Your personal passport

With security concerns on the increase, governments are measuring the effectiveness of biometrics as a means of secure identification. But can biometrics really deliver what governments are promising?

As part of the 2001 US PATRIOT Act, designed to improve homeland security after the September 11 terrorist attacks, the US Immigration and Naturalization Service will require all visitors entering the country to present identification with biometric data from October 2004. By imposing this requirement on virtually all non-Americans wishing to visit the USA, the US government has pushed biometrics into the forefront of foreign governments' agendas and sparked new debate over how far legislation can go in limiting terrorism and safeguarding security. Proponents cite the terrorist attacks in the USA and elsewhere as an argument to step up all security measures, not just at airports. Opponents of the use of biometrics in identification and verification fear that it might become another way for governments to intrude into citizens' privacy.

Biometrics are used to automatically identify individuals by measuring physical or behavioural attributes. Features such as fingerprints, facial characteristics, retina or iris patterns, speech, hand geometry, ear shape and body odour are all legitimate biometric measures, although their usefulness in distinguishing individuals varies significantly. Furthermore, the type of biometric information required and the technology used to measure it depend on the usage. In general, biometric data are either stored on a personal smart card or in a large central database and can be compared against an individual's physical feature to determine whether they are who they claim to be. Advocates of the technology argue that biometric information is much safer and more reliable than current methods of access and identification—unlike a key, it cannot be lost and unlike a password, it cannot be

forgotten. And there is little point in stealing, sharing or duplicating biometric data because they are essentially useless without the accompanying physical characteristic.

The requirement that biometric data must be highly unique to each person also limits the physical features that can be used. There should be minimum variability within a person's lifetime, but maximum variability between persons. In addition, biometric measures should be easily obtainable. Currently, fingerprints are the most commonly used biometric; they have been in use for over a century, particularly in law enforcement. Fingerprints are easily obtainable and highly unique to each person, although the way in which they are compared can make it difficult to clearly distinguish individuals. In addition, scar tissue, dirt, grease and creases on the fingers can hinder the process of obtaining and comparing fingerprints.

"What really determines biometric power is the degree of randomness and the degree of complexity in the pattern," commented John Daugman, Professor in the Computer Laboratory at the University of Cambridge, UK, who developed the algorithms behind all commercial applications of iris-recognition software. For these reasons, the iris is an ideal subject for biometric identification, because of its extensive variations. Genetically identical twins have different iris patterns and a person's two irises are as different as the irises of two different individuals. Even blind people can be identified, as long as the sightless eye still has an iris. Furthermore, the technology has been developed to the point that a person's iris can be scanned and compared with stored data within seconds, making iris recognition as fast as fingerprinting and more reliable.

Face recognition is not as reliable as fingerprinting or iris recognition, but it is easy

to implement and so is commonly used. Internal features of the face are measured, such as the distance between eyes and the length of the nose, but as the algorithms are easily tripped up by changes in hairstyle, facial hair, body weight, simple disguises, the effects of ageing, and variations in camera angle and lighting, the technology has not yet reached high levels of accuracy or reliability. According to the US National Institute of Standards and Technology, even the best face-recognition algorithms can have false-match rates as high as 43%. But, despite its drawbacks, this is probably the best biometric for surveillance, because individuals can be photographed without their knowledge or consent. The International Civil Aviation Organization, the Montreal-based UN agency that sets travel standards, recently selected face recognition as its biometric of choice for passports, with the option for a secondary one, such as fingerprints or iris images.

Ultimately, the biometric technology used depends primarily on the objective: whether the aim is to identify an individual (search their biometric against a database) or verify their claimed identity (compare their biometric data against data on a personal identification card). In principle, all biometric measures can be used for verification, but only those that are unique to a person can be used for identification. The effectiveness of any biometric depends on the false-match rate and the failure-to-match rate: when comparing a person's biometric data against a large database, falsely matching that person against someone else—for example, a suspected terrorist—could cause more than just inconvenience. Equally, failing to identify someone correctly as a terrorist is not acceptable. As Daugman said, "with all biometrics, you have to think about

Opponents of the use of biometrics in identification and verification fear that it might become another way for governments to intrude into citizens' privacy

both error rates—what's the false-match rate and what's the failure-to-match rate?" Any biometric system can make its false-match rate zero by rejecting everyone, and can make its failure-to-match rate zero just by accepting everyone. According to Daugman, the key to any biometric system is the trade-off between these two rates.

The demand for secure identification and verification is increasing in many situations, such as access to protected areas or computer systems and networks, banking and business transactions or international travel. Face recognition is already used in general surveillance, from spotting serial cheats on the casino floor to finding known football hooligans in large crowds. Many banks include photographs on credit cards to curb fraud. Fingerprints have been integrated into driving licenses in India and Argentina to combat identity fraud. In Disney World, season-pass holders access the theme park by having their fingerprints scanned. The US and Canadian Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) uses hand geometry with an ID card to speed up immigration processing for more than 45,000 participants

in the system. Many companies use iris recognition to track the attendance of their employees, while banks have been using this technology to identify customers and give them access to their accounts, particularly at cash-point machines.

However, international travel, particularly through airports, has become the focal point of biometric technology. Many countries, such as the UK, Japan, the Netherlands, Canada, Germany, Israel and the United Arab Emirates already use biometric data for security and immigration control in airports and other ports of entry by giving employees and selected customers a smart card carrying their biometric information or by comparing their data against a database. Biometric information is also used to control access for

service workers to restricted areas in an airport, including the airfield and aeroplanes. In addition, some airports use it to ease international immigration. Amsterdam's Schiphol airport uses the 'Privium' iris-recognition system in combination with a personal smart card to make immigration easier for selected customers. Iris-recognition systems have also been installed in Frankfurt Airport for pre-approved passengers and the German Federal Border Police will test the system over a six-month period. However, this might be overkill. "I don't like that application because it really under-exploits the power of iris recognition," Daugman said. "You don't really need anything as powerful as iris to do that. ...Even face recognition would be good enough for one-to-one verification."

