

BIOMETRIC IDENTIFICATION TECHNOLOGY ETHICS

© CSSS Policy Brief N° 1/ 03 – November 2003

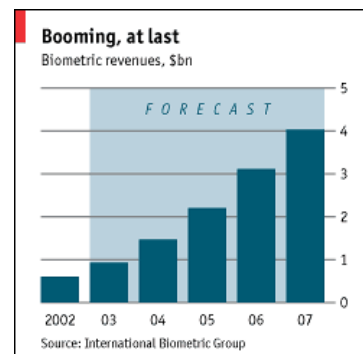
"Early in the 21st Century, the Tyrell Corporation advanced robot evolution into the NEXUS phase - a being virtually identical to a human - known as a Replicant. Replicants were used Off-world as slave labour, in the hazardous exploration and colonization of other planets. After a bloody mutiny, Replicants were declared illegal on earth - under penalty of death. Special police squads - BLADE RUNNER UNITS - had orders to shoot to kill, upon detection, any trespassing Replicant.



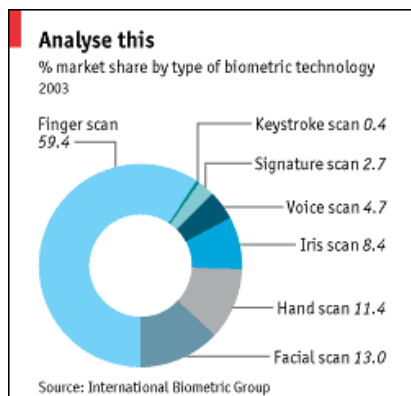
After a bloody mutiny, Replicants were declared illegal on earth - under penalty of death. Special police squads - BLADE RUNNER UNITS - had orders to shoot to kill, upon detection, any trespassing Replicant.

Replicants can be identified only by using the Voight Kampff Machine, which analyzes the iris contractions and dilatations..."

This is the initial plot of "Blade Runner", a science fiction film that became the cult movie of the 80's and is still a cornerstone of sociological science fiction. The machine that allows to identify the Replicants is a biometric devise. Biometric technologies can be defined as automated methods of recognizing or verifying the identity of a living person based on a physiological or behavioural characteristic. No longer a science fiction solution, biometric technologies are the most important innovation in the IT industry for the next few years and the biometric industry is projected to grow from \$600 million in 2002 to \$4 billion by 2007 (Table 1).



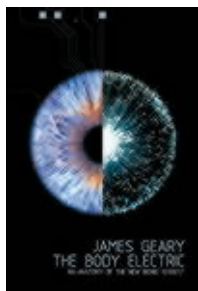
Biometric Identifications Systems consist of a reader or scanning device, software that converts the scanned information into digital form, and, wherever the data is to be analysed, a database that stores the biometric data for comparison with entered biometric data. Emerging biometrical methods of identification include fingerprints, retinal and iris scans, hand geometry, facial feature recognition, ear shape, body odour, brain fingerprinting, signature dynamics, voice verification, and computer keystroke dynamics (Table 2). Biometric products have been commercially available since 1968, but commercial use of biometrics has become unexceptional only in the last few years. Early Biometric Identification Technology was considered extremely expensive. However, due to constant developments in computer technology and reduction in prices, along with improvements in accuracy, biometrics have begun to see widespread deployment. For example, a fingerprint scanner



computer technology and reduction in prices, along with improvements in accuracy, biometrics have begun to see widespread deployment. For example, a fingerprint scanner

that cost \$3,000 five years ago, with software included, and \$500 two years ago, costs \$100 today. As a result, biometric systems are being developed in many countries for such purposes as social security entitlement, payments, immigration control and election management¹.

Even technical surveillance-related responses to September 11 have been largely based on biometrics. CCTV cameras in public places have been enhanced – as in Newham, south London - with facial recognition capacities. Iris-scan at airports - now



installed at Schipol, Amsterdam - is being implemented elsewhere in Europe and North America as well. The concept of biometric passports - in which the digital image of a person's face is stored in a microchip - had gathered steam. The demand for the introduction of harmonised biometric data (e.g.: fingerprints, DNA or iris scans) has been led by the US who have been backed by the UK. Biometric data will be included on UK passports from 2006 embedded in a microchip - which may contain other unspecified data. The EU has backed the allocation 140 million euros to developing controls at borders and of databases including biometric identifiers." (COMMISSION OF THE EUROPEAN COMMUNITIES Brussels, 24.09.2003)².

