ETHICAL PRACTICE IN THE USE OF BIOMETRIC IDENTIFIERS WITHIN THE EU

ANNEMARIE SPROKKEREEF AND PAUL DE HERT

1Tilburg Institute for Law, Technology and Society (TILT), Tilburg University and Center for Law, Science, Technology and Society Studies, Free University Brussels
2Tilburg Institute for Law, Technology and Society (TILT), Tilburg University and Institute for Communications Studies (ICS), Leeds University

Contact: a.c.j.sprokkereef@uvt.nl and paul.de.hert@uvt.nl, TILT, Faculty of Law, Warandelaan 2, 5000 LE Tilburg, NL

ABSTRACT

Ethical issues surrounding the actual and proposed use of biometric identifiers within the EU are identified. The paper starts by defining biometric technology and biometric identification. This is followed by some examples of biometric identifiers presently used in private applications across the world. These examples lead to consideration of some of the ethical problems likely to be encountered when public authorities start using biometrics in travel documents and databases. A brief exploration of current EU policy initiatives involving biometric identifiers is then undertaken to indicate the scope of the problem. A number of ethical issues surrounding the use of biometrics will be articulated, and an assessment will be made of whether the norms and standards applied to the use of biometric identifiers are appropriate. It is concluded that the application of biometric technology should be consistent, justified and linked to appropriate protections.

INTRODUCTION

Modern biometric technologies identify individuals by means of the body, making use of individual body characteristics for identification or authentication purposes. The impact of the use of biometric technologies is still unclear, but there are expectations that some biometric applications will meet public resistance. In the field of law, biometrics is burdened by historical precedent. In general, biometrics tends to be associated with stigmatisation as a result of the long standing use of fingerprints to identify criminals. It also raises concerns over loss of privacy and rights.¹ In addition, for continental criminal lawyers, some aspects of biometric technology also bring back memories of biological determinism pioneered by Cesare Lombroso (1835-1909). Lombroso was not, of course, interested in using biometrics for identification or verification, but in proving
that criminals had particular *physiognomic* attributes or deformities (Lombroso, 1876). He held that it was possible to determine character and personality traits from the physical characteristics of the face or the body, and concluded after several studies involving criminals in Italy that skull and facial features were clues to genetic criminality (Lombroso, 1876). Although his ideas have been fiercely opposed and subsequently dismissed, the idea of physical features and social conditions determining human behaviour has recently been revived. This rehabilitation of causality between physical features and behaviour coincides with technological developments in the area of biometrics. Very recently, a research group in Sweden published some preliminary findings in a study on iris scans.² It was found that in a first analysis of large groups of people, associations could be found between iris characteristics and personality in adulthood.³

Thus, a number of negative undertones are playing a role in the development and deployment of biometric identification and authentication methods. In addition, some observers have articulated fundamental objections to the use of the body for government administration or law enforcement objectives. They have argued individuals have an absolute right to control the creation and use of biometric images of themselves (Alterman, 1999). It has, also, been held that authorities are falling short of developing an adequate data protection regime, and tend to underestimate possible serious effects on individuals, such as biometric identity theft.⁴ Equally, there are human rights concerns about potential direct and tangible negative impacts of biometric technology on citizens. All in all, a range of complex and interconnected issues must be addressed in decisions about the use of biometric technology.⁵ In this paper the ethics surrounding the use of biometrics, the choice of biometric identifiers and biometric applications is assessed.

**BIOMETRICS AND THE LAW**

The use of biometrics is attractive because of the appearance of ‘an anchor’ for identity in the human body, to which data and information can be linked.⁶ The biometric identifier becomes the gateway to all data held on a person as the body provides a constant and accessible link between record and individual. Biometric identification indeed permits matches between a “live” digital image of the body and a previously recorded image of the same part, which is usually indexed to personal information. In most cases, the data will be computerised and stored for future use. Biometric identifiers can be based on measurements of physical attributes (iris scan, fingerprints, hand geometry), but also on measurements of behavioural characteristics (voice recognition) or on
recognition of facial or other features (digital face scan). These forms of biometric identification are regarded more reliable and potentially faster than visual comparison of, for example, signatures or photo IDs. In the current state of the art, however, many of these forms of biometric identification are not sufficiently reliable to be used on a large scale. The fingerprint, face scan and iris scan have so far proved to be most successful, and indeed have been introduced in many commercial applications across the world and increasingly also in Europe. American examples of private schemes include biometric systems for the purpose of monitoring employees’ working time. Such private schemes are also in use to allow for more efficient entry at facilities such as at World Disney. Another segment of the American commercial market is the hotel and catering industry with its (night) club membership schemes and restaurant booking systems involving biometrics. Less voluntary, but still private are, for example, the face scan and fingerprint scans operational at some American universities as a requirement for sitting graduate record exams.

