BIOMETRICS - WHY NOW?

Q&A WITH JAMES CANHAM

MANAGING DIRECTOR OF ACCENTURE BORDER SERVICES

How big a part will biometric technologies play in our lives as they are adopted more widely in the future?

The need to confirm ones Identity, in order to access facilities and services is not new and dates back thousands of years. In today's highly complex crime environment pass-cards, paper based passports, and passwords can get compromised but biometrics do not.

The use of biometrics for security purposes brings with it a strong element of personal accountability - with biometrics, individuals understand they alone are being granted transit or access to systems or services and this personal association with access ensures a strong since of personal responsibility and drives appropriate behaviour. In the coming years, as IT infrastructure costs reduce and new biometric technologies mature we will see an increase in the deployment of biometric solutions right across the world by both public and private sector organisations.

Which industry sectors have created the biggest impact using biometrics? What sectors are currently seeing strong uptake?

Biometric technologies are presenting new opportunities for organisations both public and private to create new innovative identity and access management solutions. With the growth of globalisation, increased mobility and the societal shift toward online activities and home-working, the pressure is on for biometrics technologies to provide more robust forms of authentication to better facilitate business and citizen transactions, to protect organisational data and to facilitate travel and trade.

With advances in biometrics technologies and improvements in IT infrastructure, there is a growing acceptance of biometric recognition technologies in our daily lives and this acceptance will grow further with time. At the moment this acceptance however is largely confined to sharing biometric details with corporate entities such as banks and employers, with a growing acceptance of it across social media networks.

Globally we are seeing a noted increase in the use of biometric technologies (facial recognition in particular) by our policing and border agency clients as well as by airlines. Traditionally facial recognition was used to enable physical access control primarily but we are now seeing greater use by public sector clients to identify persons of interest on the street (police) or high-risk travellers at border crossings (border management agencies).

In Europe, proposals for a formalised European Union (EU) registered traveller programme and entry/exit system exist as part of an EU wide "smart borders" initiative. This is exciting and a fundamental shift in the approach to border management in the EU region. These proposed changes in border management processes offer a unique opportunity for border agencies to not only improve the experience of the vast majority of travellers and simplify life for the frequent flyer, but also to focus security efforts on the small minority of travellers who pose a risk or to whom entry or exit from a particular country should not be permitted. What is more, by fully exploiting the benefits of new border management technologies, border agencies can gain a consistency and completeness in border management, better support immigration programs and revitalise the traveller experience.

Biometric technologies are also playing an increasing role in securing corporate data but is by no means the next saviour of personal and corporate security. We are seeing biometrics play an increasing role but only along with existing and more established identity and access management solutions such as smartcards, security keys, pass-codes etc. While traditional access management solutions can be compromised as a result of person-person sharing, collaboration and theft, biometrics cannot be shared (and are rarely compromised) as each Individual has his/her own unique biometrics, with them at all times. It therefore makes sense to use biometrics as part of an organisations overall data security strategy in tandem with other access management tools. Many healthcare organisations are using biometric identification solutions to enable both site/ perimeter access and access to patient data.

Aside from policing and border agencies, are biometrics being used more widely in other areas of the public sector and government?

The private sector has seen significant uptake of biometrics to enhance user experience and security in smartphones, ATMs and mobile wallets, and the potential applications of this technology have not been overlooked by government agencies. Accenture recently surveyed nearly 800 public service technology professionals from nine countries in Europe, North America and Asia-Pacific to identify emerging technologies being implemented or piloted - including biometrics/identity analytics, the internet of things, video analytics, machine learning and others.

More than two-thirds (69%) of respondents said they are deploying or considering deploying biometrics.

The study found biometric solutions are in high demand and widespread use across government agencies, with e-passports and iris recognition being implemented most frequently. The industry sector citing the highest adoption rate of biometric technologies is public safety, at 51%, followed closely by respondents from pension and social security agencies (48%).

Public service agencies' primary objectives for implementing biometrics/identity analytics

1. Increasing citizen satisfaction and engagement

2. Reducing risk and improving security

Source: Emerging Technologies in Public Service, Accenture, 2016

While historically slow to digitise, governments have in fact long recognised the potential of biometrics to improve the way they serve citizens. The US Government began using biometrics for Trusted Traveler programmes in the mid-1990s, and the current US Visitor and Immigrant Status Indicator Technology programme (US-VISIT), which has a registry of approximately 200m unique identities, uses biometric technology to enable domestic and international stakeholder organisations to verify the identity and status of travellers.

Automated e-Passport gates, using biometric recognition software, are also becoming more commonplace at airports around the world. These gates enjoy high-levels of user satisfaction, increase passenger capacity at border crossing points and enhance security. The Netherlands has relied on biometrics-enabled passports for citizens since the mid-2000s, while countries like Ireland have been using biometrics to reduce identity theft and resulting welfare fraud.

But perhaps the most important application of biometrics technology is in the creation of national identity management programmes. In India, the Government-led Aadhaar programme aims to establish a biometrics-based registry for all 1.2bn residents. The United Nations High Commissioner for Refugees (UNHCR) is also working to register and verify the identities of displaced persons. The Biometric Identity Management System captures and stores fingerprints, iris data and facial images of individuals, providing them with what is often their only personal identity record. To-date the system has enrolled over 1.3m refugees across 69 locations in 29 countries.

