Parliamentary Office of Science and Technology

postnote

November 2001 Number 165

BIOMETRICS & SECURITY

Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. It has a number of current and potential applications relating to national security and law enforcement, which are considered in this briefing.

The emergency anti-terrorism bill, soon to be presented before Parliament, will include proposals that impact on the collection and sharing of biometric data by police and customs. This gives Parliamentarians the opportunity to discuss issues relating to the use of biometric technology.

Background

A biometric is a measurement of a biological characteristic such as fingerprint, iris pattern, retina image, face or hand geometry; or a behavioural characteristic such as voice, gait or signature. Biometric technology uses these characteristics to identify individuals automatically[1]. Ideally the characteristic should be universally present, unique to the individual, stable over time and easily measurable. No biometric characteristics have been formally proven to be unique, although they are usually sufficiently distinct for practical uses. Different biometrics will be more suitable for different applications depending, for example, on whether the aim is to identify someone with their co-operation or from a distance without their knowledge.

As illustrated in the box opposite, biometrics can be used to answer two principal questions:

- Are you who you claim to be?
- Who are you?

Are you who you claim to be?

Confirming that someone is who they claim to be normally relies on something that they possess, such as a security pass, or something that they know, such as a password. Neither can provide absolute confidence. For example, security passes can be stolen and passwords are sometimes (unwisely) written down. Biometric technology offers an additional level of confidence, but with the disadvantage that, unlike a password, a person's characteristics are not secret and can therefore be copied. To confirm an individual's identity, their biometric is scanned, converted into electronic form and stored either on a card that remains in their possession or in a database. On requesting access to a building or an

Case studies

Are you who you claim to be? *INSPASS hand geometry*

The US Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) has been introduced at eight airports to provide fast immigration processing for authorised frequent flyers entering the US and Canada. On arrival at an airport, a traveller inserts a card that carries a record of their hand geometry into the INSPASS kiosk and places their hand on a biometric reader. A computer cross-references the information stored on the card at registration with the live hand geometry scan. Processing takes less than 30 seconds. If the scans match, the traveller can proceed to customs; if not, travellers are referred to an Immigration Inspector. There are more than 45,000 active INSPASS users with, on average, 20,000 automated immigration inspections conducted each month.

Who are you? *Newham Council face recognition system*

In October 1998, Newham Council introduced face recognition software to 12 town centre cameras with the aim of decreasing street robbery. Images are compared against a police database of ~100 convicted street robbers known to be active in the previous 12 weeks. In August 2001, 527,000 separate faces were detected and operators confirmed 90 matches against the database. Where a face does not match, the image is deleted; if a match is found a human operator checks the result. The introduction of face recognition technology to Newham city centre saw a 34% decrease in street robbery. The system has not led directly to any arrests, which suggests that its effect is largely due to the deterrence/displacement of crime. The face recognition system has been widely publicised by the council and 93% of residents support its introduction.

IT system, the biometric is scanned again and compared with the record to confirm their identity. Where the aim is simply to recognise an individual as someone with permission to use the system, there is no actual need to link the biometric data with any other personal information.

Who are you?
If a database of known individuals has been developed it is possible to answer the question 'who are you?' The biometric of the unknown person is compared against the database in a 'one-to-many' search. Their identity can be determined if their biometric has been entered onto the database on a previous occasion; this is much quicker than a manual system. High quality data are needed if the database searches are to give accurate results.

Applications of biometrics

There is growing interest in the use of biometrics for small-scale security of buildings and IT systems and for use in access/I.D. cards. This brief focuses on current and potential large-scale applications at a national level. These include the Criminal Justice System, immigration and asylum, and port and border security. The collection of fingerprints by the police and immigration service has long been regulated by law. Other biometric technology is regulated by general legislation (see box opposite).