In Europe, commercial applications are now widespread, many of them private membership schemes, for example, nightclubs or bank access facilities. Three Co-op supermarkets in Oxfordshire are currently running a pilot-scheme for registered clients who can pay their groceries through a pay by touch (fingerprint) system. More significantly, in many settings across Europe, systems are being tested that could develop into voluntary semi-public schemes. An example of the latter are the pilots for football supporter access to stadiums or the Privium airport security system at Schiphol airport. In some pilots participation is not voluntary. A pilot project by car rental companies and Essex police at Stansted required customers to provide their fingerprints, and if they failed to oblige they could not rent a car at the airport. Biometric data collected were kept by the rental company, but handed over to police when the car was stolen or used for another crime. Some customers felt that the measure was disproportionate, intimidating, or an invasion of their privacy.

Governments themselves are increasingly starting up projects that make use of biometrics. Faced with ever more cross border movements, fears of terrorism and serious crime, many States are in search of reliable methods to conduct clean and simple controls that can be carried out with a minimum of human error. Solutions to this demand have been found in applications that combine biometric technology with computer data applications. These make searches and checks, which would have taken hours in the past, possible with the touch of a button. It is useful to consider the UK as an example of the extent to which States are currently embedding biometric technology in public schemes. In an answer to a parliamentary question in December 2003, the Parliamentary Under-Secretary for
the Home Office listed the following projects that will make use of biometrics: first and second biometric in the British passport; identity cards programme; UK visas biometric programme; biometric travel documents; biometric residence permit; IAFS (Immigration and Asylum Fingerprints System); e-Borders programme; PITO project to use face recognition to support FIND; LANTERN (a mobile fingerprint system) and the national DNA database.\textsuperscript{13} Unless the policy changes the majority of residents in the UK will be asked to provide biometric data to a government agency over the next few years.

One of the pitfalls in the use of biometrics is the lack of acknowledgement that errors can occur. The technology is undoubtedly vulnerable to errors. This, however, depends on the type of biometrics used, and the effectiveness of the overall identification and authentication process of which the biometric system forms part.\textsuperscript{14} The standard set for the quality of biometrics should, therefore, always be high and independent of the quality of the system overall. In the context of quality, it is important to note the difference between quasi biometrics, for example digital pictures,\textsuperscript{15} and biometrics such as the facial scan plotting of up to 1820 characteristics of an individual face, which is then stored via a template on a chip. As a result of the many characteristics that can be compared in this way, the latter can obviously contribute to a much more precise and reliable identification or verification process. The quality required of biometrics in one to one searches is lower than that for one to many searches, where poor quality can lead to high error rates. Of course, human visual verification or identification also has considerable error rates. In border control situations high error rates will in practice cause (long) delays, but it will also potentially affect data subjects in much more fundamental and harmful ways. Harm may manifest itself in limitations on travel, detention and/or even criminal convictions based on misinterpreted biometric data. Robust fall back procedures should therefore form an integral part of biometric schemes.

It is clear that handling personal data takes place in a space where individual rights and collective interests meet. Data protection law and human rights law offer a legal framework governing the handling of personal data by the EU and also by national governments. There is a whole body of literature on data protection and protection of freedom of individuals in the EU,\textsuperscript{16} but the law has not been tested in the context of biometric data. As governments have only recently started to use biometrics in public schemes, there is no European case law as yet.\textsuperscript{17} It is hence unclear how concerns about the use of biometrics will be addressed by the existing legal framework.

Biometric technology used in the private sector gives rise to important additional questions that need to be answered. These questions concern, for example, the effects of parallel use of
biometrics in the private and public sector, issues concerning costs, biometric function creep, the potential for abuse of biometric data, the need to protect individuals from their inclination to trade their own privacy for financial or time gain, the regulation of the use of data for other purposes, power accumulation and so forth. These issues will be considered in this paper. It is worthwhile to first describe the proposed and actual use of biometric identifiers within Europe.

**BIOMETRICS IN THE EU**

**The Use of Biometric Identifiers**

De Hert (2007) and others provide an overview of the use of biometric identifiers in EU. The potential or actual uses include:

i. identification (one individual out of many) through storage in databanks only (Eurodac, VIS and SIS);
ii. authentication or control (one to one) through storage in a travel document with the national option of identification (one to many) through storage in a national database (European passport);
iii. authentication (one to one) through storage in a non-travel document with the national option of identification (one to many) through storage in a database (residence permit).

The tendency to use biometric data in EU wide information systems is growing rapidly. An overview of the scale of the applications and the most important policy instruments using biometric data (Eurodac, VIS, SIS and the European passport) will be given in this section.

**Eurodac**

Eurodac is a computerised, central database which holds biometric fingerprint data on asylum seekers, aliens apprehended in connection with illegal border crossing, and aliens found illegally present in a Member State. In general, these data are held for 10 years unless the individuals obtain citizenship. The purpose of Eurodac is to help establish the responsible State, by recording the country where an asylum seeker made his or her first asylum application, or the country where he or she was previously resident. Eurodac is, therefore, a database designed to search for a so-called ‘hit’, which occurs when transmitted fingerprints match fingerprints already stored in Eurodac. Member States can then establish whether an asylum seekers has
previously stayed in another Member State. The aim of the database is to determine which EU Member State is responsible for examining an application for asylum. The data are used for identification. A general unit carries out the comparisons, Member States themselves cannot conduct searches in data transmitted by other Member States.

