


# Face facts

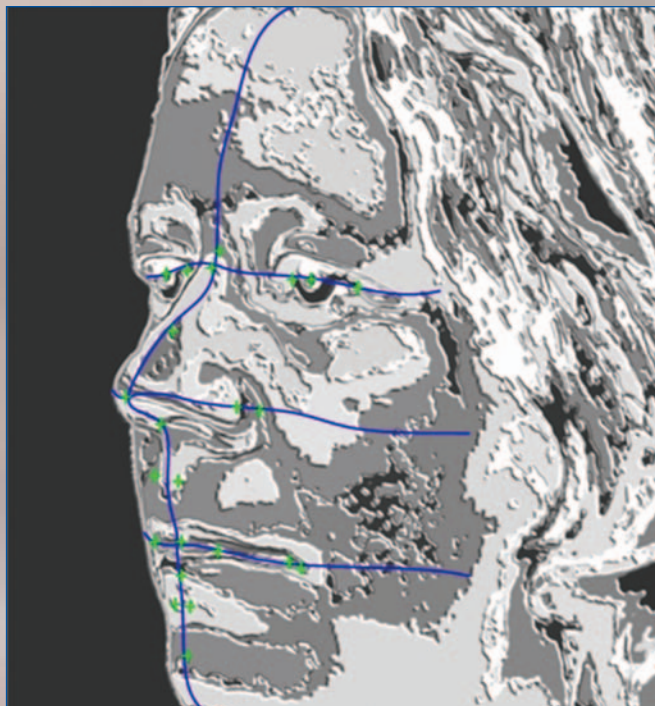
**Biometric testing - identifying an individual by face, eye and fingerprints - could be used to create an identification card which would be compulsory to every person in Britain in years to come. The ID cards could be an effective tool to help police officers but debate still rages on how effective they really are. David Cleden examines the debate.**

 A routine police patrol pulls over a vehicle being driven erratically. Instead of asking for a driver's licence, the officer snaps a digital picture of the driver's face and transmits it back to the local station via a wireless link in the patrol vehicle. The picture is compared against a facial image database, a match found, and the identity of the driver flashed up on the officer's in-car terminal - all without needing the cooperation of the driver, who may be incapacitated or abusive. Not only does the officer know who he's dealing with, he can see the full history of previous convictions, local intelligence and whether the driver is on a watchlist.

Sound far-fetched? Using biometric facial recognition, Los Angeles police are doing this right now.

Biometrics - the ability to identify an individual by measuring key unique biophysical attributes such as a picture of the iris - could revolutionise policing. Just as the twentieth century saw fingerprinting become an invaluable forensic tool, new biometric techniques such as iris pattern-matching and facial recognition could have an equally profound influence on 21st century policing. But with the debate still raging over the Government's scheme for ID cards, are biometrics really up to the job? If the technology is not foolproof, will it make frontline policing even harder? Do they infringe on civil liberties?

The Federation believes that the cards could bring benefits for



**Biometrics: identifying unique human attributes**

both the public and police officers. An individual's details can be checked instantly meaning they would not have to report to a police station and they could potentially help free up police time and help with fraud prevention.

### Biometrics in action

A useful biometric trait is something which makes you measurably unique. Three of the leading contenders are facial recognition, iris pattern measurement and fingerprinting. The father of them all, modern fingerprint identification, was first conceived back in the mid-nineteenth century by

William Herschel and Henry Faulds and subsequently improved by many others. But today's generation of portable electronic measurement devices offer new possibilities - realtime, in-situ print and palm-matching against comprehensive databases.

Many identification schemes are combining several different biometric traits as a way of reducing error rates. For example, Ident1 is a prototype biometric fingerprint system developed by the Police IT Organisation (PITO) which is set to become the platform for a National Biometric Identification Management System.

Yet biometric identification is only as good as the size and extent of the data available for searching. It may soon be possible to search beyond national boundaries - not necessarily through the exchange of records, as data protection laws are still problematic, but perhaps through 'joined up' searches of national databases.

Dr Fred Preston, PITO's director of identification, speaking at the Biometrics 2005 conference said: 'Our experience in Europe has been a reluctance to supply data to other countries but far less reluctance to interoperate with other countries. My vision is cross-country searches rather than the sharing of databases.'

All types of biometric identification rely on a three-stage process: registration, storage and comparison. During registration, a digital image (e.g. of the eye, face or fingerprint) is processed by computer to create a 'template' - essentially a string of numbers which uniquely describe the measured features. This digital code acts as a point of reference, unique to the individual, like the specimen signature held by the bank when an account is opened. Once created, the template is stored in a tamper-proof format, using digital signatures, for later comparison either in a database or on removable media such as a smart card.

For public acceptance, registration must be a swift, uncomplicated, one-time process. Two minutes is the enrolment target proposed by the International Civil

Aviation Organisation (ICAO) who are developing European standards for biometric passports. Contrast this with the eight minute average achieved in the 2004 trials carried out by the UK Passport Service which captured three different biometrics (facial, iris and fingerprints). Using a range of biometrics it reduces registration failure rates. But it has two main drawbacks: registration is a more complex and time-consuming process, and crucially, subsequent identification may be slow because of the complexity of searching the data.

