# Biometric Myths: Six Of The Best

by Russ Davis - CEO of ISL Biometrics - Tuesday, 13 July 2004.

It is probably the hottest sector in the security field today. Yet the biometrics industry, which produces human-based identification systems, is weighed down with claims and counterclaims, fallacies and myths. While some of the myths are no doubt based on an element of historical or scientific truth, some are now so out of date or inaccurate that they are almost laughable.

*Myth number one* - The first myth that needs to be dispelled is that biometrics is a modern-day idea. Despite its high-tech glitzy image, the principles behind the technology can actually be traced right back to Egyptian times, when workers building the great pyramids were not only identified by their name, but also their physical size, face shape, complexion and other noticeable features, such as scars.

It may have taken the next four-and-a-half thousand years to really get going, but the technology is now experiencing a "hockey stick" adoption curve with governments, hospitals, schools, airports, retail outlets and modern offices all successfully using this remarkably straightforward empowering technology.

## Technology truths

The problem with such a rapidly emerging industry is that many people are elevated to the position of "expert", almost overnight. This can be a particularly dangerous situation – especially when the expert used to be the company salesman or marketing executive.

This scenario has led to some of the industry's best technological fallacies, which can either be put down to pure ignorance, or worse, the stirring up of malicious rumors in order to gain competitive advantage.

Take for instance *myth number two* – iris recognition devices use lasers to scan your eyes. This damaging rumor is completely without substance, although the confusion is understandable given that the first company to produce such a system called itself IrisScan (now renamed as Iridian Technologies).

In fact an iris recognition camera takes a black and white picture from up to 24 inches away and uses non-invasive, near-infrared illumination (similar to a TV remote control) that is barely visible and very safe.

*Myth number three* – stolen body parts – is also a classic, and has been seized upon by many a Hollywood director, who are not known for letting the true facts cloud a good storyline. With most biometric devices there is an element of liveness detection, which can measure many variables, from a finger pulse to a pupil response. This would normally be enough to prevent the system from working once the body part had been removed. However, other factors quickly come into play. For example, an extracted (or enucleated) eyeball quickly begins to decompose, with the cornea clouding over and obscuring the iris. A severed finger also dies rapidly – typically becoming useless after around 10 minutes.

## New myths

Fingerprint technology also gives us *myth number four*. This relates to the inability of the technology to enrol or verify the identity of children, or women of Asian descent. This myth is relatively new, because until a few years ago it was a reasonable criticism of the technology, given the challenge of acquiring small fingers with “faint” fingerprints.

However, recent advances in imaging have led to far greater resolutions being achieved by fingerprint sensors, so boosting a biometric system’s ability to extract the pertinent information required to create a biometric template of that person.

Children, in particular, seem to hold no fear of the technology, believing it to be “cool”. It may be surprising to learn that at least 1,300 primary schools in the UK are using fingerprint technology to replace old-fashioned password-based systems in their libraries. The interesting spin off benefit here is that so many children want to use the technology that the number of books taken out increases dramatically.

**Police protection**

*Myth number five* on the list relates to the belief that fingerprint information captured by a commercial fingerprint system could somehow be used in a criminal investigation. This myth stems from a misunderstanding of how a biometric system typically works in a commercial environment.

Almost none of the available commercial fingerprint-based systems store the entire image of a fingerprint. Rather they extract information from that fingerprint to create a mathematical representation or template. This template, which is often encrypted, is designed so that it cannot be reverse engineered to reconstruct the original fingerprint image, and so is useless information to the police, or indeed a hacker. (The feeding of identical template data to a fingerprint system’s matching engine by a hacker will normally fail, as this is almost a sure indication that the data has been stolen and that a replay attack is underway.)

In a non-commercial biometric system, such as the recently announced US-VISIT system, which is being installed to monitor the comings and goings of foreign nationals in the USA, the situation is different, with full fingerprint and facial images being acquired and stored. This information can and has led to the arrest of more than 500 people since January 2004.

**The silver bullet?**

The final *myth number six* is perhaps the most important. So often biometrics are touted as the silver bullet that will rid the world of evil. Again this is to over-estimate and misunderstand the abilities of biometric technology.

For instance, contrary to common belief, biometric systems are not able to confirm with any level certainty the true identity of a person. Rather, they are able to confirm whether this is the same person that initially enrolled into the system. The person’s true identity is irrelevant to the biometric system. Confirming a person’s true identity is far more a question of checking the validity of an individual’s official identification documents, such as birth certificates or driving licenses.

Biometric technologies are also unable to perform miracles. If a government doesn't have a quality photograph of a known terrorist suspect, then the chances of stopping that person at a checkpoint using facial recognition are slim.

All that said, biometrics can play a valuable assisting role in the fight against organized crime and terrorism, but it must be part of a holistic approach, which uses many different strands of information.

**From myth to reality**

While there are many other myths plaguing the biometric industry, the good news is that the technology has been able to rise above them to claim its place at the security top table. The benefits of the technology have just been too attractive to let unfounded myths get in the way.

Some of today's best biometric systems are saving organizations time and money, while helping to raise the security bar to new heights. For example, "door-to-desktop" systems are now appearing, which merge an organization's physical access control system at the front desk with its network of computer terminals around the building. This enables an employee to replace cumbersome tokens and passwords with their fingerprint, turning the premises into a truly smart environment.

In the past, pundits have talked about mainstream biometric adoption being years away. Today, with smart passports just around the corner, and adoption rapidly increasing in places such as hospitals, schools and airports, new estimates are being measured in months. The myth that biometrics will never become a mainstream technology is truly being smashed.

**A brief history of biometrics**

Biometrics go back a lot further than their futuristic image might suggest. Even the architects of the Great Pyramids in Egypt recognized the benefits of identifying their labourers using previously noted bodily characteristics.

The Egyptians were clearly ahead of their time, as very little development in the field of biometrics occurred for around four thousand years. It was only in the late 1800s that people started to develop systems that used the fingerprint and other bodily characteristics in order to identify individuals. In 1880, for example, Henry Faulds, a Scottish doctor living in Japan, published his thoughts on the variety and uniqueness of fingerprints, suggesting that they could be used for the identification of criminals. Meanwhile, in 1900, the important Galton-Henry system of classifying fingerprints was published.

Other than a few isolated pieces of research into the uniqueness of the retina (which was finally turned into a workable product in 1985), the biometric industry remained fairly static until the 1960s, when the Miller brothers in New Jersey, USA, launched a device that automatically measured the length of people's fingers. Speaker verification and signature verification were also developed in the 1960s and 70s.
Interest from the US armed forces and intelligence agencies then emerged, but it wasn't until the turn of the century, and in particular until after 9/11, that the awareness of biometrics broke out of specialized industry circles to reach the fever pitch

broke out of specialized industry circles to reach the fever pitch levels seen today.