One major concern aired about biometric technologies is they pose a threat to individual privacy. But advocates argue the opposite, that biometrics can be used to safeguard citizens against data breaches, identity theft, fraud and other violations of personal rights. Opponents of biometrics also cite the risk involved in creating a database of iris, fingerprint or other physical identifiers that cannot easily be altered or replaced in the event of duplication or theft. But unlike a password or PIN, the physical markers used in biometrics technology are difficult to replicate.

One potential solution is to develop multi-modal systems for verification. Both Aadhaar and UNHCR's system aggregate iris, facial and fingerprint data for each person. Of course, those who are unable to provide multiple forms of ID - for health, religious or other reasons – can still participate.

Those challenges are not inconsequential, but interest and investment in biometrics are unlikely to fade.
Some analysts are predicting that the industry will undergo double-digit growth by 2020.

What are your predictions for the next 10 years?

Biometrics are presenting new opportunities for organisations to create new innovative identity and access management solutions. With the growth of globalisation, increased mobility and the societal shift toward online activities and home-working, the pressure is on for biometrics technologies to provide more robust forms of authentication to better facilitate business and citizen transactions and to protect organisational data. With advances in biometrics technology and improvements in IT infrastructure, there is a growing acceptance of biometric recognition technologies in our daily lives and this acceptance will grow with time. At the moment, this acceptance however is largely confined to sharing biometric details with corporate entities such as social networks etc. Over the next 10 years this acceptance will broaden to allow for sharing of personal biometric data with one's employer and indeed Government. In the coming years, Accenture believes businesses and governments alike will introduce biometric technologies to enable better and more secure access to their data and operations but also to protect from data breaches and data loss.

What are the main barriers to biometric adoption?

In the past biometrics solutions have been expensive and difficult to deploy and use, and these challenges have hindered usage levels. In the future, as the total cost of ownership for biometrics decreases such technologies will become more prevalent in our daily lives - be it at airports and border crossings, in banks, at hospitals or when accessing government services (Citizen ID cards etc.).

Ease of usage has also improved greatly in recent years but there still remains an unfounded belief that biometric technologies are challenging to use, unreliable, and prone to inaccurate matching. Again, with time and increased usage this misconception will be altered.

Cultural issues can still hinder the adoption of biometric solutions in some countries where individuals do not like to have their pictures taken or the fingerprints copied. In some countries there also exists a negative association of finger printing with criminality - again these cultural issues will decrease with time as citizens and employees experience benefits accruing for the usage of biometrics by both governments and businesses alike.

What are the benefits of the various biometrics modalities (voice, fingerprint /vein, eye etc.) in border biometrics and where does your preferred modality fit in?

The use of biometrics to enable access to data or to facilitate travel must be based on a multi-modal approach, because different biometric modes have different strengths and should be used for different purposes. To establish the identity of an individual fingerprints and iris are highly reliable, with fingerprints being the most common of course.
Arguably, a 'gold standard' so to speak of biometric technologies is the iris scan, because it is the closest thing to a bar-code on the body, and is difficult to spoof, but this technology while highly accurate is expensive to roll-out across an organisation as part of an access management solution.

Finger-vein technology is perhaps one of the most promising of the established biometric modalities. Finger-vein authentication captures images of the vein patterns inside a finger. As they are inside your body, finger vein patterns are virtually impossible to replicate. The procedure to capture finger-veins is also non-invasive and contactless unlike the process of giving fingerprints.

Finger-vein technologies are proving popular in the healthcare industry whereby contact and touching is not desired and also in countries where cultures they do not like physically touching machines or having their photographs and fingerprints taken.
We are also seeing increased usage of facial recognition technologies to enable physical access control primarily but less so for data access. We are also seeing increased use of facial recognition technologies by our policing and public safety clients globally.

Voice recognition technologies are also on the increase and are highly suitable for transactions that can be completed over the phone - we are seeing the increased usage of these technologies by the financial services sector globally to allow clients access their accounts over the phone.

> **Where do you think are the future opportunities for border biometrics – in terms of applications or markets/ regions?**

Clearly for some industry applications biometrics work best, but these are usually in-person transactions for example when accessing banking services or government services and where in-person attendance can be required. Mobility, health, and e-commerce activities are all increasing and all demand robust forms of authentication in the face of increasing security threats. As biometrics solutions become more affordable and reliable, organisations will have more options for acquiring and implementing the technologies to suit their own environments to help manage threats to their data. Globally we are already seeing examples of biometrics being used successfully to grant access to corporate data and customer/citizen information.

As early as 2004, several Japanese banks, including Tokyo-Mitsubishi Bank and Mizuho Bank, chose to implement vein recognitions in ATMs and for over the counter transactions, to replace PIN codes when using bank cards. More than half of the country’s ATMs are now equipped with vein readers.

Banks in other countries have since followed suit, with BPS bank in Poland being one of the latest adopters of this technology. Doing so makes it harder for fraudsters to withdraw cash using stolen or fake cards – it also makes for a more convenient interaction for the customer, with no need to remember PIN codes to access their accounts.

The United States Department of Motor Vehicles use face recognition to confirm the identity of drivers when renewing their license, as well as to search their database of existing drivers before issuing new driver licenses, this ensures unicity of identity for these crucial photo ID documents.

**This Q&A was first published on Biometric Technology Today in February 2018.*
Visit the publication ***here****.*