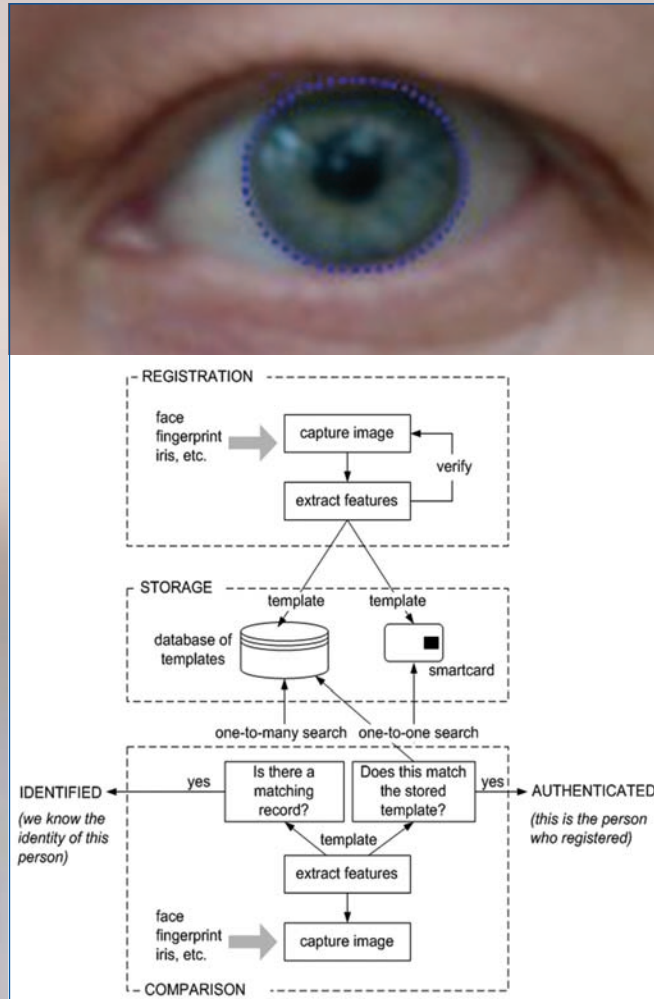
The recommendation for European biometric passports is that they contain a facial image and at least two fingerprints. The UK Government is also interested in iris recognition which is appealing for its high accuracy and identification speed when matching within a database of potentially millions of records.

In the comparison stage, biometric attributes are again captured from an individual going through a scanner. If the purpose is authentication, to verify that this individual now claiming to be John Smith was registered as John Smith, the system need only compare the current biometric with the appropriate template and verify that there is a one-to-one match. But to identify an unknown person, the system must work much harder, comparing the current attributes against each template held on the system. Some biometric techniques such as a facial recognition may throw up a shortlist of potential matches – i.e. a suspect list requiring further investigation.

### Limitations

But amidst these promising trends, it is important not to lose sight of the limitations of biometrics. Some reports suggest that recognition error rates can be as high as ten per cent, as reported by the UK Passport Service trial, rising to 40 per cent for disabled groups.

Many of the problems relate to environmental conditions. Poor lighting, excess reflection, tilting of the head, or subsequent injuries and illness can all affect successful measurement, causing the system to fail to recognise a



### Biometric: identity parade

previously registered individual, a "false negative" result or, perhaps more worryingly, to match the individual to an incorrect record, a "false positive".

No single biometric system guarantees coverage of the entire population. It is estimated that one in 50 people may have fingerprints unsuitable for biometric recognition, because of disablement or relatively common injuries such as cuts, abrasions and bruising. One in 75,000 people suffer from aniridia, the lack of an iris, and eye surgery and ageing have been shown to have detrimental effects on the long-term performance of iris recognition. With half the population of Western Europe having some form of visual correction, any technique which is sensitive to reflection from spectacles or contact lenses will be unworkable.

In September 2005, new requirements for passport photos were introduced with an eye on their suitability for facial recognition: capture the full face, look

straight ahead with a neutral expression, keep your mouth closed. But even simple requirements like these are a challenge for some disabled people or young children.

Nevertheless, establishing identity is such a fundamental part of policing that anything which improves its efficiency has to be regarded as a good thing, from the force perspective. As with any new technology, biometrics have their limitations. What will determine their ultimate success is the extent to which operational processes and the legal frameworks are able to take these fully into account.

● For more information on the Federation's view on ID cards click on:

[http://www.polfed.org/we\\_stand\\_identity.asp](http://www.polfed.org/we_stand_identity.asp)

● David Cleden writes on the subjects of technology and criminal justice issues

### Police use of biometrics

Just how will these technologies affect law enforcement? Identification plays such a core role in policing that changes may come in many different areas:

● Positive identification of suspects: a search against a National Identity Register could replace the time-consuming process of circulating photographs or reconstructions of unidentified suspects.

● Confirmation of identity: a 'one-to-one' match via a biometric identity card quickly confirms claimed identity and avoids the need to report to a police station.

● Controlled access: some forces already use biometric measures to ensure only authorised staff have access to sensitive systems or restricted areas.

● Screening for suspects – under favourable conditions, facial recognition algorithms can process CCTV footage and identify previously detained suspects. With the wider use of high definition CCTV, this could have a dramatic effect on the time-consuming and fallible screening of videotapes by officers.

● Covert surveillance of suspects – unlike fingerprinting and iris recognition, an individual may be unaware that facial identification is taking place.

West Yorkshire Police are one of several early adopters of biometric facial recognition. It is not a foolproof means of identification and, as yet can not be used as evidence, but it can be a good source of leads. In trials, more than 70 per cent of images searched against a database generated useful leads, resulting in as many as two or three arrests a week by the force. The National Crime Squad have used it to match images of missing children, and several forces are testing the more advanced 3-D facial imaging which is claimed to be sophisticated enough to even detect facial differences between identical twins.