Biometric fact and fiction (Biometric fact and fiction) (SU)
ECONOMIST, October 26, 2002

Body-scanning technology has its drawbacks

YOU'VE seen them in spy films and science-fiction movies: eye-scanners, fingerprint readers, facial-recognition systems. Such body-scanning or "biometric" systems, which can make sure that somebody really is who he claims to be, are touted as the ultimate in security technology. Systems protected by passwords are unlocked by something you know (the password), which others can find out. Systems protected by keys or their high-tech equivalents, smart cards, are unlocked by something you have (the key), which others can steal. But systems protected by biometrics can be unlocked only by a bodily characteristic (such as a fingerprint) that no one can take from you. Your body is your password.

Eye-scanning biometric technology played a prominent part in a recent science-fiction movie, "Minority Report". Its star, Tom Cruise, played a policeman accused of a crime who goes on the run. In the movie's futuristic setting, eye scanners are used to ensure that only legitimate users can access computer systems. Mr Cruise's character has eye transplants to conceal his identity, but also keeps his old eyeballs so that he can continue to log on to the police network.

That excursion into a fictional future highlights two real problems. The first is that the technology is not as secure as its proponents claim. Scanners that read fingerprints, the most widely used form of biometrics, proved easy to defeat in experiments carried out by Tsutomu Matsumoto, a security researcher at Yokohama National University. Mr Matsumoto was able to fool them around 80% of the time using fingers made of moulded gelatin. He was also able to take a photograph of a latent fingerprint (from a wine glass, for example) and use it to make a gelatin finger that fooled scanners 80% of the time as well. One advantage of gelatin is that having got past the guards, an intruder can eat the evidence.

Facial recognition, in which a computer analyses images from a digital camera and compares them with a "watch list" of known faces, is unreliable too. A study carried out at America's Defence Department found that instead of the claimed 90% accuracy rate, such systems correctly identified people only 51% of the time. Since the September 11th attacks, the technology has been tested at a number of American airports, but in one trial it was found that face-scanners could be fooled by people who turned their heads slightly. Recalibrating the system to allow looser matches caused a flood of false positives (where someone is wrongly identified as being on the watch list).

Identix, a leading supplier of facial-recognition systems, claims that its equipment's accuracy rate can be as high as 99%. But Mr Schneier, the security expert, says that even with an accuracy rate of 99.99%, and assuming that one in 10m fliers is a suspect whose face is on the watch list, there will still be 1,000 false alarms for every suspect identified. And most terrorists are not on watch lists. Face-scanning may reassure people and may have a deterrent effect, but these meagre benefits do not justify the costs.

The second and more important problem is that biometric technology, even when it works, strengthens only one link in the security chain. Its effectiveness is easily undermined by failures of process or policy. Tom Cruise's character in "Minority Report" is still able to get into the police computer network while on the run because someone has neglected to revoke his access privileges. This simple failure of process is all too common in real life. Another such real-world failure involves the use of hand-geometry scanners in airports. Each person's hand is supposed to be scanned separately, but often the first person in a group goes through the door and then holds it open.

In short, biometrics are no panacea. The additional security they provide rarely justifies the cost. And in high-risk environments such as banks or jails, other measures are still needed.