While these are local applications, the US government is keen to impose biometric identification globally. By requiring all foreign visitors to present valid passports with biometric data, the USA plans to control closely visitors who enter and leave the country. They have already been using biometrics in several border-control applications. Since 1998, border-crossing cards issued to Mexican citizens allowed to work in the USA include a photograph and two fingerprints, and the Department of Homeland Security uses a fingerprint-identification system to identify illegal immigrants. Since September 11 2001, new laws also require much more extensive use of biometrics in immigration control. All foreigners applying for a visa to enter or work in the USA are now required to provide a fingerprint. This has already drawn criticism. As columnist Thomas L. Friedman said in *The New York Times*, "Give us your tired, your poor and your properly fingerprinted" (Friedman, *The New York Times*, December 21, 2003). For the most part, these controls apply to non-Americans—US citizens merely use the technology to make their lives easier and speed their way through airport customs and immigration.

Advocates of the technology argue that biometric information is much safer and more reliable than current methods ...

Some countries were already considering the introduction of biometric information before the US Congress passed the PATRIOT Act. Like many other EU countries, Germany already has a national identity card that citizens must carry at all times and Federal Interior Minister Otto Schily is keen to add biometric data to passports as an extra security measure. Schily and US Department of Homeland Security Secretary Tom Ridge agree that biometrics should be consistently applied to curb crime and prevent terrorist activity, and according to Ridge it is up to the USA and Europe to set the path for the rest of the world to follow. German legislation has already defined the parts of the body on which biometric data can be collected—the face, fingers and hands—and Schily is a strong advocate for the technology at the European level. However, data records of German citizens will not be stored centrally according to the Federal Ministry of the Interior, as this would violate the German

Data and Privacy Protection Act, which forbids the central storage of personal data.

In the UK, the debate about biometrics is stalling as it is closely linked to the debate over a national identity card, which many Britons strongly oppose. The UK Home Secretary David Blunkett recently proposed the introduction of a national identity card that would include some form of biometric data, which would also be stored in a National Identity Register—but appropriate legislation must still be passed through Parliament. According to the Home Office's Identity Card Policy Unit, the aim of "building a new, highly secure database is at the heart of an identity cards scheme," and the UK Passport Service is planning a six-month trial to test the recording of face, iris and fingerprint biometric information. "If a reliable and robust biometric like iris [recognition] is used in them, I support it," Daugman commented, "but certainly not if an unreliable one like face [recognition] were to be chosen."

But while many governments seem to be eager to use biometric data for security purposes, critics see a large potential for abuse. In a document on airport security, the American Civil Liberties Union (ACLU) stated that the organization "does not oppose using biometric identification techniques with a proven record of accuracy, such as iris scans or digital fingerprints, to identify and authenticate persons working in secured areas of airports." However, the ACLU strongly opposes using biometrics for all airline passengers, likening this to "the high-tech equivalent of creating a National ID system", something to which they are vehemently opposed as it would be in direct violation of the Fourth Amendment to the US Constitution, which protects the right to personal privacy. In fact, the US Privacy Act of 1974 limits the rights of federal agencies to collect, use and disclose personal information, such as fingerprints and photographs. However, the act only applies to US citizens and lawful permanent residents, and includes exemptions for law enforcement and national security purposes. The key, according to the

Opponents of biometrics ... argue that the additional security ... does not justify the cost, which is estimated ... to be US \$1.4–2.9 billion for initial implementation, and up to US \$1.5 billion for annual maintenance

ACLU, is balancing security with privacy concerns. For each small increase in security, it might seem worth sacrificing another piece of personal information or increasing public surveillance, but the cumulative effect could be the destruction of privacy.

...all biometric measures can be used for verification, but only those that are unique to a person can be used for identification

Opponents of biometrics also argue that the additional security that the technology might provide does not justify the cost, which is estimated by the US General Accounting Office to be between US \$1.4 and 2.9 billion for initial implementation, and up to US \$1.5 billion for annual maintenance. Biometrics would do little to prevent illegal immigration, as most illegal immigrants avoid any identity checks. And despite government assurances that biometric identification would prevent terrorism, this hardly seems likely. For the most part, governments do not know who the terrorists are, much less have a picture or biometric data for them. Furthermore, US business fears a decrease in the number of tourists and business travellers, and in the money spent by such visitors (*The Economist*, October 18, 2003). Some European diplomats have already indicated that they would choose not to travel to the USA rather than undergo fingerprinting or other invasive immigration procedures (Friedman, 2003).

But the greatest fear with the use of biometrics is the threat of 'function creep'—if the technology is used for something other than its original intent. In particular, the potential to track individuals becomes a reality if governments store biometric data in central databases. Inevitably, public acceptance of biometric technology depends on the public's trust in their government. However, function creep might be a slow process, and not just by governments. The ACLU points to the endemic abuse in the USA of social security numbers, which are routinely requested for identification. Social security numbers are now easily abused in identity theft, which is something that the ACLU believes is inevitable for biometric data. As the history of seemingly safe identification technologies proves, it would be naive to think that biometric data will not eventually be abused.

Caroline Hadley

doi:10.1038/sj.embor.7400085