

THE IRISH COUNCIL FOR

BIOETHICS

COMHAIRLE BITHEITICE NA HÉIREANN

Irish Council for Bioethics



BIOMETRICS:
Enhancing Security or Invading Privacy?

PASIEKA / SCIENCE PHOTO LIBRARY

Q1 What are biometrics?

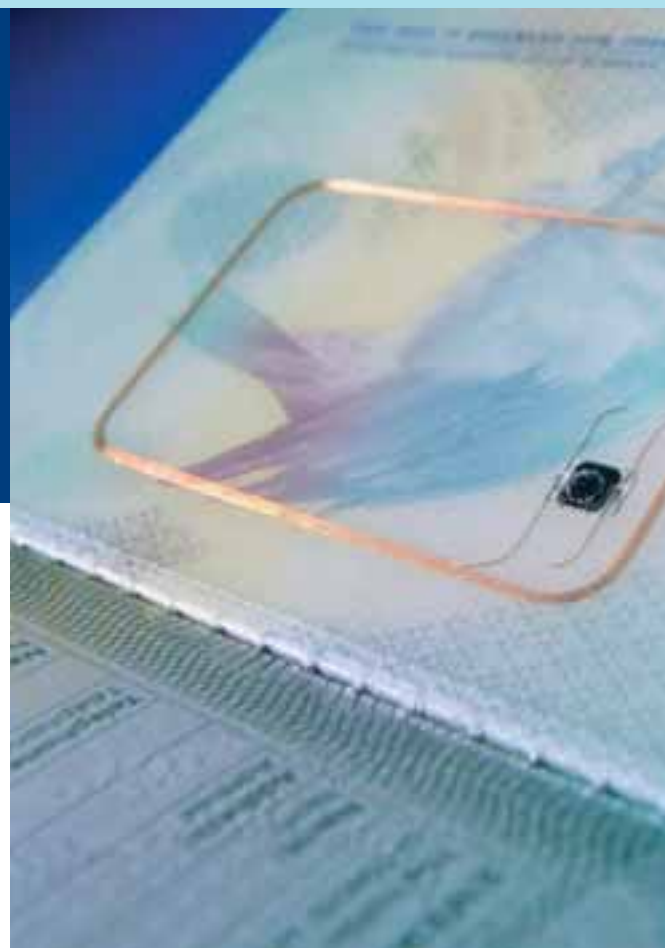
A biometric is any physical or biological feature that can be measured and used for the purpose of identification. Features can be either physiological e.g. fingerprint, hand geometry (shape), the face, the iris, the retina or behavioural e.g. voice pattern and gait (way of walking).

Q2 For what purposes are biometrics used?

Some biometric features, like fingerprints are considered to be unique to each individual and, in general, biometrics, such as iris pattern and hand geometry are believed not to significantly change with age. This makes them very useful for identification purposes. As a result, biometrics are used to confirm that individuals are who they say they are, to help identify unknown people or to screen people against a specific watchlist, such as a criminal database.

In response to terrorist and criminal activity, biometrics have been introduced with the aim of improving national security. Biometrics have also been introduced, in order to deal with the migration of millions of people between countries both legally and illegally. For instance, the European Union (EU) EURODAC system was set up to combat the flow of illegal immigrants into Member States. EURODAC is a central European database of fingerprints, which allows a Member State to check whether asylum seekers have previously sought asylum from another European country or whether they have tried to enter the EU illegally. In the US the Visitor and Immigrant Status Indicator Technology (US VISIT) Programme was started following the events of September 11th 2001. Under this system all visitors to the US must have both their index fingers scanned and have their photo taken. This information is then checked against a database of known criminals and suspected terrorists.

Apart from national security, biometrics are also used for several other purposes, such as security and surveillance, law enforcement, e-Commerce (buying and selling online), e-Government (electronic communication between governments and citizens) as well as gaining physical and electronic access to buildings or computer files. Biometrics are also being promoted as a possible solution to identity theft and fraud and are increasingly being used by banks and other commercial organisations to correctly confirm the identity of their customers. (For a list of biometric applications see Table 1).



STEVE HORRELL / SCIENCE PHOTO LIBRARY

TABLE 1

Application	Function
Time and Attendance	Individual institutions e.g. schools and employers use this system to record attendance and to control who has access to buildings or areas.
Pay By Touch	A commercial tool in the US, which allows consumers to pay for products in supermarkets and pharmacies by scanning their fingerprints and punching in a personal identification number (PIN), which is linked to their credit or debit cards.
Voice Recognition	Software used in telephone banking to create a profile of how a person's voice should sound regardless of what is being said.
Machine Readable Passports	These include a small chip storing a digital version of the passport photo as well as other information relating to name, address, date of birth etc. Passports can be used along with face recognition software to confirm the passport holder's identity.
Radio Frequency Identification (RFID)	This involves the same technology as that used for machine readable passports. Microchips are implanted in order to track goods, identify pets, and keep track of people e.g. nursing home residents or employees.
Iris Recognition	Provides a method of accessing secure areas e.g. border control and, in some airlines, allows pilots access to aeroplane cockpits.

Q3 How are biometrics collected?