Criminal Justice System

Fingerprinting

At a national level in the UK, automated fingerprinting is the only biometric in general use (see box on NAFIS opposite). An investigative project, to be completed by April 2002, is looking at the concept of using a single biometric identifier, likely to be fingerprints by default, throughout the Criminal Justice System including police, prisons and courts. Prisons already take ink fingerprints from convicted prisoners. These can be compared against the police database as proof that the intended person is being held. An automated system would give rapid confirmation of a person's identity and allow information about individuals to be shared quickly and easily.

Face Recognition

The police photograph everyone charged or convicted of an offence. Digital databases of static photos are already held by some police forces. An option might be to set up a national face recognition database, comparable with NAFIS in that it could carry out searches based on static images taken in police stations.

Face recognition technology could also be used to complement the estimated 1 million CCTV cameras already in operation in the UK, by recognising individuals covertly at a distance. This is a greater technical challenge than the use of static images collected with the knowledge and co-operation of the individual (see box on page 3). Potentially, covert recognition could be used in real time, allowing the instant identification of individuals, or offline, enabling hours of CCTV recordings to be searched quickly and without human fatigue.

Legislation regulating the use of biometrics

General

Data Protection Act 1998

The Act applies to biometric data in the same way as to any other personal data. The eight principles of the Act are that data must be fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate; not kept longer than necessary; processed in accordance with the data subject's rights; secure; and not transferred to countries outside the European Economic Area without adequate protection. The UK has joined an arrangement for the sharing of police data in the EU. In addition, data can be shared with any country in the case of 'substantial public interest'. Exemption from the Act is given where compliance would prejudice national security or crime prevention and detection. A CCTV Code of Practice has been issued under the Act[2], which explains legal requirements and includes guidance on good practice.

Human Rights Act 1998

Article 8 of the Act states that everyone has the right to respect for their private life, which includes the collection and storage of biometric information in some circumstances. Public Authorities may interfere with this right where it is in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, or for the protection of the rights of others.

Fingerprinting

Police and Criminal Evidence Act 1984

Allows the police to take fingerprints without consent when an individual is held at a police station in connection with a recordable offence; and to carry out speculative searches against a fingerprint database. Where individuals were not subsequently convicted their fingerprints were destroyed.

Criminal Justice and Police Act 2001

Allows the police, for the first time, to keep all recorded fingerprints, including where the individual is not subsequently convicted of a crime. Also allows the police to retake fingerprints to improve the quality of their records.

Immigration and Asylum Act 1999

Allows fingerprints to be taken from anyone claiming asylum and certain other categories. These currently must be destroyed when the individual is given indefinite leave to enter or remain in the UK; or in any case after 10 years. Also allows the immigration service to share these data with the police and other law enforcement agencies in relation to offences committed under the Act.

National Automated Fingerprint Identification System (NAFIS)

In March 2001 rollout of the National Automated Fingerprint Identification System (NAFIS) to all 42 Fingerprint Bureaux of England and Wales was completed. The system was introduced at a cost of £90m over 5 years. NAFIS contains approximately 4.6 million full sets of fingerprints and can be added to or searched by the local Fingerprint Bureau attached to each police force. This decentralisation gives a significant time saving over the previous system where all records were held at New Scotland Yard. 15 out of 43 forces are already able to take live fingerprint scans, which capture electronic data directly from individuals and enable rapid searches to be carried out against the database. NAFIS is used both to record fingerprint data from convicted criminals and to identify suspects from samples taken from crime scenes. It is linked to the Police National Computer, which stores criminal records.

Face recognition technology
Under tightly controlled conditions, face recognition systems can now achieve accuracy levels of 95%. However, in the real world, factors such as movement, lighting and camera angle, make it difficult to capture facial images that can be interpreted by the software. In addition, the effects of ageing and accessories such as dark glasses make finding a match against a previously stored image difficult. Where it is possible to control lighting levels and to engineer situations whereby people can be seen in a proper position by the camera, the technology may perform better. With this in mind, Oakland International Airport in the US has recently announced trials of face recognition technology in interrogation rooms. Images will be compared against a database of known criminals.