The rights of the data subject are in line with those specified by the European Data Protection Directive 95/46 and include: that he or she must be informed of the purpose for processing the data within Eurodac, of the obligation to have the fingerprints taken, of the right to rectify data, and finally, the right to request that factually inaccurate or unlawfully recorded data be corrected or erased (Arts 15–18). Data subjects entered on the Eurodac database do not carry a document containing the biometric(s) for verification or identification because the databank is the human body itself. Every time the person is subject to a control for the purposes of Eurodac, they will have to provide a body reading which can then be checked against the data held in the database. The arrangements have attracted considerable criticism because Eurodac requires the mandatory disclosure of biometric information by people who have not committed a crime. Some commentators have questioned whether it is morally justifiable to require asylum seekers and aliens to provide biometric data which is then placed in a public arena and out of their immediate control. Alterman considers that Eurodac as a government database “is a clear case of taking the person as a mere thing, using their body as a means to an end”.

There are also concerns whether the technical reliability of the biometric identification within Eurodac is of an appropriate standard. The so-called ‘False Rejection Rate’ of the various biometric identifiers is estimated between 0.5 and 1%, although official figures vary and are subject to interpretation. These arguments appear not to have had any impact on the decision making process related to Eurodac or on other European initiatives involving biometrics. Biometric verification or identification is becoming an integral part of many new measures involving the need to identify individuals. The introduction of the biometric European passport (see below) means that mandatory disclosure of biometric information has been extended to all citizens who want to travel outside the European Union.

The European VISA Information System (VIS)

Like Eurodac, the current European Visa Information System (VIS) is a centralised database. The Council has proposed a Community Regulation (“visa code”) intended to consolidate and to a certain extent reform the existing Community provisions governing
the granting of Schengen visas. The data subjects concerned are third country nationals from over a hundred different countries in the world that require a visa to enter the EU. Data on individuals can be kept for a five year period after the last expiry date of the visa or from the date that the application file was created if the visa is not issued. The database itself is operated by the European Commission (CS-VIS) and is connected via a communication network to the appropriate organizations in the Member States (NI-VIS). The responsibility for data control is split between the Commission and the Member States. After the introduction of the Visa code about twenty million requests are expected to be be processed each year. Common Consular Instructions (CCI) are in the process of being amended to streamline the introduction of biometrics. The proposed CCI biometrics introduces an obligation to collect biometrics from visa applicants and creates a legal framework for cooperation between Member States in processing visa applications. It does not provide the data subjects with their own data readable on a document for identification or verification. A biometric body check is thus the only possible way to use the system, thus again the human body is itself the tool for identification. This semi-mandatory ‘handing over’ of biometric information to a government agency sets similar ethical and moral questions as Eurodac.

The database will soon hold biometric data in the form of digitalised photographs and fingerprints. Once adopted, the CCI biometrics proposal will be incorporated in the Visa Code. The choice of the Commission to deal with some issues relating to the use of biometrics in the CCI (such as the fingerprinting of children) rather than in the VIS has been challenged by the European Data Protection Supervisor (EDPS) and others. Objections have been made to the Commission’s ability to determine exemptions of individuals or groups from the obligation to provide fingerprints. It is suggested that such exemptions should form an integral part of the VIS Regulation and not be decided by the Commission. This objection is based on two separate issues: guaranteeing democratic and transparent procedures and achieving legal clarity. The EDPS Opinion states:

“The EDPS objects... firstly, these provisions have a significant impact on the privacy of a great number of individuals and should be dealt with in the context of basic legislation rather than in instructions with a largely technical character. Secondly, the clarity of the legal regime would make it preferable to deal with this in the same text as the one establishing the information system itself”

Both the new VIS and the CCI biometrics proposal are still going through the legislative process, and the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs is soon to
decide on a report by Rapporteur Sarah Ludford that deals with some of the issues raised above.\textsuperscript{30} In December 2006, it was proposed that Europol and other law enforcement agencies should gain access to VIS data under certain conditions.\textsuperscript{31} As in Eurodac there are some data protection safeguards in the form of defined access rights, responsibilities, confidentiality and security, and data subject rights. Data subjects (in this case the visa applicants) have the right to be informed about, amongst others, the purpose of VIS, the recipients of the data, the mandatory character of collecting the data and the right to access and correct data where it can proven to be incorrect. Before the collection of biometrics, only 30\% of visa applicants used to go to consulates. The new biometric requirements mean that everybody must attend in person. This requirement is likely to mean that many applicants have to make long journeys at considerable personal expense. Those unwilling to provide biometric data have only one option: a withdrawal from the visa application process and abandonment of the plan to visit the EU altogether. As with Eurodac, concern has been expressed about the reliability of biometric identification in visa applications. The so- called ‘False Rejection Rate’ is intrinsically difficult to measure\textsuperscript{32} but has been estimated between 0.5 and 1 \% (see above). This means, with an expected 20 million visa applicants in 2007 across the EU, that there could be 100,000 to 200,000 people incorrectly rejected a visa or facing difficulties in gaining access to the EU.\textsuperscript{33}

The Schengen Information System (SIS)

