TECHNICAL REPORT SERIES

# Biometrics at the Frontiers: Assessing the Impact on Society

## For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)


EUR 21585 EN

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Institute for Prospective Technological Studies

**European Commission**

Joint Research Centre (DG JRC)

Institute for Prospective Technological Studies

*http://www.jrc.es*

**Legal notice**

# PREFACE

In June 2004, the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament (the LIBE Committee) asked the JRC to carry out a study on the future impact of biometric technologies. The then Commissioner for Research, Mr. Philippe Busquin, passed this request to IPTS for implementation; IPTS had done previous work for the Parliament in this area of policy support, and as the JRC's prospective studies institute, it was well-placed to address the matter.

In the event, IPTS proposed a prospective approach examining the way in which biometric technologies could influence everyday life. Descriptive scenarios taken from everyday life help with a general appreciation of the issues, and intellectual rigour has been assured through an analysis of the socio-economic, technological, legal and ethical aspects of the large-scale introduction of biometrics. LIBE Committee members had the opportunity of hearing from a number of experts on these particular aspects at a preliminary meeting held in October 2004.

The present report, entitled *Biometrics at the Frontiers: Assessing the impact on Society*, represents the output of the study. Its title underlines the purpose of the study to address biometrics beyond the immediate application for border control purposes, to their wider adoption and use in society.

The study highlights a number of key issues to be taken into account when considering the large-scale implementation of biometric technologies. The overall message is that the introduction of biometrics poses a number of technological challenges, but more than that, it affects ways in which we organise some key aspects of everyday life. These challenges need to be addressed in the near future if Europe is to shape the use of biometric technologies so as to derive maximum benefit from their deployment.

The work was carried out by IPTS ICT Unit staff in collaboration with external experts whose contributions have been acknowledged in the text. In addition, colleagues from other European Commission services and from the European Parliament provided their own comments and ideas. The responsibility for the work remains of course entirely with the JRC.

# Acknowledgements

This study was carried out by the 'Identity and Privacy' team of IPTS ICT Unit.

**EC- DG JRC – IPTS Authors**
Ioannis Maghiros (Project Leader), Yves Punie, Sabine Delaitre, Elsa Lignos, Carlos Rodríguez, Martin Ulbrich, and Marcelino Cabrera. Bernard Clements, Laurent Beslay, and Rene van Bavel also contributed to the report.

**External contributing authors**

Four experts were asked to contribute to the study, expressing their views on the technical, legal, social and economic implications of biometrics. They were: Professor Bernadette Dorizzi of the *Institut National des Télécommunications* (INT), FR, who authored the "Technical Impacts of Biometrics"; Professor Paul de Hert, of the faculty of Law, University of Leiden, who prepared a piece on "Biometrics: legal issues and implications"; Julian Ashbourn, chairman of the International Biometric Foundation and creator of the AVANTI non-profit on-line biometric resource (http://www.avanti.1to1.org), who wrote "Biometrics: social issues and implications"; and Jonathan Cave, Senior Lecturer at the Department of Economics, University of Warwick, UK, and Project Leader at RAND Europe, who reported on "Economic implications of Biometrics". All of these contributions are presented in summary form in Chapter 3.

**Other Contributions**

Other experts participated in workshops organised by IPTS or met with the authors and shared their views on specific topics. Their names and affiliations are included in the list below. Particular mention should be made to Mario Savastano for his contribution on the medical issues (see Chapter 2).

Orestes Sanchez Benavente, BIOSEC coordinator, Telefónica I+D, Madrid, ES
Raúl Sanchez Reíllo, Prof. Tecnología Electrónica, Univ. Carlos III, Madrid, ES
Juliet Lodge, Prof., Dir., Jean Monnet Centre of Excellence, Leeds Univ., UK
Thomas Probst, Independent Centre for Privacy Protection (ICPP), Kiel, DE
Mario Savastano, Ing. Senior Researcher IBB - National Research Council of Italy
Angela Sasse, Prof. Human-Centred Technology, UCL, London, UK
Z. Geradts, A.C.C. Ruifrok, J. Bijhold, National Forensics Institute, NL
T. Doulamis, A. Litke, Dr. Dpt. Elec. Eng., National Technical Univ. Athens, GR

We would also like to thank the following European Parliament and European Commission colleagues for whose comments we are grateful:
Emilio De Capitani and Katrin Huber (EP),
Pascal Millot, Marie-Helene Boulanger, Peter Hanel, Ralf Mossmann, Michel Parys (EC DG JLS),
Andrea Servida, Guenter Egon Schumacher, Antonis Galetsas (EC DG INFSO).

# Table of Contents

# Preamble

Imagine that someone wishes to access their e-mail through a PC which is inviting them to log on. The message on the screen reads *Place your right-hand index finger on the reader and hold for two seconds*. The person does so and almost immediately the screen reads *Welcome*.

Convenience and security combine to enable access to the service by authorised users and prevent non-authorised access. There is no need to remember passwords, no need to have a password policy and no risk of password loss. The result is a reduction in error and fraud through stronger confidence in the authenticity of official documents like passports and driving licences. The process is also a lot more efficient because of its very simplicity. This, in a few words, is what biometric technologies are supposed to bring to the processes of identification and authentication in the future.

Biometrics are already firmly on the political agenda, and were so well before the events of September 11. Modern economies require increasing levels of mobility on the part of the workforce, and in an emerging networked Information Society, physical identity is increasingly being replaced or supplemented by its digital equivalent. So quite apart from present-day security concerns, these underlying trends drive the need for more and better means of identification. Biometric technologies seem to offer a solution for stronger identification.

Despite their usefulness however, implementing biometric technologies raises several concerns. These emerge both from the exceptionally large scale of deployment and from the need to protect collected data from abuse.

Whether because of a perceived need for increased security, or through a desire to provide more confidence in the use of Information Society services, and in particular public services, governments have taken the first steps in considering deployment of these technologies. In doing so they have laid themselves open to criticism from some quarters regarding a possible erosion of civil liberties, and from others regarding a proliferation of different and uncoordinated systems of identification.

It is our view that the implementation of biometric technologies by governments is both inevitable and necessary, and that the criticisms, issues and challenges raised must be addressed as part of the implementation process. However, our research has led us to a much broader hypothesis: that initial 'governmental' applications for border control and eGovernment services will give way in the future to a wider use of biometrics for commercial and civil applications. We have termed this 'the diffusion effect', arising from an increased acceptance of biometric identification by citizens in their dealings with governments, and leading to a positive perception of its value and convenience for other purposes.

# EXECUTIVE SUMMARY

This Summary is divided into three sections; the first explaining the purpose of the study and structure of the report; the second the main conclusions and recommendations; and the third summarising the contents of the report. Any summary is of necessity concise; readers are advised to consult the main body of the report for more detailed background and explanation on any given issue in this complex field.

## I. Purpose and Structure of the Report

In spring 2004, the LIBE[1] Committee of the European Parliament asked DG JRC to carry out a prospective study on the impact of biometric technologies. The study kick-off meeting took place in Brussels the following July with a view to delivering a final report early in 2005. The present report constitutes that deliverable.

The prospective approach has led to one of the main messages of the study: that biometric-based identification will proliferate in society, extending from initial government use to civil and commercial applications, and that this proliferation will have a profound impact on society. We try to assess the long-term implications of this so-called 'diffusion effect' and suggest policy initiatives that might minimise any negative impacts.

The aim of this report is to examine some of the issues raised by the large-scale implementation of biometrics so as to help enhance the quality of informed decision-making at the European level.

In order to achieve this, four scenarios have been designed to depict a future society where biometrics are used in many different ways. The scenarios represent likely applications of biometric technologies rather than a prediction of possible outcomes. They aim to stimulate discussion and raise awareness about the emerging issues. The report also attempts to address the current lack of data and research by considering the social, legal, economic and technological challenges and analysing in depth four biometric technologies - face, fingerprint, iris and DNA. The report concludes by identifying a number of issues that policymakers need to address.

## II. The Report's conclusions and recommendations

The introduction of biometrics affects the way our society is evolving towards a knowledge society and poses a number of technological challenges. These need to be addressed in the near future if policy is to shape the use of biometrics rather than react to it. A pro-active approach embracing a number of different policy areas – security, industrial policy, competitiveness and competition policy – is one fully consistent with the Lisbon goals, ensuring that Europe reaps the benefits of governmental initiatives in this important area.

[1] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

The study has identified a number of issues that require further consideration and action so that Europe can benefit from the large-scale deployment of biometric technologies. Two overriding conclusions provide the basis for the report's recommendations:

- **The 'diffusion effect'.** The use of biometrics can deliver improved convenience and value to individuals. It is expected that once the public becomes accustomed to using biometrics at the borders, their use in commercial applications will follow. The diffusion effect is likely to require the addition of specific provisions on biometrics to the existing legal framework. New legislation will be needed when new applications become widespread and necessary fallback procedures are defined.

- **There is a need to recognise the limitations of biometrics.** The main reason for introducing biometric systems is to increase overall security. However, biometric identification is not perfect - it is never 100% certain, it is vulnerable to errors and it can be 'spoofed'. Decision-makers need to understand the level of security guaranteed through the use of biometric systems and the difference that can exist between the perception and the reality of the sense of security provided. The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness.