As biometric becomes important, also its medical implications are becoming critical. In its final report the SIBIS project – funded in the "Information Society Programme" of the European Commission (SIBIS, 2003) - has identified some crucial issues in medical biometric applications such as confidentiality, reliability and effectiveness. According to a comprehensive European Commission funded study (BIOVISION, 2003) biomedical implications of biometrics are both direct and indirect: « A clear assessment of the medical issues should pre-empt these concerns, so that, for example, reluctance to use certain sensors is not easily justified on hygiene fears [...] These considerations are termed the direct medical implications of the application of biometrics and their impact should be examined for those systems that are likely to be most widely used. There is another class of medical concern, termed indirect medical implication, where physical or mental characteristics or conditions might be deducible from biometric measurements ». Biometrics may affect biomedicine at least in three senses:

1) **Applications for security purposes and to restrain access to sensitive data** - Security issues are becoming more and more relevant to the health system. It is enough to think of the need to restrain dual use technologies (i.e., technologies that can be used to produce both drugs and bioweapons), to improve secure communication and information

¹ Nearly every major credit card supplier, such as VISA and Mastercard, are developing biometrics as a means to reduce fraud and help prevent stolen identity. Some automotive manufacturers already offer biometrics for added security and convenience on vehicles. In Illinois Inmates must submit to retinal scanning, coming and going from jail to court appearances. A French primary school has introduced an iris scanning system with the capacity to scan children as they selected items at the school canteen and electronically debited their account. In the private sector, Lotus employees pass through a hand-geometry scanner to pick up their children from in-house day care. Coca-Cola is using hand geometry at the time clock to prevent workers from "buddy punching" a late colleague's time card. Microsoft has announced plans to use a fingerprint-based biometric ID system with their new Windows software.

² The Commission proposals provide for the mandatory storage of the facial image as a primary biometric identifier in order to ensure interoperability. A secondary biometric identifier should be added, which should be the fingerprint, as it provides the best solution for so-called "background checks", the identification in databases. The Commission's intention is to bring forward the final date for the implementation of the photograph from 2007 to 2005 and at the same time, require Member States to integrate biometric identifiers into the visa and the residence permit for third country nationals in a harmonised way, thus ensuring interoperability.

exchange between healthcare service providers and networks (e.g., in clinical trials, in transborder networks such as organ exchange organisations, etc.), to limit physical access to buildings and hospital wards, and to authenticate medical and social support personnel. Also applications to restrain access to sensitive data are vital. As electronic medical records are extensively used, they are likely to be protected by biometric identifiers. Safe identifiers are also requested to control access to medical databanks (genetic, tissue, etc.) and many hospitals and healthcare organizations are already deploying biometric security architecture to ensure the trust of patients. If it becomes common to use biometric identifiers, there will be a tendency to centralise in the same bank (or in interconnected banks) biometric, medical, economic, legal data. Data matching (the process of linking systems, by a biometric or another one identifier) and "interoperability" of information systems provoke many ethical concerns (Clarke R, 1994). In particular they arise when biometrics are used beyond their original purpose, without the informed and voluntary consent of the participants (the so-called "function creep").

2) Applications to avoid illicit use of social welfare and medical support - The need to administrate scarce resources in social and medical care makes crucial to avoid illicit use of social welfare and medical support. Departments in charge of social assistance in countries like the USA, Canada, Spain and the Netherlands are launching programmes for detecting and preventing duplicate benefits. This is a kind of fraud that involves the collection of more benefits than one is entitled to, by entering the program under two or more identities. A wide consensus appears to exist concerning the high levels of this type of fraud, and hence concerning the urgency of the need for new identification practices. It is claimed that the introduction of biometrics would result in billions of savings on public spending. Also unauthorized use in assistance programmes (e.g., heroin addicts who participate in methadone maintenance plans) could be tackled by using biometric identifiers. Most groups targeted by biometric identifiers are made up by people who are not able to identify themselves (e.g., infants, dementing elderly, incapacitated patients) or other vulnerable groups (e.g., disabled persons, drug abusers, migrants and mobile populations). They are critical populations from an ethical point view because they are unable or less able to give an informed consent.