The Schengen Information System (SIS) is an EU large scale computerized database, which ah\'s been operational since 1995. It was created as a compensatory measure following the abolition of controls at internal borders within the Schengen area, and was integrated into the EU framework by the Amsterdam Treaty. The objective of SIS I is to exchange data on people, including immigration data, and objects in order to uphold security,\textsuperscript{34} it does not contain biometric data. A Second Generation system SIS II was agreed by the EU Justice and Home Affairs Ministers on 2 June 2006 and is expected to replace SIS I at the end of 2007.\textsuperscript{35} SIS II will introduce the ability to process biometric data, particularly fingerprints and face scans. All 27 EU Member States, plus Iceland, Norway, Switzerland and Lichtenstein will be connected to SISII. A European Parliament report has pointed out that there has been no targeted impact assessment on the use of biometrics, and that specific provisions detailing fall back procedures to protect individuals who are wrongly identified are lacking.\textsuperscript{36} The real capabilities of the biometric identifiers chosen within SIS II for identification have not yet been assessed.\textsuperscript{37}
In many EU Member States access to data held on SIS I has been a contentious issue.\textsuperscript{38} According to the Schengen Convention\textsuperscript{39} data in SIS I can be searched and accessed by authorities designated by the contracting parties for the purpose of border checks and controls, and other police and customs checks, when carried out inside the country and in accordance with national law. Data relating to foreign nationals\textsuperscript{40} may be searched by authorities responsible for issuing visas, residence permits or the administration of aliens.\textsuperscript{41} Schengen does not set limits to the number of persons with access authority, leaving access regulation to the national laws of the contracting parties instead.\textsuperscript{42} Consequently, the lists of people with access differ considerably from country to country. Access to SIS II will be widened to authorities such as vehicle licensing authorities, Europol, Eurojust and national prosecutors. SIS II, however, will only store biometric information that can be legally linked to an alert in SIS II.\textsuperscript{43}

Competent authorities will use SIS II to exchange data, including biometric fingerprints and face scans, using the same platform as VIS (see above) but with a separate access route. Levels of access will vary and will be regulated in accordance with European data protection provisions. There are questions about the clarity of the rules governing collection and access to data in SIS II, including the desirability of granting access to immigration data to police and asylum authorities.\textsuperscript{44} The criticisms focus on loosely defined access criteria to subject data where access is for a purpose other than SIS II. The possible use of SIS II biometric data for investigative purposes might pose serious risks for data subjects if the significance of biometric evidence is over-estimated by the courts.\textsuperscript{45} The use of biometrics for identification (comparison of one to many) is proposed for future implementation within the SIS II system. Despite these concerns about function creep and the use of a technology at such a large scale without substantial testing, SIS II is generally regarded as a privacy friendly system that fits in with the classical tradition of European criminal law.

The European Biometric Passport

The European biometric passport was introduced with the adoption of a Council regulation for security features and biometrics in passports and travel documents issued by Member States.\textsuperscript{46} E-passports issued by Member States must include a storage medium (RFID chip) that contains a facial image,\textsuperscript{47} and fingerprints shall also be included in interoperable format.\textsuperscript{48} As far as biometric features are concerned these must comply with the standards laid down by the International Civil Aviation Organisation (ICAO) in Document 9303.\textsuperscript{49}
The Annex to Regulation 2252/2004 lays down the minimum level of security required and specifies the materials to be used, printing techniques, protection against copying and so forth. The reason given for introducing biometrics is stated to be rendering the passport more secure and establishing a more reliable link between the holder of the passport and the passport itself. The EU has opted to include a system called basic access control that requires a long code number to be written inside each passport, which can be optically scanned. The reader has to send this code back to the chip in the passport before it can read its full contents. This means that in practice to read the chip contents, the passport needs to be opened and placed on an appropriate electronic reader. Border officials will compare the photograph on the chip with that in the passport and the person in front of them, confirming the bearer’s claim to the identity associated with the passport. This amounts to one to one comparison. Automated comparison is not yet an explicit aim of the Regulation but such a development can be inferred from the formulation of long term EU policy objectives such as the envisaged European register for passports. The biometric data which are taken upon application for a passport and stored in the passport itself can be stored on a national data base, but this is not prescribed by the Regulation 2252/2004. As the decision to set up a data base, and thus also the data protection and privacy issues related to it, are left to the Member States, the rights of data subjects that have been identified in the case of VIS, SIS and Eurodac do not apply here. As e-passports can be read in all Member States (and possibly also outside the EU) there is an inherent data security risk linked to controls within individual countries. The ease with which data might be read remotely and decrypted by criminals or corrupt authorities is subject to debate. The underlying principle is thus mutual trust between operating countries. There is a concern whether this trust is easily extended to authorities outside the EU when EU citizens use their passports to travel beyond the EU.