**Recommendations**

The above conclusions lead to the following recommendations:

1. **The purpose of each biometric application should be clearly defined.** The use of biometrics may implicitly challenge the existing trust model between citizen and state since it reduces the scope for privacy and anonymity of citizens. Clarity of purpose is needed to avoid 'function creep' and false expectations about what biometrics can achieve. Such clarity is particularly needed to ensure user acceptance.

2. **The use of biometrics to enhance privacy.** Biometrics raise fears related to privacy, best expressed by the term "surveillance society", but they also have the potential to enhance privacy as they allow authentication without necessarily revealing a person's identity. In addition, by using multiple biometric features it is possible to maintain related personal information segregated and thus limit the erosion of privacy through the linkage of separate sets of data. The more policy measures are able to encourage the use of biometrics to enhance privacy, the more biometrics will be acceptable to the public at large.

3. **The emergence of a vibrant European biometrics industry.** The large-scale introduction of biometric passports in Europe provides Member States with a unique opportunity to ensure that these have a positive impact, and that they enable the creation a vibrant European industry sector. Two conditions would appear to be necessary for this to happen. Firstly, the

creation of a demand market based on wide user acceptance, by clearly setting out the purpose and providing appropriate safeguards for privacy and data protection. Secondly, the fostering of a competitive supply market for biometrics. This is unlikely to emerge by itself and will need kick-starting by governments – in their role as launch customers, not as regulators.

4. **Fallback procedures.** Since biometric systems are neither completely accurate nor accessible to all, fallback procedures will be needed. In the case of physical access systems (e.g. border control) skilled human operators need to be available to deal with people that are rightly or wrongly rejected. Whatever the application, whether in the private or public domain, the fallback procedures should be balanced – neither less secure, nor stigmatised. People with unreadable fingerprints, for example, have the same need for dignity and security as everyone else.

5. **Areas for Future research.** The study has revealed several areas where further data and research is needed. These include:

   - ***Research and Technological development.*** Biometric technologies provide a strong mechanism for authentication of identity. Biometrics cannot be lost or stolen, although they can be copied, and they cannot be revoked. However, the technology is still under development. Technical interoperability and a lack of widely accepted standards, as well as performance and integrity of biometric data are major challenges that need to be addressed.

   - ***Multimodal biometric systems***. Multimodal systems are those which combine more than one biometric identifier. For example, it is currently planned to use face *and* fingerprints in EU border control systems. Research initiatives have been launched on the application of multimodal biometrics in mobile communications (e.g. mobile telephones and other devices). However researchers need more test data to work with and there is still much work to be done**.**

   - ***Large-scale field trials.*** So far, empirical data on the real-time large-scale implementation of biometric identification involving a heterogeneous population is limited. Field trials will have to be conducted to fill this gap. Such trials could also provide realistic cost-benefit data. Moreover, there is a need to exchange best practice and to harmonise Member State initiatives. The European Commission's Directorate General for Information Society and Media has taken some initiatives in this regard.

# III Content of the Report

## 1. Some Basic Definitions

A biometric indicator is any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification. Such features can be categorised as physiological (e.g. height, weight, face, iris or

retina.) or behavioural (e.g. voice, signature or keystroke sequence). Some biometric features are persistent over time while others change. All biometric features are deemed 'unique' but some are less 'distinct' than others and thus less useful for automated identification purposes. The distinctiveness of any biometric feature depends also on the effectiveness of the sampling technique used to measure it, as well as the efficiency of the matching process used to declare a 'match' between two samples.

Biometric identification is a technique that uses biometric features to identify human beings. Biometrics are used to strongly link a stored identity to the physical person this represents. Since a person's biometric features are a part of his or her body, they will always be with that person where ever he/she goes and available to prove his or her identity. Biometric technologies may be used in three ways: (a) to verify that people are who they claim to be, (b) to discover the identity of unknown people, and (c) to screen people against a watch-list.

Biometric identification works in four stages: enrolment, storage, acquisition and matching. Features extracted during enrolment and acquisition stages are often transformed (through a non-reversible process) into templates in an effort to facilitate the storage and matching processes. Templates contain less data than the original sample, are usually manufacturer-dependent and are therefore not generally interoperable with those of other manufacturers. Templates or full samples thus acquired may then be held in storage that is either centralised (e.g. in a database) or decentralised (e.g. on a smart card). As a consequence of the statistical nature of the acquisition and matching stages, biometric systems are never 100% accurate. There are two kinds of possible errors: a false match, and a false non-match. These errors vary from one biometric technology to another and depend on the threshold used to determine a 'match'. This threshold is set by the operators depending on the application.

The report uses seven widely-accepted criteria to assess biometric technologies: universality, distinctiveness, permanence, collectability, performance, acceptability and resistance to circumvention. The degree to which each biometric technology fulfils a given criterion varies. It is only useful however, to compare the technologies based on the criteria once a specific application and a concrete identification purpose have been set. For example a convenience application (e.g. controlling access to food in the student cafeteria) may tolerate a significant error rate while a high-security application (such as controlling access to a nuclear site) would require minimal error rates.

There are currently few biometric applications that have millions of enrolled individuals and thousands of deployed devices. Those that do exist are typically in law enforcement and in certain civil areas. Physical access control (access to a site) is another area that has been developed and logical access (in particular online identity) is forecast to be a fast-growing use of biometrics in the future. More importantly, the integration of biometrics into passports and visas will be the first truly large-scale deployment in the European Union. It still remains to be seen whether biometric applications will be deployed where individuals voluntarily participate because they find the application beneficial and convenient.

## 2. Biometrics Issues

At present, many applications of biometric technologies exist both in the private and public sector. Some of these are considered large-scale, for example the FBI fingerprint database in the US or the Malaysian multi purpose smart card. But so far no application comes close in scale to the proposed scheme for passports and visas. The widespread implementation of biometric applications in the public sector and their potential proliferation in the private sector will pose a series of challenges which policy-makers need to address. The report examines the social, economic, legal and technological implications of biometric technologies, and includes a short but important analysis of the medical implications. In each of these analyses, the issues of security, privacy, interoperability with other systems and costs are examined.

### Security

Biometric systems are more secure than traditional identification systems. But they only represent a secure identification process in that they provide a strong link between physical persons with their identity data. This means that the integrity of the linking process must be high. This will depend on the secure operation of each one of the four stages of a biometric identification process (enrolment, storage, acquisition, matching). In addition it cannot rely on secrecy, since most biometric features are either self-evident or easily obtainable. On the other hand, since biometrics are only a part of the system, it is not enough to secure the biometric system if the rest of the process remains open to circumvention. In the end, the notion of a biometric identifier being absolute proof of identity has to be discarded. Biometric identification systems are subject to errors and circumvention and thus are not perfect. It is important for whoever uses biometric identification systems to understand this principle.

### Privacy

While the use of a biometric technology is not an invasion of privacy, in many cases the way the digital data is produced, stored, compared and possibly linked to other information about the individual, may raise a set of concerns. Although these are concerns the existing legal framework for Data protection can handle the widespread diffusion of biometrics into the commercial sphere may challenge the legal framework in ways that will have a negative impact on user acceptability. For example should the habit of sharing biometric data among private sector entities proliferate, then it is likely that users may find that the current data protection frame is unable to protect them adequately and thus become disenchanted with convenience application altogether. Moreover, one would have to consider ethical consequence of large scale deployment. One could argue that the use of a part of oneself (the biometric feature that is being digitised, stored and compared) as one's identity is eliminating the space that we traditionally place between our physical selves and our identity. Currently, any individual has the option of changing identity if the need arises (e.g. witness protection programme). This becomes harder or even impossible when identity is tied up with the physical self.

## Interoperability

For any emerging technology, interoperability across geographical borders and business sectors, across processes, devices and systems is beneficial to its diffusion. National interests in maintaining control and vendor resistance (aspiring to future market dominance due to lock-in effects) are natural barriers to interoperability. There is significant work being done at national and international levels to develop standards, which will be useful in promoting open systems development and interoperability. Technical interoperability is likely to be achieved in the near future but interoperability of processes may be more challenging especially when biometrics become more widely diffused in society.

When systems become more interoperable, the need for building safeguards against abuse grows as well. Moreover, since individuals have many different biometrics at their disposal, there is the possibility for different applications to make use of different biometrics, in the sense that limited interoperability may create barriers and thus protect against abuse. Such systems may still be compatible at the data transmission level and thus it may still be possible to cross-check information as to who was identified and where.

## Costs

Costs vary between technologies and also between low-end and high-end equipment within any one technology. It is the purpose and scale of an application that determine costs. Thus costs will depend on the choice of open- or closed-system architecture, type of application, centralised or decentralised storage, whether encryption is used as a means of data protection, and the decision of where in the system matching takes place. Moreover, enhanced market competition or market distortions will also impact on costs, as will regulatory decisions on interoperability, standards and intellectual property rights. In addition, it must be noted that real costs include overall system security (at all biometric stages) as well as those of the fall-back system which is an indispensable element of any proper biometric application.

