Isabelle Moeller*, Chief Executive, Biometrics Institute, has been at the helm of the Biometrics Institute for 17 years. In that time the organisation has grown into the most respected independent, multi-stakeholder forum for the biometrics community in the world.

although some countries do not yet meet the new bar set by the regulation. It will probably not be a universal model until penalties become real and a business-challenging part of the landscape – and customers voting with their wallets – for all stakeholders to take the issue seriously. Achieving the right balance between convenience, security and privacy is an ongoing challenge but not an insurmountable one. We have released a range of good ▶

It must be remembered that people will be uncomfortable sharing their personal information if they are not told what it is being used for – or by whom

So long as privacy challenges are managed appropriately, biometrics have a role in achieving the seamless customer journey in an airport

*"If a competitor implements different technology to yours which halves the time it takes to board passengers, where might that leave you?"*

practice guidelines to help organisations assess and implement a responsible and ethical use of biometrics, which we are urging anyone operating in this space to consult. These include our updated privacy guidelines which we believe are the most comprehensive, universal privacy guidelines anywhere in the world. This year's upgrade fills in the gaps often left by GDPR and will help organisations – no matter which field of biometrics they operate in – to develop good practice in collecting, storing and processing data.

Transparency surrounding trials and their results as well as the collection, use, storage and processing of biometric data is essential. This needs to happen before implementation, not after.

Gaining and retaining public confidence, if the algorithms of a biometric gate struggle with diversity, will be hard. The onus is on providers to make this work so no one is disadvantaged by the technology – defying its very purpose.

As we have already seen, if technology is applied without properly addressing potential flaws, then regulators may opt to restrict usage until they, and the industry, can ensure proper privacy protections.

### Is the future biometric?

Biometric technology is not the silver bullet. Even with the rapid performance enhancements we've seen recently, the focus now must be on re-shaping policies and processes to allow technology to be an enabler.

So long as privacy challenges are managed appropriately, biometrics have a role in achieving the seamless customer journey. By consenting to the use of biometrics on their end-to-end journey, passengers can be identified by different biometric sensors at several touch points through the airport. Their personalised departure details could be displayed on screens as they approach. Passengers with reduced mobility could be guided to their gates on automated wheelchairs without the hassle of waiting for airport staff to push them. Airlines could reduce delays by knowing where passengers are, if they will be on time for their flight or if their luggage needs unloading.

However, we must be mindful to not forget those challenges and throw the looming Entry/Exit System deadline and the work Brexit will bring to European borders into the mix.

More ethical and robust privacy practices will lead to greater customer buy in, allowing airlines and airports to get to know their customers better – and provide them with a better service.

The advance of biometrics can be a high risk space. As a competitor implements different technology to yours which halves the time it takes to board passengers, where might that leave you? Pay attention – change is happening now.

We know there are lots of conversations waiting to happen and the industry needs to tackle them together. Where do privacy impact assessments need to be carried out? What kind of legislation would help? Once concepts are accepted, answers can be found. ∎

The Biometrics Institute is an impartial, international forum where these conversations take place with some of the key privacy advocates, vendors, academics and governments from around the world. Following a debate with Microsoft in June about the ethical use of biometrics, the conversation will continue with a multi-stakeholder community at the Biometrics Institute Congress in London in October.

### BIOMETRICS WEEK 2019 – INCLUDING THE BIOMETRICS INSTITUTE CONGRESS

- 28-31 October 2019
- More than 40 speakers
- Up to 300 international delegates
- **biometricsinstitute.org/event/ biometrics-congress-2019/**