Again there has been no impact assessment on the introduction of biometrics at such a scale across the EU. Nor has there been an independent assessment of the reliability of biometric data or a large scale field trial to ensure the successful deployment of the chosen biometric systems (European Commission Joint Research Centre, 2004). Although the chip units (chip, its operating system, the antenna and the plastic covering in which it is housed) have been tested under laboratory conditions, their ability to withstand real-life passport usage is unknown. There are many reports that raise doubts over the durability and reliability of the chip units used by the Member States. In the UK for example, e-passports are intended to last ten years but the RFID chip units only have a two year warranty. In addition, there is uncertainty about the justification for the EU to insist on the
use of two biometric identifiers. The US for example, only uses one identifier (a digital photograph) and also the ICAO standard for travel documents is restricted to one biometric identifier. The choice for fingerprints as a second identifier seems disproportionate at first sight. It has been claimed that the second biometric identifier is necessary to ensure greater reliability.

“Existing security standards are improved even further by the integration of two biometric identifiers…… by introducing an even more reliable link between the holder of the visa and the residence permit”.

The effect of this on the individual providing the samples, however, and the social impact of fingerprinting the entire population have not been assessed. In fact, the financial, time and privacy costs of using two biometric identifiers have not been offset against the benefits. The decision to add a second identifier appears to have been poorly thought through.

A Call for a Debate

The rapid introduction of the new European biometric passport caused considerable concern. A large number of non-governmental organisations and data protection officers etc have signed an open letter voicing deep concern over the future handing of private data by the European Union. The objections included the legitimacy of using a binding Regulation as the legal basis for European Union action, and above all, the speed and impact of the proposals. There has been little public outcry, although in a few Member States there has been some public debate about biometrics and national identity cards. A lack of debate is not without significance, since the introduction of biometrics in EU identity and travel documents may exacerbate the ‘trust deficit’. An analysis of the text of European Union documents shows that there is increased political will to consider a central database, or a system of connected databases, in the near future. The principles of interoperability and availability have been introduced in the third pillar and there is a move towards mutual police data exchange. In 2007 the Commission issued a far reaching communication on interoperability and increased synergies between EU information systems such as SIS, VIS and Eurodac. Thus, the EU has gradually extended the use of biometric technology in its information systems, but has not shown equal commitment to evaluating and limiting the use of biometric data. One question arises as to whether the incremental process of introducing biometrics is unstoppable or could be reversed if there were compelling reasons to do so.
The ‘open letter’ has been followed by more detailed calls for a reassessment of the policy on biometrics and the impact of the measures taken. The Future of Identity in the Information Society (FIDIS) a network of excellence has published the so-called Budapest declaration. The declaration is based on research which indicates poor levels of security linked to implementation of the European passport. European governments have not established appropriate personal security measures. They have effectively forced citizens to carry passports that dramatically decrease personal privacy and substantially increase the risk of identity theft. The European Data Protection Supervisor, a significant number of members of the European Parliament and several non-governmental organisations have proposed changes and asked for increased assessment of the impact of biometric data on privacy. Analysis of the potentially harmful effects of biometric applications in combination with other technologies such as video face recognition systems may require the development of privacy impact assessment tools beyond those currently in use to the so-called surveillance impact assessments. Such assessment involves analysis of the impact of biometrics on a range of values that transcend individual privacy. It is recognised that privacy is not only an individual value, but is important for society as a whole and acts as a foundation stone for values such as a free and equal society, sociability, trust, and democracy. Surveillance impact assessments require a paradigm shift from considering the effects on individuals (the basic test for privacy protection until now) to considering the impact on society. There is a growing body of literature that identifies a need for a broad debate, more public consultation and/or surveillance impact assessment. In this debate the ethical issues that surround the use of biometrics by European and national authorities will have to be addressed.

THE USE OF BIOMETRIC DATA: MORAL AND ETHICAL ISSUES

In day to day life morality and ethics are used as synonyms but in reality it is important to distinguish between the two. Morals relate to the general views, thoughts and convictions possessed by everybody. These views form the basis for judgments on what we can consider right or wrong. Morals can be the result of an extensive search, and of long reflection, but this does not have to be the case. Often the judgment on what is good or bad is based on basic instinct developed through upbringing, (group) culture and life’s experiences. Moral judgements, however, do not necessarily stem from critical reflection and they may be inconsistent.

Ethics is the branch of philosophy that investigates morality, and in particular, the varieties of thinking which guide human conduct
and may be assessed. Ethics concerns the way we can come to a moral judgment. It is an investigation of norms and standards that form the basis on which groups or communities regulate their own functioning and decide what is acceptable or not, in the light of desired goals.\textsuperscript{65} Consideration of ethics requires critical analysis of these standards and (moral) norms, providing a logical justification for ethical criteria. There is, however, an inevitable tension between the rigorous analysis that forms the basis of ethical behaviour and the potential inconsistency and organic nature of moral judgements.\textsuperscript{66}

Moral concerns about the use of biometrics can of course be of a fundamental or causal character. Fundamental norms concern the principal act of using biometric identifiers and place direct and strict limitations on this use. Causal norms concern the (not yet completely foreseen) consequences of their use. This distinction has been used to clarify the issues surrounding the use of the ‘body’ in biometrics.\textsuperscript{67} Fundamental moral concerns of a fundamental character evolve around notions that the human body is intrinsically private and therefore unsuitable for identification or authentication processes.\textsuperscript{68}

In this paper we will concentrate on moral concerns that are of a causal character. The critical consideration of standards and (moral) norms in the use of biometric identifiers cannot produce a definitive answer because every ethical argument is based on normative, basic convictions that cannot be proven. There should be, however, identification of core values and their underlying assumptions and principles. These should be subjected to a thorough examination. This amounts to an assessment of the causal moral framework governing the use of biometric identifiers. An analysis of ethical practice related to the choice of biometric identifiers is then geared towards a thorough examination of consistency. This is essential since the norms and standards applied in the use of biometric identifiers should be consistent and there should be justification for each possible use.