## Social aspects

Biometric technologies are just a tool, but their social implications may be far-reaching. Europe faces the challenge of better understanding the longer-term implications of large-scale deployment of biometrics so as to ensure their beneficial implementation. The following four themes have been identified as the main social issues:

1. **Clarity of purpose in relation to biometric applications.** “Function creep” is an important concern, i.e. that technology and processes introduced for one purpose will be extended to other purposes which were not discussed or agreed upon at the time of their implementation. Thus it is important to be

clear about what the needs of the application are and how biometrics will be able to achieve them.

2. **Interoperability and equivalence of performance and process.** This is not only a technical issue. Process equivalence (for instance backup procedures that are the same everywhere) is extremely important as it impacts on system performance, especially where biometrics are used in international situations (e.g. border control).

3. **Human factors, usability and social exclusion.** Human factors such as age, ethnicity, gender, diseases or disabilities (including natural ageing) ought to be studied on a case-by-case basis so as to minimise the possibility of social exclusion of a small but significant part of the population. More research is also needed on the usability and the user-friendliness of biometrics in real-life situations.

4. **Impact upon the trust model between citizen and state.** People may temporarily accept a loss of some of their personal freedom in exchange for a more secure world. But when government control is perceived as excessive, disproportionate and/or 'too efficient' this may lead to an erosion of trust which will be in the interest of neither governments nor citizens.

## Economic aspects

Biometric technologies are strong identification technologies and as such influence the level of 'trust' in economic transactions. In other words they can help reduce fraud and thus help materialise the efficiency and equity gains of the Information Society. They help simplify things from the user's perspective and minimise the likelihood of error. At the same time their widespread deployment in the public sector will make identification over the network easier, more secure and may bring down costs per secure transaction. This in turn will help consumers make more efficient transactions. Standards and interoperability issues, however, determine widespread adoption and shape economic challenges. The following five themes summarise the economic implications of biometrics:

1. **The concept of optimal identity.** The economic importance of identity is growing in a digital society, but the strongest identity protection is not necessarily the optimal one. This important point is explored in depth in the report.

2. **Negative implications of stronger identification.** Identity errors and abuse may become less frequent, but when they happen, they could potentially be more dangerous. For example identity theft may become less frequent but more severe and with wider social repercussions.

3. **Interoperability is vital for market operation.** There is a serious danger that the biometrics identification market – and markets that depend on identity –

may fragment into clusters that will not interoperate, thus becoming vulnerable to monopolisation or dominance by a few players.

4. **Biometrics-related IPRs threaten open competition.** The unregulated exploitation of intellectual property rights to aspects of biometrics can significantly reduce competition in biometrics and/or distort development, direction and speed of uptake.

5. **Public sector uptake will shape the market.** The use of biometrics in eGovernment initiatives and associated large-scale public procurement could be key levers to ensure open and competitive markets, and rapid and socially-productive innovation.

## Legal aspects

Up to now biometric technologies have been operating in various closed environments; by contrast, their use in private transactions will be based on consent. The existing legal framework does not hinder public and private actors from implementing applications. The deployment of biometrics does not threaten procedural rights (i.e. rights in a court of law); their use is deemed intrusive but within reasonable limits and a few unresolved issues arising from the data protection framework have not hindered recent choices for biometrics in European passports. However, their widespread implementation and the fear of a 'surveillance' society that may follow from the so-called 'diffusion effect' may call for a rethink of the legal tools available. The following four themes are briefly described so as to enable a better understanding of the legal implications of biometrics:

1. **Enabling legal environment.** The existing legal environment (privacy and data protection) is flexible in that it is an 'enabling' legislation legitimising the *de facto* commercial use of personal data. Data protection rules regulate the use of biometrics but they lack normative content and raise no ethical debate.

2. **Opacity/transparency rules required.** Data protection (transparency rules) does not specify what the limits of use and abuse of biometrics are. Opacity (privacy) rules may prohibit use in cases where there is the need to guarantee against outside steering or disproportionate power balances.

3. **Wider implementation raises fundamental concerns.** As biometrics are diffused in society some concerns are gaining in importance: concerns about power accumulation, about further use of existing data, about specific threats related to the use of biometrics by the public sector, about the failure to protect individuals from their inclination to trade their own privacy with what seems to be very low cost convenience.

4. **Use of biometrics in law enforcement.** It is imperative that biometrics evidence be regulated when presented as evidence in courts of Law so as to protect suspects adequately (e.g. being heard, right to counter-expertise).

## Technological aspects

Biometric technologies are still largely undergoing development and are not yet mature enough for widespread use in society. Enrolment is the first and most important stage of any biometric application since the overall efficiency, accuracy and usability of a system depends on this stage. Re-enrolment during the life-cycle of an application is not only necessary because of natural and accidental changes to biometric features, but also to ensure that the acquisition of the sample patterns is performed using state-of-the-art sensor technology. However, not enough large-scale trials exist to help draw conclusions on enrolment procedures. Biometric sample or template storage and their protection are also very important issues. Storing can be done in centralised databases or on portable media such as smart cards or tokens. The report examines the following four technological concerns:

1. **Performance/Accuracy.** There will always be a compromise between the level of accuracy that can be obtained from a biometric system and the level of performance obtained in operating a live system with a threshold based on operator- or application-defined constraints.

2. **Biometric Privacy.** Biometrics could be used in the future to enhance privacy by using a biometric feature to encode a security key, for example a PIN code which allows access to a bank account. There are many advantages to this use of biometrics – primarily that keys thus produced are not linked to the original patterns, are not stored and can be revoked at will.

3. **Interoperability.** Technical interoperability and the availability of widely accepted standards and specifications are issues that are currently being researched. They are particularly important in border-control applications, in which different countries are inevitably involved but that will also be the case in the future with worldwide consumer applications (e.g. bank ATMs).

4. **Multimodality.** Combining several modalities, e.g. fingerprint and iris, in sequence results in the improvement of a system's overall efficiency, while combining them in parallel improves a system's flexibility by providing alternative modes for the verification/identification process. The choice of which modalities to combine is driven by the specific application design. This combination may be performed at different stages of the process, resulting in various benefits. Multimodality could also be viewed as a security enhancement, for example by having the system request alternative modalities to be tested at random in an effort to keep potential impostors at bay.

## Medical aspects

Direct medical implications include potential risks to human health from the use of biometrics as well as public concerns related to possible hazards. Indirect implications relate to the ethical risk of biometric data being used to reveal private

medical information. The former are more a matter of public perception while the latter are more difficult to deal with. Developing this further:

1. **Direct Medical Implications.** Interaction with a biometric sensor holds two potential health risks. If the system uses a contact sensor there is a risk (real or perceived) of the sensor being contaminated. The real risk may be minimal, especially when compared to similar everyday actions (touching doorknobs, railings) but the perceived risk may have a negative impact on public acceptance. Regular cleaning (e.g. through periodic irradiation with UV light) can minimise concerns and improve sensor performance. The second risk relates to technologies that use radiation to assist acquisition (e.g. retinal scanning which use infrared light). There is a fear that this radiation could be damaging to the eyes. Retinal scanning could cause thermal injury on the back of the eye, but it is a biometric technique that is not currently in use. Data from iris recognition equipment manufacturers show no evidence that iris systems could pose a risk. It would be reasonable however to validate this claim in independent laboratories.

2. **Indirect Medical Implications.** These are more controversial as they refer to fears about the possibility of biometric data revealing sensitive health information, leading to ethical concerns. *Iridologists* allege that the iris exposes potential health problems, but these claims are scientifically unfounded and thus the only risk may be one of public fear. Retinal scanning could have serious implications as it may enable detection of a subject's vascular dysfunction. There are also concerns that in the future, face recognition may be used to detect expressions and thus emotional conditions. The ethical debate gets extremely heated when the use of DNA is considered, although the regions of DNA necessary for identification are 'non-coding' (i.e. to the best of current knowledge, these regions do not hold genetic information so do not code for any genes).

## 3. Overview of selected biometric technologies

It is also worth looking at selected individual technologies in-depth so as to understand the challenges specific to each. Details of the four selected technologies are presented below, followed by a brief comparison.

**1.** **Face** recognition is used every day by humans for identification purposes. It is considered less intrusive than all other technologies and has thus a higher level of user acceptance. But for machine identification it poses more of a technological challenge, currently having lower accuracy rates than the other principal modalities. Face recognition is characterised by its theoretical potential to operate at a distance, with or without user cooperation. This could lead to systems that recognise an individual passively, improving convenience but also raising privacy fears. Face recognition also holds the risk that the biometric identifier may be "stolen" without a person's knowledge as people nearly always have their faces on public display, thus it is critically important to make systems which are practically impossible to spoof.

2. **Fingerprints** are the oldest and probably best known biometric identifiers given their intensive use by law enforcement agencies. In the past, highly-skilled people were used for fingerprint recognition but now the whole process can be reliably automated provided that all parameters are under strict control. The extensive experience with fingerprint technology is likely to pave the way for the inclusion of fingerprint readers in consumer electronic devices. The two main challenges to be addressed are (i) an estimated 5% of people are not able to enrol and (ii) there is a lack of interoperability in an open commercial context.