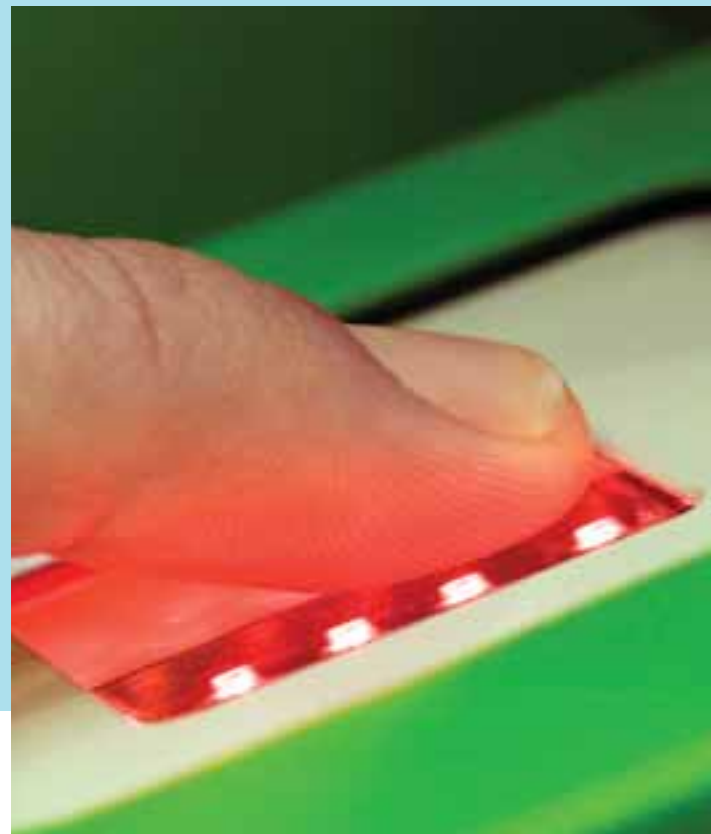
In general, biometrics are collected using sensors e.g. cameras (face recognition), telephones (voice recognition) and fingerprint scanners. People have to enrol before they can use biometric systems. Enrolment involves a copy of a person's biometric feature being taken, converted into a digital format and stored on an electronic database. For example, in the case of a system that uses fingerprints to grant access to a building, a person would have to have his/her fingerprints taken by a sensor and recorded so that s/he can be recognised in the future. The next time the individual presents his/her fingerprint to the sensor this data is compared to the stored copy (also known as a template) using a mathematical formula. If the templates match the individual is granted access.

Q4 How accurate are biometrics?

While biometrics are said to have many benefits for society, it should be noted that these new technologies are not 100% accurate or secure. For example, some biometrics, such as hand geometry or gait are not totally unique to each individual, therefore, their use is limited to small scale systems e.g. a small business might use hand geometry to grant employees access to a building or to monitor employee time and attendance. In addition, while fingerprints are considered to be unique, they can become damaged, which can cause problems with fingerprint scanning systems. Indeed, even if machines are functioning optimally, human error can result in inaccurate data being collected.

Opponents of biometrics have raised concerns about the ability of people to outwit biometric technologies, a practice known as "spoofing". For example, spoofing might involve using fake fingers and fingerprints or contact lenses to fool biometric sensors. However, proponents argue that improvements to the technology such as "liveness" detection e.g. detecting the oxygen levels in the blood in fingers or muscle movement in the iris, thereby indicating a person is alive, help to reduce the likelihood of spoofing. They also state that human supervision of biometric systems e.g. by airport security or border control officials will help to establish that the biometric used really does belong to the person trying to use the system.

Multimodal biometric systems combine a number of biometrics to identify people e.g. fingerprint and facial recognition, which may need to be presented in sequence, at the same time or alternately. Proponents argue that using a combination of biometric identifiers can reduce the potential for spoofing systems, therefore



JAMES KING-HOLMES / SCIENCE PHOTO LIBRARY

making them more secure. They also argue that multimodal biometrics can provide an opportunity for individuals who cannot enrol with one particular biometric feature e.g. due to disability, to enrol using alternative features.

Q5 Are there any health risks related to using biometric technologies?

Concerns have been raised regarding the possible health risks of biometrics. Opponents argue that there is a possibility of eye damage arising from the use of iris scanning equipment. It should be noted that, to date, there have been no reported injuries from using iris scanners. Opponents of biometrics also express unease regarding the cleanliness of the sensors used, stating that participants may feel uncomfortable about touching a hand-geometry scanner or placing their face against an iris-scanner after other people have done so. Proponents of biometrics, on the other hand, claim that safety concerns are unfounded and declare that, for instance, hand-geometry scanners are no more unhygienic than a door handle. In addition, they state that hygiene mechanisms, such as regular cleaning or sterilisation of sensors should invalidate such concerns. Furthermore, proponents argue that the introduction of remote scanning (scanning from a distance) will mean that it will not be necessary to actually touch some types of sensors in order to be identified.

Q6 Are biometrics a threat to privacy?