**Ethical Issues and Biometric Data**

Schomberg (2007) provided a comprehensive overview of the ethical issues particularly related to nanotechnology. Schomberg addressed the need for an ethical framework that encompasses the unintentional consequences of a new technology and also the features of collective decisions in complex societies. The shortcomings of conventional ethical practice in the context of new technological developments are clearly demonstrated in the research.\textsuperscript{69} We have adapted the work of Schomberg (2007) to provide a preliminary assessment of ethical issues that surround the use of biometrics as follows:
• respect for fundamental principles (EU charter for Human Rights, and national constitutions)
• secondary principles and rights (right of access to information, data protection principles)
• dual use of technology (efficiency, security, criminal investigation)
• issues of human dignity (in machine-man interactions)
• surveillance society issues (choice, power, empowerment, transparency and accountability, consent and communication with the user)
• non-discrimination, social exclusion and equity (the digital divide and issues related to physical problems causing un-readability of biometrics such as disabilities or age)
• function creep (should the use of the data for new future applications be facilitated or prohibited)
• health and hygienic concerns about biometrics (physical contact between people providing the biometric data and the official enrolling the individuals)
• status of the data (e.g. identification of medical conditions arising from data collection that were not foreseen and not consented to by the data subject)
• advances in medicine as a challenge to the use of biometrics (transplantology, sex change, plastic surgery)
• ethics of risk assessment and assessment of any impacts on society
• hype effect of new technologies (how to assess the likelihood of biometrics achieving the objectives set?)

Norms and Standards

Some of the ethical issues, such as fundamental rights, data protection principles and function creep, outlined above can initially be considered with reference to existing data protection principles. At the same time extent to which biometric data constitute personal data is being fully debated. A generally accepted starting point is that biometric data should, indeed, be regarded as personal data and should fall under legislation intended to protect privacy. Relevant existing data protection principles that encompass most of the ethical issues listed above include: confidentiality, purpose specification, proportionality and individual participation. The latter principle requires that personal information should only be collected with the knowledge and consent of the individual and that any storage of personal information should be accurate, complete and up-to-date. In addition, the data subjects
should have access to their information and the ability to amend any inaccuracies. Confidentiality, purpose specification, proportionality and individual participation are identifiable norms and standards that should inform decisions on biometrics. The use of biometric data involves the application of these principles in a clearly identifiable way. This will promote consistency in the application of this new technology.

Other ethical concerns, however, such as social exclusion, equity, transparency and accountability, do not lend themselves to this approach. Nor can issues such as dual technology use, identification of unforeseen medical effects and the problem of overconfidence and over reliance on new technologies be readily addressed through existing privacy legislation. Here the overriding ethical concerns relate primarily to consistency in procedure. The seriousness of the concern and significance of the interests at risk should be reflected in how decisions are made, who makes the decisions, under which procedures, and within what time frame.71

Thus it is possible to reshape some ethical concerns about the use of biometrics in the European schemes described above on the basis of four data protection principles, confidentiality, purpose specification, proportionality, and individual participation. Each of these principles raises significant questions and issues on the use of biometric data:

1. **Confidentiality**: Can a biometric data subject refuse or limit the use of the data by authorities not trusted by the individual? Have the biometric data systems and processes been sufficiently tested to guarantee a minimum level of confidentiality protection?

2. **Purpose specification**: Is there sufficient protection against unauthorised use of the data beyond the original purposes? Can different functions continue to be added over time? To what extent is the collection of biometric data likely to cause discrimination? Does the absence of ‘clear purpose’ limitations make the use of biometric data capable of exploitation by both the public and the private sector?

3. **Proportionality**: Are the biometric data adequate, relevant and proportional in relation to the purpose for which they are collected? Why is it that in some measures the number of fingerprints is not restricted to two and there is no an explanation as to why the number is unspecified? Since a residence permit72 is not a travel document, it seems to be inconsistent that the specifications for permits are in line with the ICAO document no 9303 on travel documents and not with higher specifications normally applied to national ID cards?

4. **Individual participation**: Can this be jeopardised because the holder of a document cannot physically see the data on a document? Does
the absence of a right to a legal remedy against decisions made on the basis of biometric information jeopardise participation? Are there procedures put into place if data becomes unreadable? Have, for example, procedures been instigated to avoid stigmatising those individuals with unreadable fingers?