3. **Iris** recognition technology is apparently mature enough to be used commercially in high-security applications in both identification and verification modes with excellent performance results. According to manufacturers' claims, so far there has never been a false non-match. Yet it has a smaller share of the market than hand, face and fingerprint techniques. It involves a non-contact, consensual enrolment process. However, it is said to produce a sense of discomfort as users are not certain as to where to focus when providing a sample. Also, not everyone can enrol satisfactorily.

4. **DNA identification** is based on techniques using a specific part of the 'non-coding' DNA regions, i.e. regions of DNA that to the best of current knowledge bear no genetic information. It is mainly used in forensic laboratories as it does not allow a real-time identification. It is a highly accurate technique where exclusions are absolute and matches are expressed as a probability. DNA enrolment is always possible, but DNA identification is expensive, time-consuming (several hours), and needs skilled human intervention. It is also not possible to distinguish between identical twins (contrary to fingerprints or irises, for instance).

**Comparing the different modes.** By comparing each biometric mode one may reach simplified conclusions such as: fingerprint technologies perform well on many aspects and this is the reason that they are chosen for most applications; face technology is still very weak technically in terms of performance and accuracy; iris recognition performs exceptionally well but has a relatively higher failure-to-enrol rate and is less accepted; DNA technologies are not well accepted and need a lot more time to produce a decision result, which explains why they are mostly used in forensics.

## 4. Scenarios on future biometrics

The objective of the biometric scenarios presented in this report, is to broaden the scope of thinking on the future of biometrics and to raise key issues that might at present be overlooked. Four scenarios are depicted: biometrics at the borders, in the health sector, in business and in everyday life. They can be placed on a continuum ranging from public-sector applications, to private applications with little or no government involvement. Privacy, security, usability and user acceptance concerns differ according to the environment.

Scenario 1. **The everyday life scenario** depicts a day in the life of a traditional family, in the form of a diary entry by the teenage son. The scenario draws attention to one basic fact about biometric technologies: that they can never be 100% secure. There is a trade-off between allowing impostors through the system (false accept) and denying access or services to legitimate users (false reject); the choice of threshold will depend on the nature of the application.

Scenario 2. **The use of biometrics in business** can be for various purposes: internal (e.g. for employees) and external (e.g. with clients, other companies). The scenario is presented as a memo to the senior management of a large multinational supermarket chain which has embraced the use of biometrics but is concerned that it is not reaping the expected benefits (access control, auditing working hours, and customer loyalty). It shows that back-up/alternative procedures are important and that biometric access systems are only as secure as their weakest link, which is, in this case as in most cases, human. The scenario describes how users concerned about their privacy may reject biometrics when there is little perceived added value for them.

Scenario 3. **The health scenario** presents an exchange of e-mails between two doctors in different countries. Strong identification is essential in the health sector - retrieving medical histories, administering medicine, handing out prescriptions, and carrying out medical procedures, all rely on the correct identification of the individual. In addition there is a strong need for privacy given the sensitive nature of medical data. These two requirements make the health sector a very likely field for the application of biometrics.

Scenario 4. **Biometrics at the borders** is likely to occur within the shortest timeframe as concrete plans for this application already exist. By focusing on three destinations and three family members, the use of biometrics is illustrated by different age groups in countries where different legal and regulatory regimes apply. The importance of secure enrolment is highlighted by following the family in their quest for necessary visas.

# INTRODUCTION

Biometric technologies can be used to identify people by pairing physiological or behavioural features of a person with information which describes the subject's identity. It is almost impossible to lose or forget biometrics, since they are an intrinsic part of each person, and this is an advantage which they hold over keys, passwords or codes. These technologies, which include amongst others, face, voice, fingerprint, hand and iris recognition, are the basis of new strong identification systems.

However, biometric technologies are still largely under development despite the fact that they have been used in various applications over the past 40 years. In addition, they form only part of an identification system. There are challenges for such systems, on the one hand emerging from the need to adequately protect them from abuse, and on the other as a result of their wide-scale implementation and the impact that may have on society. There is currently a lack of data and research relating mainly to the non-technological challenges and more specifically to the large-scale introduction of biometric identifiers, including their use in visas, residence permits and passports.

The purpose of this report is to address that lack of data and analysis, with the aim of enhancing the quality of informed decision-making at a European level. A wide-ranging prospective study has been carried out which will try to address the impact of biometric technologies and applications on people's everyday life and the potential policy issues, in a comprehensive manner. It is not the purpose of this report to argue for or against biometrics. It is equally not the purpose of the report to address the requirements of the international or European political agenda, which are briefly described below. Rather, at the end of the report, the reader should have enough knowledge about biometrics and their current, emerging or potential consequences to make an informed decision. This may support the introduction of biometrics that not only protect society but also advance it for the better while allowing services to flourish.

## *Objective*

The objective of this study is to increase the knowledge base on the large-scale implementation of biometrics so as to enhance the quality of informed decision-making at the European level.

## *International and European Agenda*

As a response to the September 11 terrorist attacks on the US, and clearly based on concerns about threats to global security, the US Government strongly advocated the inclusion of Biometric Identifiers in travel documents (EUR 20823 EN, 2003). The current US security policy regarding biometrics is mainly based on two decisions:

- After the 30 September 2004, all foreigners (even those from the 27 Countries listed in the visa waiver programme - VWP) will have to accept to provide a high resolution digital picture of their face and their fingerprints;
- U.S. law initially required citizens of VWP countries to have machine-readable biometric passports by October 26, 2004; Congress extended the deadline for biometric requirements in VWP passports to October 26, 2005 to allow more time to resolve technical issues.

In May 2003 the ICAO (International Civil Aviation Organisation) published new standards for MRTD (machine readable travel documents) in order to introduce biometric technologies. These standards are in line with the US initiative. The face has been selected as the primary biometric, in the form of a high-resolution digitalised image which will be stored on a contactless chip, in order to facilitate global interoperability in border-control identification.

The topic of biometrics is not a new one for the European institutions. A Council regulation was adopted (December 2000) for the establishment of "EURODAC" which is a fingerprint database of asylum seekers and illegal immigrants. The European Council of Thessaloniki (June 2003) agreed to go ahead with biometric identifiers in third country nationals' visas and citizens' passports. As a consequence, of the Council conclusions it proposed to introduce biometric data into travel documents in order to improve the accuracy of identification and make travel documents more secure against counterfeiting.

Regarding the European agenda, five proposals from the EU institutions constitute the main European platform for the introduction of biometric identifiers:

1. 24 September 2003: Proposal for a Council regulation amending (EC)1683/95 (uniform format for VISA) and (EC)1030/02 (uniform format for residence permits);
2. 8 June 2004: Council decision (2004/512/EC) establishing the VISA Information System (VIS);
3. 13 December 2004: Council regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States;
4. 28 December 2004: Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM(2004) 835 final;
5. 28 February 2005: Commission decision C(2005) 409 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.

The European Parliament, which had previously rejected the Commission's proposal (April, 19, 2004), passed the new proposal on December 2, 2004 stipulating that biometric data should only be used for verifying the authenticity of the passport and should be handled only by competent authorities[2].

[2] EurActiv 15, Dec04: http://www.euractiv.com/Article?tcmuri=tcm:29-133440-16&type=News

## *Report Structure*

This brief introduction continues by presenting four scenarios which exemplify biometric use in the not so distant future. The main body of the text is then structured in five parts. Chapter 1 introduces the key concepts: what biometrics are, how they work, and for what purposes they can be used. It also briefly introduces four issues which are prominent in the discussion on biometrics: security, privacy, interoperability and cost.

Chapter 2 provides specificities of biometric technological systems and touches upon the medical aspects of biometrics. Also, Chapter 2 briefly introduces four main biometric modalities: face, fingerprint, and DNA. The advantages and disadvantages of using combinations of these biometric technologies are also explored.

Chapter 3 presents a detailed analysis of the social, legal, economic and technological aspect of biometrics. On social issues, the report notes that biometrics touch upon the trust model between citizen and state and that socio-demographic and cultural differences, psychological factors and usability are important. Economic aspects include the market side (growth of the sector main players), the direct and indirect impact on the economy, as well as issues regarding intellectual property rights. From a legal point of view, biometrics are evaluated with regard to human rights, privacy and data protection legislation. Finally, from a technological point of view, the technological challenges for Europe are reported.

Chapter 4 takes up the scenarios that are presented just below in the introduction. It briefly analyses the scenarios which aim at illustrating current and future challenges of the introduction of biometrics throughout society. The identified issues lead to conclusions and policy recommendations developed in Chapter 5.

There are two annexes to this report. The first annex provides further information on the four selected biometric technologies: face, fingerprint, iris and DNA. IN the second Annex the questions originally posed by the European Parliament's LIBE Committee are presented and the areas of the report through which these have been answered are highlighted. A glossary and list of references can be found at the end of the report.

## *SCENARIOS ON BIOMETRICS IN 2015*

### OBJECTIVE

Scenarios are one of the main tools for looking at possible futures. Rather than predicting the future, they are used to stimulate discussions on identifying and understanding the key relevant issues when thinking about possible futures. The biometrics scenarios presented here give a vision of a future society (2015) where different biometrics are used for a wide range of purposes and applications. Their goal is to open up the scope of thinking on the future of biometrics. The use of biometrics is presented in four different environments: in Everyday Life, in Business, in Health and at the Border. The reader is also referred to Chapter 4 of the report, which provides an analysis of these scenarios and summarises the main conclusions that emerge.

