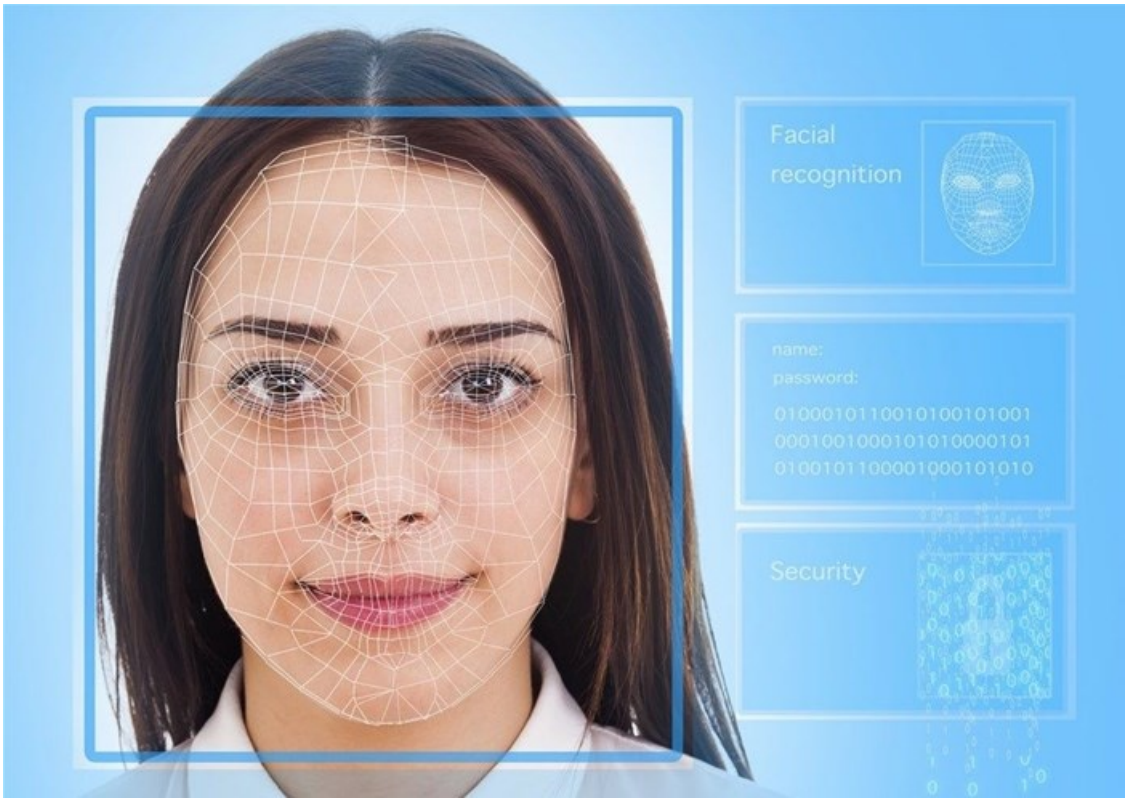
BIZCOMMUNITY

Clearing the air around facial recognition in travel

By Thierry Mesnard

1 Feb 2019

Biometrics are already a fact of life in today's travel, but there are concerns about privacy issues. We need to separate fact from fiction.



By now it’s impossible to ignore the biometric solutions cropping up in airports around the world and the technology will be piloted at Cape Town International from March 2019, with further pilots down the line at King Shaka and OR Tambo.

It’s not difficult to see why, either: at a baseline, biometrics holds significant promise to enhance security, speed up and smooth out friction in the air travel experience. But along with these benefits comes the perceived risk of privacy compromise for the individual. These concerns are valid, but it is necessary to separate fact from fiction to achieve a clear understanding of biometric technology.

In the United States, for example, the Department of Homeland Security’s Customs and Border Protection (CBP) agency is enabling the use of facial recognition, which is, in turn, encouraging multiple innovative pilot projects for scenarios ranging from bag check to boarding, in partnership with several major airlines and airports.

However, valid (and expected) questions and concerns have been expressed by consumer privacy advocate groups, a portion of the media and a minority of travellers. In fact, 60% of respondents to a global survey, Biometrics Institute Industry Trend Tracker 2018, feel that privacy and data protection concerns are restraining the biometrics market.

Healthy public discourse about facial recognition's viability as well as information security or privacy implications should be encouraged. However, thanks to a jaw-dropping amount of misinformation and subjective conclusions being erroneously drawn, the biometric waters are muddied.

Let's take a step back, stick to the facts and dispel some common myths or misconceptions around facial recognition and the way it will work in travel.

Myth 1: Airlines will keep passengers' identities and facial data on-file.

In this age of increasingly frequent data breaches, airlines don't want to store any more personally identifiable information (PII) than they absolutely have to, lest they incur additional IT burden, expenses and liability.

In the example given above, when you visit the United States, the CPB captures your facial image on arrival as part of admitting you into the country. These images are then used to compare to your face when you depart.

Myth 2: Facial recognition replaces current security measures.

Facial recognition doesn't mean secure documents will disappear. Digital passports, traditional IDs and even those stored on mobile devices will still be heavily involved in the traveller verification process. Longstanding airport security like manual inspections of physical identity and travel documents will remain in place for a long time to come.

What will likely be phased out are boarding passes, but those had little security value or true verification mechanisms behind them anyway – they're mostly symbolic tokens for logistics.

Myth 3: Facial recognition is the precursor to a Big Brother scenario inside airports and beyond.

With facial recognition for travel purposes, it's worth noting the distinct difference between surveillance – constantly scanning a crowd for identification – and the use cases for verification at check-in or boarding currently being proposed and piloted in some countries around the world.

In the latter, it's a 1:1:1 closed loop match in that the live face presented need only match the digital face image on the passport and the reference image associated with the flight manifest. No data is stored away, no additional data is gathered, no further matching is executed and nothing leaves the transaction.

This is likely to emerge as best practice, and will thus likely be applied when this technology arrives in South Africa.

The use of facial recognition for identification would be something that the police or security services would undertake and would thus be governed by the relevant laws.

Myth 4: The technology isn't currently reliable enough to be trusted.

Technology matures rapidly in the modern era. Facial recognition is already standard in the Microsoft Windows operating system and on some models of iPhones; consumers can see for themselves how well these applications work. The technology being introduced in airports is just as good.

There are limitations, of course, including the necessity for good lighting, but that would apply even to a human agent:

people don’t see in the dark, either. It is because of limitations like this that a human expert constantly backs up facial recognition for now.

And there’s an advantage that the technology confers, too. Facial recognition in its current state also isn’t subject to nearly the same conscious or unconscious biases that inherently skew human judgement. In that way, it’s already a step up.

Couple that with the fact that facial recognition has been fine-tuned in more controlled scenarios and put through rigorous real-world field tests. Even better, recent and coming developments in AI and machine learning will only advance facial recognition’s capabilities and increase levels of accuracy.

If facial recognition and its potential benefits for air travel are going to get a fair shake, we must work from a verifiable, consistent set of facts rather than being distracted by fiction, distortions and conspiracy theories. After all, the purpose of the technology is safer, easier and more convenient travel. And that benefits us all.

ABOUT THE AUTHOR

Thierry Mesnard is vice president of sales in Africa at Gemalto