Other ethical issues relating to biometrics (for example the dual use of technology or the ethics of risk assessment) are not capable of resolution solely on the basis of the legal principles outlined above. There will have to be a wide and informed consultation process that encompasses citizens and scientific experts as well as national and European policy makers to address the issues appropriately. The use of Article 7(2) comitology procedure to add technical specifications for biometric identifiers in the residence permit requires some thought. It has been criticised as fundamentally undemocratic and argued that where such basic individual interests are at stake decisions would be better made through the co-decision procedure. This has in fact been suggested by both the European Parliament and the European Data Protection Supervisor but without success.73 In this respect, at the interface of public and commercial applications the establishment of European capabilities on testing and certification of biometric components and systems is also important and in need of urgent consideration. Technical and organisational measures should be standardized, tested and audited properly.74 This would ensure that the use and control of biometric identifiers occurs through robust, clear, justified and public decisions. These should be transparent and open to review, interrogation and verification.

CONCLUSION

The variety of ethical issues involved in decisions on biometric identifiers is considerable. Mapping the ethical and governance aspects of biometrics, however, is an important task which must underpin the public and democratic deliberations needed to create and sustain public support for this technology.75 In this paper we have not been able to deal with all the ethical issues in relation to EU biometric schemes, much more work is needed. It is important that a framework is developed to allow norms and standards in the use of biometric identifiers to be assessed particularly on the basis of consistency and transparency.

It is clear that there has been a rapid growth in the use of biometric data. Many of the choices on the type of biometric data and the technology used remain largely unexplained and unclear. There seem to be a number of factors, such as improved
security that have driven forward the use of biometrics and hindered informed debate. Biometric technology designed to bring benefits and to solve pressing problems, may also bring unintended and unforeseen consequences. This is the paradox often associated with new technology and must be faced now, before biometric applications are rolled out. Biometric applications are currently being developed so that it is not too late to debate ethical issues related to the technology. The longer and wider the deliberation, which should include informing and involving the public, the safer the use of biometrics is likely to be.

There are a number of issues that we believe particularly worthy of discussion and debate. The problem of function creep is not to be underestimated. It could be limited through stricter legislation, particularly limiting the use of specified biometric data to a particular purpose. Public distrust should be of considerable concern to legislators. User acceptance should be actively promoted through ensuring transparency of decision-making, clear procedures and increased resources dedicated to data protection. Over reaction to perceived threats should be avoided. Such a response has tended to cause an overly hasty application of biometrics. There has been a lack of distinction between the need for identification and the need for verification as a consequence. This has resulted in ignorance about off line verification and other potentially privacy enhancing features of biometric technology. The centralized storage of biometric data has not been linked to the exploration and development of privacy enhancing features for biometric data. Centralization, also suggests a de facto accumulation of power by the State. The lack of awareness of the rights of data subjects and absence of clear procedures to protect rights is a further problem. Obviously these could be put into place, including the right to review through courts and powers to impose fines on the part of data protection agencies or the European Data Protection Supervisor (EDPS). Any stigmatisation of individuals as a result of over confidence in the accuracy of the technology ought to be avoided. A realistic understanding of the reliability and accuracy of the technology should be linked to appropriate procedures to protect data subjects from technology failure.

Social risks and any administrative misuse might be minimised through the development of techniques that set controls on the numbers of data controllers, limit access points and restrict access conditions to guarantee specified uses for the stored biometric data.

We are at the beginning of an expansion in the use of biometric data made possible by technological advances. It is crucial that legislation keeps abreast of technical developments, meets the challenge of ethical problems arising from biometrics and has the confidence of the public.
NOTES

1. Traditions vary from country to country. In some European countries fingerprints have been used for a variety of law enforcement purposes, whilst in the UK their use has been restricted to identification of criminals only. In parts of Asia fingerprints have been used as signatures on contracts and in Africa, for example, as registration for the right to vote.

2. Not to be confused with the simple iris scan as used in commercial applications for authentication or identification purposes, see below note 9 and Brey (2004).

3. Larsson et al. (2007) regard the iris as a future tool for genetic personality research. It should be pointed out, however, that this is the only study that has been published which suggests that iris characteristics are associated with personality. Results will need to be replicated by independent researchers as potentially the associations found can be a local phenomena, the analysis was made on large groups of people (not individuals), and the effect found is quite modest.

4. The European Data Protection Supervisor has issued several opinions expressing this view. See for example: OJ C 91/38 of 19 April 2004 on the Second Generation Schengen System.

5. See for example Lodge (2006a) and (2005).


7. Recent research by the Coop found that of the 1,000 shoppers questioned in the three stores, half had already signed up to the scheme or planned to do so soon and the trial has subsequently been extended to three more supermarkets. Available at http://software.silicon.com/security/0,39024655,39160744,00.htm.

8. For example, voluntary pilot fingerprinting schemes at the Dutch football clubs Ajax, Feyenoord and Vitesse, see De Volkskrant, 17th January 2007, p. 17.


10. The aim of this project is to prevent criminal organisations from stealing rental cars by using stolen passports, driving licenses and credit cards as reported by TWA nieuws, 2007, nr 1, p. 46. For customer reactions and the first results of the trial are available at http://news.bbc.co.uk/1/hi/magazine/6129084.stm.