Immigration and asylum

Although biometrics are not currently used for general immigration purposes it may be possible for both visas and passports to carry biometric identifiers as a way of reducing the use of fraudulent documents, improving security, or tracking people's overseas travel.

In relation to asylum applicants, the Immigration and Asylum Fingerprint System (IAFS) has been used by the immigration service since spring 2001. A full set of fingerprints is recorded from all applicants, aimed at the detection of multiple applications and benefit fraud. Small-scale evaluation has shown this automated system to be achieving 98% accuracy prior to expert verification. Immigration enforcement officers are equipped with portable scanning units from which they can transmit data through their mobile phones, allowing an immediate check to be made of an individual's identity. The law allows for these data to be shared with certain other agencies for immigration related offences only (see box on legislation on page 2).

From spring 2002 all new asylum applicants will receive a card carrying their fingerprint biometric in place of the standard acknowledgement letter, which is expected to prevent document fraud. The Dublin Convention[3] states that asylum may be claimed only in one EU state. A central EU database of fingerprints from all asylum seekers ('Eurodac') is being established to support this and is expected to become operational during 2002.

Port and border security

The areas where biometrics could be used include:

- Confirming that a passenger boarding a plane is the same individual who checked in. Passengers would be asked to agree to a biometric scan at check-in and again at the gate.
- Providing rapid approval to anyone with immigration clearance, freeing up resources to focus on other travellers. The INSPASS system in the US is an example of this (see Case studies box on page 1), although high maintenance costs have meant few savings in this case.
- Controlling access to restricted areas. This would apply to staff, who would gain access to buildings either through demonstrating that they matched the biometric stored on their card or through comparison with a database.
- Identifying known terrorists or criminals. Biometrics would be scanned from people passing through airports and compared with a database of known criminals or terrorists. Canada has recently announced plans to identify high-risk passengers (the criteria have not yet been defined) at border crossings and airports. Fingerprint scans from these people will be compared against the Canadian national database and shared with international agencies.
- Gathering intelligence on people's travel patterns. This would involve scanning and storing biometrics from all individuals passing through airports. Patterns of travel, particularly if compared internationally, could reveal useful intelligence information. Application on this scale would be likely to raise privacy concerns and may contravene the Data Protection and Human Rights Acts (see box on legislation on page 2).

Issues

Accuracy and other technical issues

The UK Biometrics Working Group[4], established in 1999 under the aegis of the Office of the e-Envoy, is leading international work on agreeing criteria for evaluating the performance of biometric systems, vital if the technology and data are to be shared internationally. While high accuracy may be achieved under test conditions, in practice factors such as greasy fingers on fingerprint scanners or the effect of variable lighting on face recognition cameras have a significant effect on performance. In addition, access for people with disabilities needs to be considered, together with the willingness of individuals to offer their biometric. This is may be a particular issue with iris and retina scans, which could be perceived to carry a health risk.

The key performance measure is the rate at which a system makes mistakes. A bank would not want genuine customers to be refused service at an ATM and an airport would not want to allow a suspected terrorist onto a plane; but no system is perfect. The acceptable rate of errors will depend on the application but becomes a particular concern where large numbers of individuals are involved. For a system to add value over existing manual processes it is essential to specify the acceptable level of errors before implementation. For example, 63 million passengers travel through Heathrow each year. If fingerprint scans offering 98% accuracy were introduced there would be over 1 million errors each year; with 99.9% accuracy there would be 63,000 errors - more than 1000 every week. At this level of accuracy, security staff and passengers may lose confidence in the system and not co-operate with its implementation.

If a database of biometrics were to be developed the accuracy of the information would need to be verified. Concerns raised over the accuracy of data held by the Police National Computer[5] have led to measures aimed at ensuring that data are accurately and promptly recorded, and regularly reviewed and updated. The same applies to biometric databases. For example, poor

quality biometric scans could lead to errors in identification and ageing may mean that face scans become out of date.