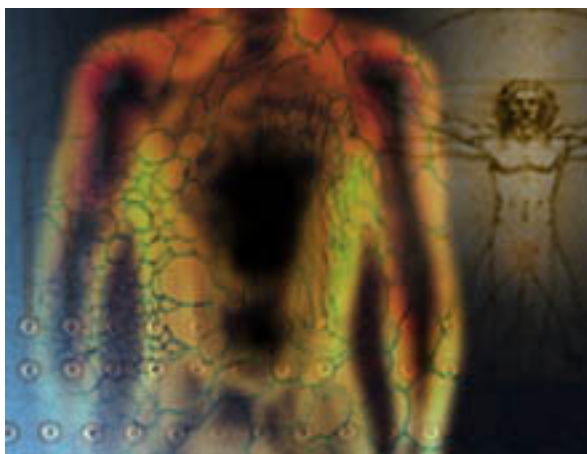


3) Biometrics as a potential source of biomedical information about an individual - The "living issue" is an important issue in biometrics. Biometric identification could be fooled by a latex finger, a prosthetic eye, a plaster hand, or a DAT voice recording. Biometric devices must therefore be able to determine whether there is a live characteristic being presented. For example, fingerprint sensors might incorporate pulse oximeter technology, and iris scanners might test for pupillary response. By monitoring "living characteristics" biometric devices become a source of sensitive biomedical data; e.g., pupillary responses depend on whether one has been drinking or taking drugs, whether the person is pregnant, and with the variabilities of age in general; changes in blood flow are typically associated with several medical conditions as well as with emotional responses. There are ways in which you might be able to sense the emotional attitudes from some biometrics, e.g. nervousness in a voice pattern and anger from a facial image. There has been some exploratory work in this area. Moreover recent scientific research suggests that biometric features can *per se* disclose medical information. Certain chromosomal disorders – such as Down's syndrome, Turner's



syndrome, and Klinefelter's syndrome - are known to be associated with characteristic fingerprint patterns in a person. Knowing that certain medical disorders are associated with specific biometric patterns, researchers might actively investigate such questions as, can biometric patterns be linked to behavioral characteristics, or predispositions to medical conditions? If these questions are answered affirmatively, biometrics might become not only an identifier, but also a source of information about an individual. Finally also future and likely use of genetic test information and DNA profiles in biometrics bear many risks of discrimination and the multiplication of compulsory testing procedures.

The number of biometric devices in use in Europe has jumped from 8,550 in 1996 to more than to 50,000 in 2001 and biometric industries revenues are expected to more than triple in the next two years. "Biometrics seem headed for dramatic growth in the next few years. But calm, public discussion of their benefits and drawbacks has been lamentably lacking" (The Economist, *Prepare to be scanned*, Monday December 8th 2003). Biometrics, by their very nature, may compromise privacy in a deep and thorough fashion. In 1999 the



International Biometric Industries Association (IBIA) issued their "Statement of Principles and Code of Ethics". The IBIA states: "IBIA Members believe that biometric technologies should be used solely for legal, ethical, and non-discriminatory purposes. They are therefore committed to the highest standards of systems integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law in all biometric applications" (Mintie D, 1999). The most significant privacy concerns raised by biometrics relate to the threat of function creep.

Function creep, or mission creep, is the process by which the original purpose for obtaining the information is widened to include purposes other than the one originally stated (Davies S, 1994). Obtaining medical information from biometric identification is an emblematic example of "function creep". It seems likely that as biometrics become more pervasive, the research community will begin to determine whether these measures can reveal more about a person than only his identity. For instance, by comparing selected biometric data captured during initial enrolment and subsequent entries with the current data, biometric technologies may detect several medical conditions.

There is thus a crucial need to initiate a public debate on ethical and policy aspects of emerging biometrics. The CSSC aims to promote international - European and transEuropean - dialogue on bioethics of biometric identification technologies, and to identify points of agreement and disagreement. In the long term, we want to contribute to promote innovative strategies and collaborative research in this field.