### SCENARIO 1: BIOMETRICS IN EVERYDAY LIFE

**The diary of Constantin, a teenager born in the late 20th century**

I got into a bit of trouble at school today. One of my friends, Ed, has been banned from the cafeteria because his parents haven't paid the school fees on time. I think that's unfair, so I helped him spoof the cafeteria entry system. It uses iris recognition which is very secure if installed properly but the cafeteria uses cheap readers that are easy to fool. I just printed a high-resolution picture of my iris and Ed presented that to the system. Our trick has been working fine for the past few days, but yesterday it seems they realised my iris was being scanned twice a day – I never thought the system checked for double entries! They sent me to the headmistress's office who wasn't happy. She called up Mum at work and asked her to come over to the school. I wish Mum hadn't been able to come because she made such a fuss. If only the fingerprint scanner in the car's ignition had broken down, it would have delayed her from coming. My parents think that the fingerprint scanner is great because it lowers their insurance premium, but it's a pain for me because I'll never be able sneak out with the car until they enrol me onto the system.

In the meantime, granny had to go to the nursery to pick up my little brother because Mum was at school with me. It's a big nursery and they're paranoid about strangers picking up the wrong kids so they spent lots installing a multimodal biometric system a few years ago. Granny enrolled in the system right at the start but she's never had to use it up until now. It works with face and voice recognition, and it's supposed to unobtrusively scan and recognise parents as they ring the doorbell and ask for their child. Well that's not how it worked in granny's case – the system didn't recognise her so the door wouldn't open. All face recognition systems perform much worse if the stored template is old and I guess for granny the situation was even worse because she's aged a bit. The nursery wants to be tight on security so the system is set to a low number of false positives. But that means it gets more false negatives and doesn't recognise the people that it should.

If it doesn't work right away, what you're supposed to do is stand very still in front of the camera with a neutral expression for a few seconds, so that the face recognition system can get a good shot. Then you speak clearly to a microphone so that the voice recognition system can do its job. Well granny says a queue of parents started building up behind her and she got very nervous which made her voice begin to falter. I can imagine her expression wasn't all that neutral either. The more flustered she got, the less likely the system was to recognise her. Eventually a member of the nursery staff came to the door and let her in.

They checked her ID against their records and saw that she's been authorised by my parents, so they let her collect my brother.

It's not as if granny doesn't know how to use face recognition systems; her Over-65 bus pass has a facial template stored on the smart-chip. But the template on the bus pass is renewed every year which makes a difference. Also, I suppose the bus pass system allows quite a high rate of false positives. It makes sense; after all people are more concerned about preventing a child being kidnapped than stopping someone getting a free bus ride.

We got home to find dad sorting through his files on our virtual residence. Each person in the family has their own storage space which only they can access. We used to use passwords to gain access but Dad realised that I always knew what his password was (because he always had it written underneath the keyboard!) and he was worried about all the work-related files he keeps on there so he changed the system. Now you have to scan your iris to access the system – it's the latest gadget around the house.

Dad bought the newest type of reader and I can't spoof it like the one at school. Not that I'm too bothered though – I'm not interested in what Mum and Dad store there anyway. The funny thing is that Dad's the one with the most problems using the system because he's so short-sighted that the second he takes his glasses off, he can't see where he's supposed to focus.

I can hear my brother in his bedroom next door, playing around with his new teddy bear. My parents call it his "biometric bear" and they think it's so high-tech, but it's just a regular teddy bear that has a voice recognition system. When they bought the toy, Mum typed in my brother's name and registered his voice so when the teddy hears my brother speak, it replies to him with his name. My brother loves that – now he wants all his toys to say his name.

Granny is downstairs in the kitchen preparing some dinner. It's a good thing Dad was here to turn the hobs on for her because she still hasn't enrolled her hand in the cooker's biometric system – and it's not likely she'll do so today after her experiences at the nursery. At home she uses an old-fashioned cooker but Mum and Dad bought a cooker with a hand geometry reader for our house in order to avoid accidents with my little brother around the house. Granny says that she's learned to use enough biometric systems and the cooker is just one system too many. I keep telling her hand geometry readers are the easiest things to use but she won't listen to me.

Having said that, there are times when biometrics can be a real hassle. My friend Max has just bought the latest Tomb Raider game and I wanted to use it too. I borrowed it off him at school today but it turns out that the program asks for the purchaser's fingerprint in order to start up. I've got a little kit which I bought online for spoofing fingerprints, but Max needs to come round here first so we can make a copy of his print. Instead this afternoon I'm stuck here writing in my diary.

It's not all bad though… at least no-one can read what I've written without my iris.

## SCENARIO 2: BIOMETRICS IN BUSINESS

M&G Superstores, Inc.
Head Office

### MEMO TO SENIOR MANAGEMENT
### IMPLEMENTATION OF BIOMETRIC TECHNOLOGIES

Recently Management has been concerned about the use of biometric technologies within the working environment of M&G Superstores as well as in the superstores themselves. It is important to remember, as announced when biometrics were first introduced at M&G Superstores, that such an identification system will only be effective if all of its elements work together. In the words of our founding father Miles Graham, "There is a logic in technologic".

Personnel entrance: The biometric access system which clocks hours worked was introduced to replace the outdated system of punch-cards. It is therefore important that all employees pass through the system otherwise the hours they work will not be registered.

Lately there have been large queues at the hand recognition device at the North entrance. Guards at the North entrance should be reminded that they are only there to monitor employees using the biometric access system and they must not under any circumstances open the barriers to let employees bypass the biometric check. The procedure clearly states that if the system denies access to an employee, he/she should immediately leave the queue and go through the secondary access point, through the guards at the South entrance. Failure to comply leads to delays and inconvenience.

A case was reported last week of a nervous employee being rejected due to sweaty palms. Instead of accessing the South entrance however, she insisted on gaining access through the main gate. As she became increasingly anxious, her palms became even more sweaty, and the queue got larger and more impatient. Had she not been so persistent and accessed the secondary access point, the inconvenience to other employees would have been avoided. Remember the words of Miles Graham: "Obey, don't delay".

Merchandise purchases: it is imperative that all Purchase Managers adopt and embrace the remote multimodal biometric transfer system which has recently been implemented. This system allows large amounts of money to be transferred securely worldwide. All that is required is biometric enrolment at our local bank branch. Purchase managers are reminded that they must register multiple biometrics (all ten fingers, face and iris are recommended). At least one of these biometrics must be reserved for bank use alone; the fourth or fifth finger of either hand are recommended for this purpose as these fingers are not demanded by other major applications. The speed and security of these transactions help reduce financial and

storage costs, and ensure harmonious relations with our providers.

Biometrics at our stores: There was a great deal of initial enthusiasm at M&G Superstores when the face-voice biometric application was introduced. Our "enrol and win!" promotion was a huge success, and the numbers indicate a substantial rise in customer traffic due to the novelty effect of biometrics. However, our Customer Services department have since received a series of customers' complaints:

- Profiling: customers seem concerned that we are monitoring when they come to the store and what they purchase. Although this is something we used to do anyway with our customer loyalty cards, there seems to be resistance to biometrics being used for this purpose. We are currently considering installing a pseudonymous biometric system, where the only information collected regards the spending patterns of our customers and some general information about them – but not their identity.
- Delays at entrance: customers seem irritated with the biometric system at the entrance, which causes delays. Although they have the option to by-pass this entrance, they need to queue in order to benefit from the savings of our "check in, check out" promotion.
- Respecting disabilities: we at M&G Superstores have a comprehensive accessibility policy. However, some disabled people are discriminated against because they cannot enrol in our biometric systems. Common sense and customer service should prevail, allowing for the disabled to enjoy the same benefits as everyone else. In the words of Miles Graham: "Don't forget or neglect – just respect".
- Given the positive results with the discotheque trial, senior staff are urged to set up collaborations with local companies (e.g. movie theatres, video rental shops, etc.) to join our 'only enrol once' program. The details of this program will be explained via the intranet training system, but it is imperative to have many local companies participating. Sharing our biometric database equals sharing of investment costs while for consumers, the convenience of a single enrolment needs to be highlighted.

While we should all be positive and enthusiastic about the business opportunities that biometric technologies offer, the Management recognises the teething problems involved with large scale implementation of biometrics. Senior management are asked to keep this in mind, to apply common sense where necessary, and remember we have invested in biometrics in order to gain a competitive edge and survive in a competitive market. It is up to you to ensure we succeed.

## SCENARIO 3: BIOMETRICS IN HEALTH

Dr. Adele Mattsson, a paediatrician, and Dr. Vasily Nowak, a neurologist, used to work together at the same hospital until Dr. Nowak moved to a different country about a year ago. They now keep in contact via email.

