ARGUS

Challenging the Biometric Myths

Argus Global

5 Meadow Court, Witney
OXON, OX28 6ER, England

+44 (0) 1865 989470
info@argus-global.co.uk

Challenging the Biometric Myths

Hollywood films and science fiction novels have led to some major misconceptions about biometrics and how they are used.

Most notably, it has placed biometrics in a league where they are misunderstood more than most other technologies on the market today.

Here we'll explore some of those myths and explain the thinking behind them, why they persist and why these perceptions are misleading.

Myth 1: Biometrics are expensive

Biometrics can be expensive, but not always. It depends on which biometrics are used, how they are used and the scale of the implementation.

In terms of biometric type, an iris camera is typically more expensive than a fingerprint reader. Also costs for the same kind of technology can vary widely.

Biometrics that are used in low-risk consumer applications, like laptop-integrated fingerprint readers and face recognition-enabled Smartphones, have a lower unit cost than the biometrics used for controlling site access at a government or defence site. This is simply because there are high-end and low-end applications, with varying degrees of speed and accuracy.

Scale and complexity

Scale and complexity also play a part in the cost to implement. A project that requires multi-modal biometrics (the use of more than one biometric) and integration across sites or with other systems will cost more than an iris access control system at a pharmaceutical plant for example.

Yet good economy and return on investment are also achievable in larger more complex projects.

Good solution providers will adopt an 'agnostic' approach where integration is possible across all technologies.

Myth 2: Biometrics are too complex

There's no denying that the underlying algorithms used in biometric technology are complex and therefore difficult for us normal business people to understand. But then, very few of us understand the technology that's used in a microwave or a car, and most of us can operate both. All you need to understand is the overriding concept of how biometrics work on a day-to-day basis. Any manufacturer worth their salt will be able to simplify biometrics to a level where you can understand the basics.

Your concern should be with the complexity of the user experience – both of the biometric device itself and the application. Again, good developers and manufacturers will design an interface that is simple to operate by people of varying technical aptitude. It is essential that any biometric device can be used by people who have little or no knowledge of technology.

The key is knowing how biometrics can work in your particular organisation and how you will benefit – whether that's through improved efficiency, lower overheads, reduced exposure to risk, or a combination of these.

The complexity usually comes when establishing how to integrate the technology, if that's a requirement but for the main it isn't and most solutions can be deployed with little fuss or impact on other business or security systems. But, as with any other business system, like Human Resources, Time and Attendance or Customer Relationship Management, this is largely dependent on what you already have and how you want biometrics to fit within that.

Myth 3: Biometrics breach privacy

There are groups who believe biometrics have the potential to violate privacy. And that's exactly why we have laws like the Data Protection Act, to regulate how we handle and use data. Good developers will create protections and security conforming to legislation.

The misconception is that biometrics in and of themselves are a privacy violation. Cases like the recent Facebook face recognition scandal, where Facebook has continued to use people's data for photo tagging, even after individuals have opted out of having their data used in this way have not helped. Biometric and Systems providers would agree that this is inappropriate and that there needs to be better regulation of how face recognition is used on social media sites and other consumer applications.

Of course when biometrics are used well, the protection they offer is invaluable.

Biometrics can't be copied, stolen or lost

In fact in many ways biometrics protect people's identity far more than they risk violating it. Unlike passwords, PINS and other forms of 'ID', biometrics can't be copied, stolen or lost. With these forms of ID, it is the card or PIN that is given access, rather than the individual.

In fact biometrics are the only form of identification that truly identifies a person. They ask: 'Who are you?' rather than 'Are you who you say you are? That means the likelihood of someone gaining access to your personal information other than you, whether your bank details or passport information, is significantly reduced.

In the case of biometrics, False Acceptance Rates (FAR), where people are mistakenly identified as someone else, are typically very low. Especially where security is at a premium, say at border control or in a government building, organisations almost always use the more robust technologies, like iris recognition and multi-spectral fingerprint technology. Iris ID has shown a FAR of Zero.

There have been tests in the past where latex imitation fingers have fooled fingerprint readers into a false acceptance. But the recent development of multi-spectral fingerprint readers lay to rest this concern; multi-spectral technology will only accept live fingers, as they work by detecting the blood that flows through a finger.

Biometrics and data access

The other issue here is a muddying of the waters when it comes to the actual biometric device and the data it gives access to.

Yes, biometrics gives people access to data if they have permission. However the process of biometric identification itself is simply about how the data is accessed. So, if Biometrics make the data more secure, then you are actually doing more to protect people's privacy.

A particularly misleading argument against biometrics, is that biometric images can be stolen and used to gain access. In fact, the way biometric information is held makes this near impossible. Once a biometric, like an iris, has been scanned at the point of enrolment, a template is produced that consists of encoded and encrypted data. It's that template which is matched to an individual's iris/finger/face/finger/vein, when they present themselves for future identification. It is a protection designed into the software that prevents the theft of that template and producing a replica from it that would fool a biometric device into false acceptance.

You must also bear in mind that biometrics aren't a panacea for all security requirements. In the same way that, if you leave a door open, you can't blame a faulty lock for a break-in, you need to ensure that the networking and physical location of your data is secure. Biometrics offer an additional physical layer of security: they cannot be held responsible for every which way that information can be accessed.

Myth 4: Biometrics are slow

As we've discussed, biometrics do vary; one of the main ways in which they vary is speed.

The following factors will affect the speed of a biometric device:

1) **The level of interaction required with the user.** For example, some face recognition technologies require no physical interaction at all, which is why they are typically used in areas of large throughput, like airports. However these are slower than finger or iris.
2) **The speed that the device can search and match the database.** Some biometrics are faster than others but generally most are quite able to be deployed in situations where speed is important. When we compare different matching speeds we are comparing systems that are all generally able to return a match in under 2-3 seconds

from very large data bases. So finger, iris, face and the like are nowadays routinely used in high traffic environments.

Having said this, it would be unfair for us to make unequivocal statements about the speed of any given technology, so it's important to check this with your biometrics provider. We would highly recommend visiting a site to see how the technology is used and therefore the speed at which people are processed.

In summary

We hope that this paper has given you a good overview of some of the myths that surround biometrics and how they've come about. It should also reassure you that many of the myths about biometrics are unfounded.

As with any technology it is important to query suppliers about any concerns you may have, so that they can address these misconceptions and hopefully put your mind at rest.