Fraud and identity theft
It is has been suggested that the use of biometrics could significantly decrease fraud, whether relating to social security benefits or 'stolen' identities. On the other hand, it is likely that fraudulent biometric identities could be developed, creating a new threat and posing a new challenge for law enforcers. Creating a biometric identity could involve either stealing electronic data files, or creating a physical replica (e.g. contact lenses etched with a false iris image).

A detailed risk analysis examining each known point at which electronically stored data could be compromised would be necessary to allow a secure biometric database to be maintained, and this needs to be built into the costing for any system. One risk factor worth noting is that 70% of cases of data theft involve current or former employees.

It is more difficult to prevent the replication of biometric features – after all, we leave our fingerprints behind on everything we touch. Manufacturers are looking for ways to protect systems. For example, to thwart the use of replicas, some fingerprint scanners claim to accept readings only from warm fingers.

Privacy
Human rights groups such as Liberty suggest that where biometrics are used, and seen to be used, for a clearly defined and stated purpose, the technology will be more acceptable to the general public. There are, however, concerns over 'function creep', where biometric information collected for one purpose could subsequently be used more widely with the individual losing control over their personal information.

For example, if biometrics were to be used to track passengers from check-in to the gate there is no need to retain any data beyond that point, or even to relate their biometric data to any personal information at all. However, the retention of personal and biometric data could provide intelligence on people's movements and identify passengers of interest to the authorities. The former may be quite acceptable to many people, but fears of the latter and the association with 'Big Brother' may make them feel less comfortable with voluntarily offering biometric scans.

A similar concern may arise over the potential for data sharing between agencies. The collation of private information from different sources could enable conclusions to be drawn that go far beyond the original purpose of the data collection. A question then arises over whether it is acceptable to share the data from selected groups of people and how such groups would be defined. Is it acceptable to subject anyone on the police fingerprint database (NAFIS) to a greater level of surveillance than others in the population? What would the criteria be for drawing up a more defined list of, say, suspected terrorists?

Lastly, concerns may arise over the possibility that people's biometrics could be used for wider purposes without their consent. For example, a retina scan could reveal if someone is susceptible to stroke; unlikely to be something that an individual would want their employer or insurance company to know. Similarly, technological advances may enable DNA profiling to be carried out automatically, and with it the possibility of deducing a range of genetically determined information about individuals. While the Forensic Science Service holds a database of over 1.3 million DNA samples, currently they are not allowed to investigate the genetic characteristics of identified individuals. However, samples from crime scenes can, and increasingly will, be used to provide intelligence for the police on crime suspects.

Overview
Biometric technology has the potential to deliver widespread automatic identification of individuals by measuring particular characteristics. However, when considering whether a biometric system could add significant benefit over alternative strategies, the performance of the technology in the field, social and financial factors would need to be examined.

To maximise the benefit of biometric technology to intelligence operations a large amount of information, on a large number of people, collected over a long period of time would be needed. This raises civil liberties issues. To address these, clear criteria defining whose data can be collected, for what purpose, how long it can be retained and who has access to it, need to be followed.

The Data Protection Act, where enforced, does give clear requirements for the conditions under which it is acceptable to collect, store and use personal data. However, while limited exemption is available where compliance would prejudice national security or crime prevention and detection, adherence to the principles of the Act would seem desirable.

Endnotes
1 DNA analysis cannot currently be carried out automatically and so is not classified as a biometric.
2 CCTV code of practice: www.dataprotection.gov.uk/dpr/dpdoc.nsf
3 The Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, Dublin 1990.
4 UK Biometrics Working Group: www.cesg.gov.uk/technology/biometrics/index.htm
5 'Phoenix Data Quality' Police Research Group 1998; 'On the record' HMI of Constabulary 2000.

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of public policy issues that have a basis in science and technology.

The Parliamentary Office of Science and Technology, 7 Millbank, London SW1P 3JA Tel 020 7219 2840

www.parliament.uk/post/home.htm