### First E-mail

**From:** Mattsson Adele
**Sent:** 04 February
**To:** Nowak Vasily
**Subject:** News from the hospital

Dear Vasily,

There have been lots of changes at the hospital. We now have different biometric systems implemented. The first one to be installed was the physical access system for the medical supplies storerooms. Rather than having to type in a code to unlock the door, we now have a verification system that works with smart-cards and iris recognition. The hospital issued off-the-shelf smart-cards to all authorised people, which store our iris template. To enter the storerooms, we have to bring our card near the sensor, position ourselves correctly in front of the system, focus on the iris reader, and then wait for the matching process to occur. Once our identity has been verified, we are allowed to enter. The system keeps a log of everyone who has accessed the storeroom and it makes use of RFID tags[3] on the supplies to audit what has been taken. I'll tell you something – there's been a noticeable drop in the quantity of supplies we use up each month but also a reluctance from staff to be the one to retrieve legitimate supplies. After the success of this first system, hospital management looked into other applications for biometrics (with much encouragement from biometric suppliers). Some of them have worked very well while others quickly proved to be impractical.

Network access was one of the next areas to be tackled. You remember that IT staff asked us to choose long passwords and to change them regularly, but that rarely happened. It didn't help that we were asked to pick a different password for every system (patient records, financial records, appointment schedules). Now we have single sign-on access for all systems. We use our fingerprint as a password when accessing medical records; our workstations and laptops now have fingerprint readers on the mouse. This is checked against the central database, which stores our fingerprints and access rights. There was a long discussion about the choice of biometric; some people were wary about using fingerprints, or any other biometric which requires a contact reader because of the high risk of cross-contamination. That was the reason after all that iris recognition was chosen for access to the storerooms. But good-quality iris scanners are expensive and we didn't have the funds to install one on every workstation. In the end a compromise solution was reached. The fingerprint readers are irradiated periodically with UV light and they are cleaned regularly. The latter improves reader accuracy and now that everybody has learned how to place their finger on the reader correctly, we have few usability problems.

Like I said, there were other ideas that were simply unworkable. Others were implemented in a rush without taking into account working practices or the obvious logistical problems. For example in an effort to ensure that patients would always receive the correct medicine, the nurses were armed with PDAs complete with mobile fingerprint scanners. The idea was that patients would enrol their biometrics upon entry to the

[3] Radio frequency identification **(**RFID**)** is a method of remotely storing and retrieving data using devices called RFID tags. *Source: Wikipedia*

hospital and then the nurse would check the patient's biometric against the template stored in the PDA, each time before administering a medicine, in order to confirm the patient's identity and the prescription. You can imagine the difficulties that arose. Sometimes patients had bandaged hands or damaged fingers and it wasn't possible to get a reading; other times the nurses didn't need to check the fingerprint because they knew the patient well, but the system required every patient's biometric to be logged when receiving medicine. The risk of cross-contamination with patients was so high, that nurses had to be very careful to clean the reader thoroughly after each use. This added enormous time overheads to their work. Hospital management eventually decided to withdraw the fingerprint readers and replace them with a more practical system using RFID tags. After all biometrics aren't always the right solution.

I hope everything's going well for you with your new medical practice. I've read a lot about the implementation of national health cards over there and I was wondering what your views are on the matter.

Best wishes,

Adele

## Second E-mail

**From:** Nowak Vasily
**Sent:** 09 February
**To:** Mattsson Adele
**Subject:** Re: News from the hospital

Dear Adele,

It's good to hear from you and it sounds like the hospital is as busy as ever. How is everyone coping with the new systems? I've seen examples like the ones you described. Results depend indeed on the application and the implementation.

One use of an internal biometric that has caught on at many maternity wards here is a DNA register that ensures new mothers take home their own baby, preventing mix-ups and babies being taken illegitimately. Mothers-to-be give a sample of DNA when they enter the hospital, which is analysed and the template is stored. Soon after birth a DNA sample is also taken from the baby. The mother's and baby's templates are linked in the database which is read-only, preventing anyone from tampering with the records. Of course the samples are discarded once they have been used to generate a template, and the templates are only stored until the mother and the child leave the hospital.

The health card is also an interesting application. Contrary to what some people think there is no centralised database of medical records. Something like that may be implemented in the future but for now the costs of securing the data, due to privacy concerns were judged to be too high. In fact the national health card we have is little more than an ID card with some medical information. The health card here though also stores the image of a biometric on the smart-card which they say is to enable medical staff to authenticate a patient's identity with greater confidence, but I haven't seen a use for that yet because in practice nobody asks patients to undergo a biometric check. The full image was chosen over a template to avoid tying down all hospitals and medical practices to one technology supplier. Hopefully biometrics will soon be standardised at a European level; it will then be possible to store the template alone whilst allowing for full interoperability, leaving more space for medical information.

The main driver for these biometric cards was to cut down on identity fraud in the health sector and to limit healthcare to those who are entitled to it; having said that, the benefits aren't limited to the government or private insurance companies alone. Several cases have been reported where the allergy or medication information on the card saved a life.

An area where I see real potential for biometrics is home healthcare. Biometrics can offer much greater confidence in remote authentication processes than passwords or

tokens. Ideally everyone would have a good-quality iris scanner or fingerprint reader attached to their own computer so that they could access their medical files from the privacy of their own home, but I think we're still a long way off from that.

Please send my regards to everyone at the hospital.
I hope to hear from you soon,

Vasily

## Third E-mail

**From:** Mattsson Adele
**Sent:** 16 February
**To:** Nowak Vasily
**Subject:** Re: News from the hospital

Dear Vasily,

You asked how everyone here is coping with the new systems. I would say pretty well on the whole. In the beginning we had training courses to help people enrol their biometrics and show them how to use the biometric readers. Some were already familiar with biometric technologies, having used them at airports or in other areas; others had to learn, but did so quickly. In general when we can see the purpose and the usefulness of the new technology, we are quick to accept it. Problems arise if the technology is introduced as part of a badly thought out application.

Of course there is also the issue of visibility and liability which concerns many of us doctors. If a patient is in a critical condition, we sometimes carry out risky procedures in order to save a life. If biometric identification is used to track our every action though, who can say whether doctors will risk personal liability in order to go the extra mile?

On the subject of medical record databases, I too was very sceptical at first because of well-known privacy risks. But there are ways of creating databases without sacrificing anonymity. Biometrics can be used as a tool to achieve this. The medical record can be stored with the person's biometric as the key. It contains no personal identification data. In a database of millions, the only way of locating the correct record is to have the biometric key and of course the only person who has that is the one to whom the record corresponds. Clearly there are technological challenges here, a very accurate biometric technology is needed to perform this kind of one-to-many search, there have to be back-up procedures in case someone's biometric changes, for any reason. All this exemplifies how biometrics are not in themselves 'good' or 'bad' but a tool that can be put to good or bad use.

I have to go now but stay in touch.
Take care,

Adele

## SCENARIO 4: BIOMETRICS AT THE BORDER

John Braun is an EU citizen who regularly makes trips for business and leisure. For him, travel has always been a hassle, particularly the long queues and waiting times at airport terminals. When biometric schemes for frequent travellers were introduced, quite a few years back, he was among the first to join. On his next trip, during the month of August, John will be travelling with his 78-year old father Gerard and his 9-year old daughter Martine.

### At the travel agent

First John goes to his travel agent.

"Good morning, I'm here to pick up three tickets booked in the name Braun."

"Certainly, just one moment...
Here we are. Three tickets, two adults, one child, flying from Amsterdam to Dubai on July 27th.
Leaving Dubai on August 2nd for Beijing.
Finally departing Beijing August 16th, with a 4-day stopover in Bangkok, arriving Amsterdam August 21st.
That's quite a journey you've got ahead of you! Would you also like our help in arranging visas for your destinations?"

"Yes please."

"Well, for Dubai you don't need a visa. The UAE have a watchlist system using iris recognition. They store the iris pattern of those who have been deported or banned from the country for whatever reason and then they might ask you to pass an iris scan to check that you're not on their list. For Thailand and China you will need a visa however. Thailand has chosen the iris as the biometric for its visa system."

"The iris... we don't have the iris on our passports. Does that mean we'll have to go to the embassy?

"Yes unfortunately it does. All passengers will have to go to the embassy to enrol in person. But I'm assured that the process doesn't take too long."

"How about China? I've heard that they make all passengers do DNA tests."

"Well that's partly true. They ask visa applicants to provide a DNA sample which they will analyse in order to obtain a DNA fingerprint. It doesn't take too long though again you have to go to the embassy in person. They attach this "fingerprint" to your visa but they don't check everyone's DNA as they pass the border. In fact only under exceptional circumstances will they ask you to undergo a DNA test while there. They use it for foreigners who have broken the law, drug traffickers, smugglers and so on. Nothing that would apply to you and your family."

"But we still have to go to the embassy to provide a DNA sample."

"Yes I'm afraid that's standard procedure. I'll start the applications for you. When you go to the embassy, you quote the reference number and all you will need to do is enrol your iris/DNA as appropriate."

**A month later, John, Gerard and Martine go to the Thai embassy.**
They present themselves at the visa office with the reference number from their travel agent. The official first has to check their passports to ensure that the correct people are enrolling their data. If the enrolment is fraudulent (i.e. a person enrols their biometric data, but it is linked to someone else's identity) then the whole visa application is compromised. Having had their identities confirmed, John, Gerard and Martine wait in line to enrol their irises. This can be a cumbersome process as it may take more than a few attempts. Martine has never used an iris scanner before so the embassy employee has to help her through the process, telling her where and how to focus her eyes.

