Challenging the biometric myths

Sci-fi mystery and images of Tom Cruise have led to some bloated and fantastical misconceptions about how biometrics are used. Most notably, it has placed biometrics in a league where they are reviled and misunderstood more than most other technologies on the market today.

Here we hope to explore some of those myths and explain both the thinking behind them, why they persist and why these perceptions are (thankfully) wrong.

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, but of course this depends on the manufacturer, with costs for the same kind of technology varying widely. As an example, the individual iris cameras that are used to control access at a manufacturing plant will cost considerably less than an iris camera that's used in areas of high throughput, such as in airports and at border control.

Likewise, biometrics that are used in low-risk consumer applications, like laptop-integrated fingerprint readers and face recognition enabled Smart phones, have a lower unit cost than the biometrics used for controlling site access at a government defence site. This is simply because, and as we see time and again with other technologies, there are high-end and low-end applications, with varying degrees of speed and reliability.

Biometrics that must be fast and/or used in areas of high risk, will always be far more costly than those used in low risk/low throughput environments.

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, will cost more than an iris access control system at a pharmaceuticals plant.

Yet even in larger projects, costs needn't escalate out of control.

Good solution providers will adopt an 'agnostic' approach where integration is possible across all technologies. Agnostic technology enables the reconciliation of biometric hardware with third party software solutions – like building management systems - so that complex and expensive customisation isn't required.

Biometrics are too complex

There's no denying that the underlying algorithms used in biometric technology are complex and therefore difficult 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.

As implementers of biometric technology, all you need to understand is the over-riding 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 interface – both of the biometric device itself and the enrolment technology. Again, good 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 the above.

The complexity usually comes when establishing how to integrate the technology. But as with any other business system, like HR, T&A or CRM, this is largely dependent on what you already have and how you want biometrics to fit within that.

Biometrics breach privacy

There's no doubt that in the wrong hands, biometrics have the potential to violate privacy and contravene laws like the data protection act. But that's the key term here: in the wrong hands. Any technology, when used inappropriately, whether a Customer Relationship Management system, or a database used for holding personal banking information, can be a threat to our privacy. And that's exactly why we have laws like the data protection act, to regulate how we handle and use data.

The misconception that biometrics in and of themselves are a privacy violation, is probably the most inaccurate and ironically, most widely held view of biometrics. This is largely due to high profile cases like the recent Facebook face recognition scandal, where Facebook has continued (as we write) to use people's data for photo tagging, even after individuals have opted out of having their data used in this way. Most people would agree that this is inappropriate and unethical; and that very much includes the minds behind biometrics themselves. No-one likes to see their hard work either a) go to waste or b) be used for purposes that it is wholly unintended for.

Biometrics can be used flippantly and incorrectly, but when used well, the protection they offer is invaluable. Because once you strip back the hysteria, it's possible to see that in many ways biometrics protect people's identity far more than they risk violating it. For one, 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.

False Acceptance Rates (where people are mistakenly granted access) are typically very low, and 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. As an example, the *i*evo multi-spectral fingerprint reader has an FAR of less than 0.00001%; likewise iris ID claims an FAR of 1 in 1.2 million.

There have been tests in the past where cadaver and play doh imitiation fingers have fooled fingerprint readers into a false acceptance. But the recent development of multi-spectral fingerprint

readers lay to rest this concern, as multi-spectral technology will only work with live fingers, as they work by detecting the blood that flows through a finger.

In a far-fetched scenario, it could be possible to construct a latex finger and pump a substance through it to achieve a likeness to a live finger, but the sheer effort and sophistication required renders this an extremely unlikely scenario. And if it were to happen, it's fair to suppose that it would be a rare event.

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 *do* give people access to data, but the process of biometric identification itself is simply *how* the data is accessed. So it stands to reason that if you're accessing data more securely, you're reducing the chance of people gaining access to that data, ergo, you're doing more to protect people's privacy.

In the case of Facebook, the great irony is that most people use the social networking site quite freely: bandying about personal data on a daily basis and without a 2nd thought. But throw the word 'biometrics' into the mix and suddenly it becomes a whole different ball game. Suddenly we're concerned with what's happening with our data, despite years of carelessly shouting about what's happening in our lives on the internet. It does beg the question 'What does photo tagging leave you exposed to that you weren't exposed to before?'

This is not to negate the issue, but rather to say: are biometrics really the problem here?

A particularly misleading, but equally pernicious argument against biometrics, is that biometric images can be stolen and used to gain access. This works on the (quite simply, false) idea, that there's a database somewhere with an image of an iris, face or fingerprint on it. In actual fact, there's no such thing. Once a biological entity, like an iris, has been scanned at the point of enrolment, a template is produced that consists of encoded data. And 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 almost an impossibility that someone could steal that template, crack the code, and produce a replica from it that would then fool a biometric device into a false acceptance.

For anyone who does entertain this as a possibility, we would ask you the question: 'So what's the alternative?' i.e. what other method of identification is proven to be more secure than, and will therefore offer a higher degree of privacy, than biometrics?

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 wide open, you can't blame a faulty lock for a break-in, likewise you need to ensure that the networking and physical location of your data is secure. For example, how robust is the casing? Are there ways that people can access this information by hacking into a network? All biometrics do is offer one physical layer of security; they cannot be held responsible for every which way that information can be accessed.

Biometrics are slow

As we've discussed, biometrics do vary and one of the main ways in which they vary, is speed. Several things will affect the speed of a biometric device. These are:

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.

2) The speed that the device can search and match the database. Iris templates are lighter, so they take less time to match, unlike some fingerprint templates, which are typically large and unwieldy, which makes matching more time-consuming.

   Having said this, it would be unfair for us to make unequivocal statements about the speed of any given technology, so this is something that you must ask for proof of from your 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 many ways this will be far more useful in your assessment of the technology than the cold facts.

In summary

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

As with any technological implementation, 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.