11. This development is, of course, happening across the world wide see www.queensu.ca/sociology/Surveillance/.

12. The question (82580) was submitted by David MacLean on 13th September 2005 and the answer can be found at: http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm060931/text/60913w2385.htm#06091916000121.

13. Some smaller projects involving the Home Office include IDENT1, Application Registration Cards (ARC); ISRP, VIAFS, IRIS, C-Nomis, pilot of methadone dispensing system using iris recognition at HMP Eastwood Park, and trial of fingerprint based access control to IT systems in prisons. Information available at http://gizmonaut.net/blog/2006/12/03.


17. For American case law see Freeman (2003).
19. See the annual reports on Eurodac, the first of which was published in 2004: SEC (204) 557, 5 May 2004.
20. OJ L 281/31 Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
22. See the paper by Brouwer that can be retrieved from the Challenge website, Data Surveillance and Border Control in the EU, http://www.libertysecurity.org/article289.html.
23. See for a more in depth discussion Hert et al. (2007).
25. These have been introduced in the form of a proposal for a regulation by the European Parliament and by the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications: COM (2006) 269 (Commission, 2006e).
26. The Biodev I experiment conducted by Belgium and France in 2004/2005 has resulted in 180,000 biometric visa applications on the database.
27. The introduction of the new VISA code and adapted CCI is one of the priorities of the recent German presidency see http://www.eu2007.bmi.bund.de/cln_028/nn_1034496/EU2007/EN/DomesticPolicyGoals/Topics/VisaPolicy/VisaPolicy__node.html__nnn=true.
29. See EDPS Opinion published on 27 October 2006 p. 3.

32. See the report by experts of the European Biometrics Forum (forthcoming, October 2007).


34. Article 92 of the Schengen Convention referred particularly to access alerts on persons and property for the purposes of border checks and other police and customs checks.


36. For example, working documen DT/659386EN.doc of 21.3.2007, p. 10.

37. ibid.

38. See Kabera Karanja (2002) which presents a case study on access to SIS in Austria, at p. 6–7 in particular.

39. Articles 92, 101 and 96.

40. This concerns data entered pursuant to Article 96.

41. Within the framework of the application of the provisions on the movement of persons under the Convention (Article 101 (2)), see Kabera Karanja (2002).

42. In practice, the number of people with access can be considerable, in 2002 in Austria alone 30,000 individuals had access. They used 16,000 stationary terminals around the country and an unknown number of movable lap tops with basic data that had to be verified later (Kabera Karanja, 2002, p. 6).

43. For an overall view on the interoperability and synergies among European databases envisaged in the area of Justice and Home Affairs, see COM (2005) 597 final (Commission, 2005b).

44. See for example Thomas (2005), 392–394.


46. Regulation EC no 2252/2004 of 13 December 2004. Despite the advice of the European Parliament against central storage of the biometric data, the Regulation allows such storage.

47. Since August 2006.

48. From 28th February 2008 at the latest.

50. In several EU policy proposals reference is made to the creation of a future European Criminal Automated Identification System (AFIS), see for example COM (2005) 597 final, (Commission, 2005b) p. 8.

51. See European Biometrics Forum (forthcoming) and Hoepman et al. (2006).


56. Geert Munnichs (Rathenau Institute, the Hague) has commented that in the Netherlands a situation of blind trust could suddenly turn into blind distrust once the Dutch general public wakes up to the reality of the surveillance society (in a conference address at the University of Amsterdam “How important is Privacy?” on 1st June 2007). See also Vedder (2007) and for a further elaboration on the issue of trust see the work by Lodge for example (2006b) pp. 8–13.


59. See note 43.


62. It should be noted here that the need to assess the impact of biometrics on society was recognised by the European Commission when it commissioned the Biometrics at the Frontier Report in 2004 (European Commission Joint Research Centre, 2005). The report suggested that large scale field trials should be carried out.

63. Lips et al. (2006); Bennet and Raab (2006); Balzacq and Carrera (2006); Thomas (2005); Lodge (2005) and (2006b); De Hert and Sprokkereef (2006); Ball et al. (2006); Ashbourn (2005); Steward (1999); LSE (2005), Ball and Murakami Wood (2006) and many publications from the FIDIS network.

64. This distinction is based on the work by Reiss and Straughan (1996) on the science and ethics of genetic engineering.

65. On “practical ethics” see LaFolette (2005) and also van Willegenburg (1993).


68. See Alterman (1999).

69. Schomberg (2007), p. 20 which was based the work of Nordmann et al. (2006).


71. The BITE project (Biometric Technology Identification and Ethics project) has also done some pioneering work on ethics and biometrics available at http://www.biteproject.org/.

72. The proposal for a Council Regulation amending Regulation No (EC) 1030/2002 laying down a format for residence permits for third country nationals, see the


74. The necessity of agreeing on standards is highlighted by a report produced by the European Biometrics Forum (forthcoming, October 2007), which has a separate section on the role of standards and testing/certification in the protection of privacy and the increase of trust in biometric systems.


REFERENCES


Lombroso, C. (1876). *L’Uomo Delinquente*. Hoepli; Milan, Italy.