At the Chinese embassy the process is similar, only this time rather than scanning their irises, they are given a swab of cotton and asked to wipe it against the inside of their cheek. The DNA analysis will take at least an hour so the family go for a quick lunch before returning to have the visa chip affixed to their passport.

**At Schiphol, the trip starts.**
"Daddy, why are we waiting?"
"We're waiting to get our passports checked dear"
"But why don't they check them when we go to Spain or France?"
"That's because those countries are inside something called the Schengen zone and inside that zone they don't have to check our passports."
"But why do they have to check them now?"
"Because we're leaving the Schengen zone, they have to check to see if we are who we say we are"
"But daddy why..."
"Just wait a while till we sit down on the plane Martine and I'll explain anything you want."

On the flight, while John answers his daughter's endless questions, Gerard glances over the in-flight electronic magazine.

**In-Flight Electronic Magazine**

**SCHIPHOL PROUD TO ANNOUNCE NEW BIOMETRIC SAFETY MEASURES**

On July 1st, Schiphol Airport announced new safety measures designed to make its customers feel even safer. Fingerprint readers have been installed in air traffic control towers to ensure experienced staff are always present in the control tower. Schiphol spokesperson, Daphne Dorst said, "Biometrics are generally associated with identification for security purposes, but just as important is their ability to confirm a person's presence at a specific location. By incorporating the readers into the keyboards used by controllers, we are able to monitor presence in the control tower and thus guarantee that our customers are always in the best possible hands."

**UAE border control**
When the family reach Dubai, they go through passport control which is a similar process to the one at Schiphol. The immigration officials choose who has to pass by the iris scanner so that the authorities can check they do not appear on the watch-list. The Braun family can walk straight through, and are allowed to proceed to baggage collection without scanning their irises.

"I'm sure that can't be very secure," Gerard comments to his son. "They didn't scan our irises. How do they know we aren't on the watch-list?"
"They have a system called Advanced Passenger Information or API," John explains, "From the moment we booked our tickets, the airline forwarded our information to the UAE immigration authorities. They've done background checks on all the passengers and they can identify in advance which ones they need to question. The officials use their own judgment to decide who to examine further."

**After a week in Dubai**, the Braun's journey continues with a flight to Beijing. On the plane, John picks up the newspaper and an article catches his eye.

A TRAGIC AFTERWORD TO THE MOTTI CASE

How can we make the witness protection scheme work in a world where biometrics are everywhere? That is the question police and judicial authorities are asking themselves after the main witness from last year's Motti trial, was reportedly murdered late last night.

The victim, Lucy X, will be remembered for providing the key evidence that led to the conviction of Mr. Motti. Having received death threats, both before and during the trial, Lucy X was offered a new identity and a new life under the witness protection scheme. She traded in her old name and old passport for new ones; unfortunately she could not do the same with her biometrics. Prior to the trial, Lucy X had been enrolled in a number of private biometric schemes with supermarkets, banks, fast-food chains, and other stores.

Police suspect that this information was accessed by Mr. Motti's associates, who traced the biometrics to Lucy X's new identity.

Seven hours later, the Brauns have arrived in Beijing.

"Daddy are they going to do DNA tests on all of us to check who we are?"
"No Martine, I think the process will be similar to what we went through at Dubai."
"But then why did we have to go to the embassy to give a DNA sample?"
"We gave the sample so that if the authorities have any doubt about who we are, they have a way to test it. In that case they would ask us to wait at the airport for about an hour while they analysed a sample of our DNA in order to match us to our visa. But don't worry Martine, they are unlikely to check us."

The family make their way through passport control without being asked to undergo a DNA test and the face recognition system does not cause any problems

either. Beijing airport spent a vast sum of money preparing for the 2008 Olympics and in order to control the problems face recognition systems have with lighting conditions, they installed cameras in small booths with controlled lighting and no reflective surfaces, which continue to function satisfactorily.

**In Bangkok two weeks later**, things don't go quite so smoothly. Gerard suffers from glaucoma and this means that spots can sometimes appear on his iris, which confuses the iris recognition system. The technology is believed by some to be infallible, because it always produces a match by the third attempt. When Gerard's iris fails to match the one stored for his visa, officials ask him to step aside for further interrogation. John tries to explain his father's medical problems, but the officials have to follow standard procedures. Eventually they receive confirmation from the Thai embassy in the Netherlands, that Gerard Braun has indeed been issued with a visa and they let him through after a lengthy wait.

**Arriving back at Amsterdam**, the family once again wait to go through passport control. Gerard turns to his son and says, "I remember when I used to travel with your mother, we rarely waited in such long queues. The passport officials waved everyone through. Sometimes they barely glanced at the passport." "Oh it's not so awful now Dad. It may take us a bit longer to get through passport control but look at it this way: if we weren't waiting here, we'd be waiting for our luggage. At least our bags will be waiting for us by the time we pass all these biometric checks."

# CHAPTER 1: BASIC BIOMETRIC CONCEPTS

## *1.1 Definitions*

### 1.1.1. What are biometrics?

A biometric is a physical or biological feature or attribute that can be measured. It can be used as a means of proving that you are who you claim to be, or as a means of proving without revealing your identity that you have a certain right (e.g. access), just like a PIN (personal identification number) or a password. The crucial difference is that the biometric is something that is part of you, rather than something you know or can carry with you (Hopkins, 1999). Examples of physiological biometric features include height, weight, body odour, the shape of the hand, the pattern of veins, retina or iris, the face and the patterns on the skin of thumbs or fingers (fingerprints). Examples of behavioural biometrics are voice patterns, signature and keystroke sequences and gait (the body movement while walking). While it is sometimes argued that DNA should not be classified as a biometric, because it is not externally observable, for the purpose of this study DNA is considered a biometric, in so far as it is a body feature which can be used for identification and verification purposes.

Biometric characteristics are said to be 'distinctive'. The distinctiveness of a biometric varies by the technique used to measure it and the process through which two similar biometrics are declared as matching. Thus, no biometric feature sampling process is exactly repeatable. Biometric characteristics can be considered as a bridge between an identity record and the individual this record belongs to. In this way it establishes a 'trusted' method to strongly link the stored identity with the physical person it represents. This type of biometric identity verification is desirable and needed on many occasions.

The key difference of biometrics to other digital identifiers, such as passwords, PINs or credit cards is that biometrics cannot be lost or forgotten; since biometric measurements are part of the body, they will always be present when needed. Moreover, the process of identification is automated or semi-automated. In some cases this automation mimics something humans do in everyday life (face or voice recognition), but for most technologies automation is necessary because humans alone would not be able to distinguish different individuals (iris recognition, hand patterns).

Biometric (just like traditional) identification works in four stages: enrolment, storage, acquisition, matching. Firstly, individuals are enrolled, i.e. a record associating the identifying features with the individual is created. For example, an iris scan is performed and the result is labelled "John Miller". Secondly, a record of that scan is stored somewhere. There are two options for storage: the records can be stored in a central database, or in a decentralised way, for example on smart cards or tokens. Thirdly, when identification is required, a new sample of the feature is

acquired (a new iris scan performed). Finally, the newly acquired record is compared to the stored record. If they match, the individual has been identified[4].

### 1.1.2. Features of biometric identification

Biometric identification is a statistical process. Variations in conditions between enrolment and acquisition as well as bodily changes (temporary or permanent) mean that there is never a 100% match. For a password or a PIN, the answer given is either exactly the same as the one that has been stored, or it is not – the smallest deviation is a reason for refusal; for a biometric, there is no clear line between a match and a non-match. Whether a match exists depends therefore not only on the two data sets to be compared, but also on what margin of error is deemed tolerable. A 90% probability of a match may or may not be considered acceptable, depending on the implementation of the biometric in question and the application security requirements.

As a consequence of this statistical nature, biometric systems are never 100% accurate. There are two kinds of possible errors: false matches, and false non-matches. A false match occurs when an acquired template is erroneously matched to a template stored from enrolment, although the two templates are from two different persons. A false non-match occurs when an acquired template is not judged to match the template stored from enrolment, although both are from the same person. These error rates vary from one biometric technology to another, and they depend very much on the setting of the threshold above which a "match" is calculated: a 99% threshold will have more false non-matches and fewer false matches than a 98% threshold, and so on.

Any biometric application must therefore provide a fallback procedure to deal with these errors. Fallback procedures are equally necessary to deal with people who have difficulties to provide a sample of any given biometric. This can be permanently, e.g. for sight-impaired people using an iris recognition system; or it may be temporarily, e.g. for an individual with a bandaged face using a face recognition system. The percentage of the population giving rise to a variety of such problems may be small but significant. Therefore, fallback procedures will need sufficiently flexible human involvement to handle the variety of potential problems.

A second point worth mentioning is that the biological data themselves, the so-called samples, need not actually be stored in the biometric identification systems[5]. Iris pictures, fingerprints and faces are converted via mathematical algorithms and stored into fixed format files so-called templates. The use of biometric algorithms facilitates the statistically constant matching of the features extracted during acquisition. Whilst the algorithms are different for each technology, this procedure is usually non-reversible, i.e. it is not possible from a template to recreate the sample which was its source. Another advantage of the use

[4] More in detail on system architecture is provided in chapter 2 on Biometric Technologies
[5] However, sometimes the original samples are stored outside the biometric identification system database, for example DNA in criminal investigations.

of algorithms to create templates is that a new and different template can be produced if the previously produced template has been stolen and is abused by a third party, even though the biometric characteristics of the body themselves are not revocable - your fingerprint remains your fingerprint, even if someone else has obtained a copy of it.