The right to privacy i.e. our right to control access to ourselves and to our personal information is protected by the Irish Constitution. However, this right is not absolute and may be overridden in the interest of society and community safety, as in the case of terrorism or a national emergency e.g. the outbreak of a contagious disease, such as human avian influenza (bird flu).

Opponents of biometrics have raised concerns regarding the way in which personal information is obtained, stored, compared with watchlists, and possibly linked to other information about an individual. Critics argue that because biometrics are strongly linked to a person's identity and cannot be changed or reissued in the same way as a password or PIN, there is a serious threat to privacy if such information were to get into the wrong hands. Opponents also state that, depending on the biometric identifier used, additional information can be discovered e.g. iris scans can indicate alcohol and drug use and facial biometrics can reveal information, such as sex, age and race. They also express unease regarding the possible use of DNA as a biometric identifier beyond its current use in criminal investigations, which could potentially provide genetic and medical information about an individual and result in their being discriminated against.

Concerns have also been raised that the use of personal information could gradually expand and information could be transferred to third parties with or without a person's knowledge. This phenomenon is known as "function creep". Opponents express unease regarding the risks associated with function creep, where

information might be used in ways that were not originally intended e.g. marketing or for deciding whether somebody should be offered a job. Opponents also raise concerns in relation to how access to biometric databases will be controlled, and the possibility of unauthorised third parties hacking into systems in order to obtain an individual's personal information.

However, proponents of the technology argue that a lot of personal information can already be collected legally from everyday activities, which can provide information about a person's interests and background and that biometrics pose no greater threat. For example, details of the phone numbers a person calls can be stored, banking and credit card transactions can be tracked, library records can be documented and even a supermarket/shop loyalty card can keep track of an individual's purchases.

Furthermore, proponents argue that using biometrics will enhance privacy and protect personal information from unwanted intrusion. They state that, privacy can be maintained in some instances, by storing biometric information on a smart card, which is carried by an individual as opposed to being held on a central database; by using encryption (putting data into a secret code so it is unreadable by unauthorised people) or by storing biometric templates in a separate database to the database storing personal information e.g. name, address and date of birth.

Q7 Is consent necessary for participation in a biometric system?

In order to protect individual autonomy i.e. one's ability to make independent choices without any external influences, it has been argued that participation in biometric programmes should be optional. However, this freedom of choice is not always guaranteed e.g. as part of the UK's biometric immigration system, an individual coming from outside the EU wishing to obtain a visa must provide 10 fingerprints and have his/her photo taken. In this case, while the system at first appears optional and individuals are asked for their consent, failing to give it effectively means that they will be unable to obtain a visa to travel to the UK. Opponents

of biometric technologies state that those individuals who are unwilling to provide biometric data should be given an alternative method of providing the required identification information.

Opponents of biometrics have also expressed unease regarding the use of biometrics for identification purposes without the consent of individuals, an issue that may arise more with the increasing use of remote scanning. They argue that given the personal nature of biometric information, and its association with an individual's identity, consent should always be obtained.

Proponents, on the other hand, argue that consent is not always necessary and that in some instances protecting the greater good of society should outweigh individual autonomy e.g. in the case of illegal immigration or international terrorism.

Q8 Will biometric technologies lead to discrimination?

Opponents have raised concerns that some of the information collected from biometric systems could be used in profiling and categorising people, potentially leading to the discrimination of certain groups or individuals. From a security point of view, proponents argue that the use of such profiling techniques has been successful in preventing potential terrorist attacks. However, opponents point out that the presence of biometric security measures will not necessarily prevent future terrorist attacks. For instance, a number of the terrorists involved in the attacks on September 11th 2001 travelled to the US using their own passports and held valid visas.

Q9 Is the introduction of biometrics a proportionate response to possible security threats?

While biometrics are expensive and are less than 100% accurate, many governments believe that the benefits of biometric systems, in terms of national security, greatly outweigh any risks to privacy or health and have decided to introduce a number of programmes e.g. biometric passports, immigration programmes and national security systems. Similarly, biometrics have begun to appear in smaller settings, for instance, there are a number of examples in Ireland and abroad where institutions e.g. schools and employers have introduced biometric systems in order to record the time and attendance of pupils and staff and some commercial organisations are using biometrics to confirm their customers' identities. Proponents argue that biometric programmes increase security and efficiency and provide greater convenience and peace of mind to consumers.

Opponents of biometrics, however, argue that a "Big Brother" style society will be the inevitable consequence of the increased use of biometric technologies, enhanced surveillance methods and increasingly connected databases. They also raise concerns regarding the appropriateness of introducing expensive, technically complex biometric systems to achieve goals that could potentially be achieved in other ways.

Similar arguments have been made regarding the storage of large amounts of personal and biometric information in central databases, given the potential risks of unauthorised access or the loss of important and sensitive personal records. The potential for such risks was highlighted in the UK, when in 2007 discs containing the personal records of 25 million individuals, including their dates of birth, addresses, bank accounts and national insurance numbers were lost in the post.



CONEYL JAY / SCIENCE PHOTO LIBRARY



The Irish Council for Bioethics
Regus House, Block 4,
Harcourt Centre, Harcourt Road, Dublin 2.

E-mail: info@bioethics.ie