## *1.2 The seven pillars*

Biometric features include various subsets of body characteristics, but not all such subsets are suitable for identification purposes. For example, a photograph of one particular body part (the face) is sufficient for many purposes, while a photograph of other body parts (say, elbows or feet) is useless. The evaluation whether a particular body characteristic is suitable for biometric use can be done on the following seven *criteria* (Jain et al., 1999):

TABLE 1: Seven pillars of Biometric Wisdom

| | |
|---|---|
| **Universality** | All human beings are endowed with the same physical characteristics - such as fingers, iris, face, DNA - which can be used for identification |
| **Distinctiveness** | For each person these characteristics are unique, and thus constitute a distinguishing feature |
| **Permanence** | These characteristics remain largely unchanged throughout a person's life |
| **Collectability** | A person's unique physical characteristics need to be collected in a reasonably easy fashion for quick identification |
| **Performance** | The degree of accuracy of identification must be quite high before the system can be operational |
| **Acceptability** | Applications will not be successful if the public offers strong and continuous resistance to biometrics |
| **Resistance to Circumvention** | In order to provide added security, a system needs to be harder to circumvent than existing identity management systems |

We will evaluate each of the four biometrics technologies covered in this report (fingerprints, face recognition, iris recognition and DNA) according to these seven criteria in chapter 2. However, one must bear in mind that the degree to which each criterion must be fulfilled by a biometric depends clearly on the application for which it is used. A border control check must be done in a few seconds; a criminal investigation can take months. A convenience application, say highway tolls, may

accept a significant error rate; a banking system will require a much lower one. It is therefore necessary to look at the purposes for which biometrics can be used.

## *1.3 Biometric Application Types*

In functional terms the current uses of biometrics can be categorised under the following headings: verification, identification and screening. Another potential use of biometrics, though not yet in a mature state of development, is biometric encryption.

### 1.3.1 Verification (1-to-1 matching)

Verification[6] is a test to ensure whether person X is really who he or she claims to be. Two types of verification can be envisaged: with centralised storage or distributed storage.

a) Verification with centralised storage

If a centralised database[7] exists (produced once at enrolment and updated with each additional user) where all biometric data and the associated identities are stored, the biometric sample of the claimed identity is retrieved from the database. This is then compared to the live sample provided by person X, resulting in a match or a non-match. Two types of error are possible for verification: (i) a false match (person X is not who he claims to be but the system erroneously accepts him, i.e. acceptance of an impostor; also known as false positive) and (ii) a false reject (person X is who he claims to be but the system fails to make the match, i.e. rejection of a legitimate person; also known as false negative). The matching can be done locally on the device temporarily storing the acquired sample or remotely by the hardware that stores the sample acquired during enrolment. False rejects will cause unnecessary inconvenience to innocent individuals whereas false matches are more insidious as they allow a fraudulent individual to pass, but the mistake goes unnoticed by the system.

b) Verification with distributed storage

If the biometric data is stored in a memory device[8] that is carried by the individual, for example a smart card or a chip integrated into an identity document, person X will provide a live biometric sample and this will be compared to the biometric data stored on the memory device. This can be done either by the verification system which retrieves person X's biometric data from the memory device and compares them to the live sample, or by the memory device itself, if it is sufficiently

[6] Although the process of verification is sometimes termed positive identification to avoid confusion the term verification will be used throughout.
[7] In this section we assume that the database has not been tampered with and that information has been enrolled correctly without fraud.
[8] Memory devices can be anything from barcodes or magnetic strips, to contact or contactless IC chips

sophisticated to perform the verification[9]. The identity details are either stored on the memory device or written on the accompanying documents e.g. in the case of a passport, identity information might be printed next to the chip. If the verification process succeeds, then person X is confirmed to be the valid bearer of the identification documents. As before, false acceptance and false rejection errors are possible. In addition, there is the possibility that the documentation or the memory device are fraudulent or have been tampered with.

### 1.3.2 Identification (1-to-many matching)

Identification is used to discover the identity of an individual when the identity is unknown (the user makes no claim of identity). Contrary to verification, for the process of identification a central database is necessary that holds records for all people known to the system; without a database of records, the process of identification is not possible.

When person X comes to be identified, he provides a live biometric sample, e.g. a fingerprint is taken or the iris is scanned. The data is processed and the resulting biometric template is compared against all the entries in the database to find a match (or a list of possible matches). The system then returns as a response either the match (or list of possible matches) it has found, or that there is no match against the enrolled population. Identification may result in one of two types of error described previously: i.e. a false match or a false reject. Since the system checks against a database of enrolled templates or full images, the maintenance of the integrity of the database is essential in protecting individuals from identity theft.

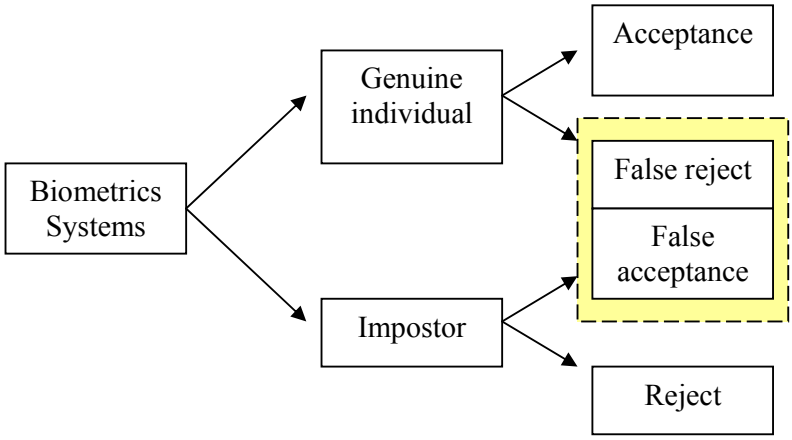



FIGURE 1: Generic Biometric system process (EUR20823EN, 2003)

### 1.3.3 Screening

The third type of process is screening, which makes use of a database or watch-list. A watch-list contains data of individuals to be apprehended or excluded. A record on the watch-list may contain only biometric data for a wanted individual or may also have identity information, depending on what is known. Everyone who passes

[9] In this case the memory device would have to be a chip with an on-board processor.

the screening process provides a biometric sample, which is checked for matches against the watch-list. The key feature of a watch-list is that people are not on the whole identified; they will only be identified if they appear on the list. If there is no match the person passes through and their biometric sample should in principle be discarded. In the case of a match, a human operator decides on further action. Screening can take place overtly, for example at border control or covertly, such as scanning a crowd with the use of security cameras.

### 1.3.4 Encryption

This technology is still in a very early phase and will not be available for large-scale applications in the near future. With biometric encryption, no biometric sample is stored; instead an individual uses one of his physiological characteristics as a kind of encryption and decryption key in order to encode and decode information. Since the process of creating a template is irreversible there is no fear of anyone else being able to re-create the encryption key while the rightful owner is the only one that can decode the information. However, there are technological challenges to overcome if this application type is to be widely deployed, such as the fact that biometric samples are only statistically similar[10].

### 1.3.5 Biometric Applications: what they are used for?

Biometric identification and verification systems will be increasingly used in the future. One reason is that in a society that is increasingly mobile, flexible and digital, there is a need for more efficient identification systems. A second reason is that criminals have acquired great expertise in circumventing the old identification systems. In addition, as biometric technologies become better, cheaper, more reliable and more convenient, they will increasingly be implemented in other environments such the everyday life, in businesses, at home, in schools, and in other public sectors. This can be labelled the "diffusion effect".

In practical terms, biometrics will be used mainly for four purposes[11]: law enforcement, physical access control (including border control), logical access control and convenience. Traditionally, the most widespread use of biometrics has been in law enforcement. Fingerprints have been used since the 19th century, and more recently DNA analysis has become routine in assisting criminal investigations. It is due to this history that many citizens associate enrolment in biometric systems with criminals and hence tend to resent it. Therefore, it is important to underline that law enforcement is only one among many possible application areas.

Law enforcement is however until now the only area where large-scale applications have been in use for some time. Physical access control based on biometrics has so far been mostly limited to private companies' premises, i.e. small-scale applications. However, there are a number of trials underway or recently completed, many of which are at airports, which have tested biometrics access with large

[10] Further information to be found at: http://www.dss.state.ct.us/digital/tomko.htm
[11] See also chapter 3.2.3 "The biometrics market"

numbers of customers, rather than employees. Most importantly, on the government side the integration of biometrics into passports and visas will for the first time create truly large-scale physical access control applications.

Logical access control (in particular online identity) is forecast to be a fast growing use of biometrics. With more and more transactions such as e-banking, e-commerce and e-government taking place online, biometrics offer a promising way of establishing secure identities especially when face-to-face contact between the participants in the transaction is not possible. This is particularly important for high-value financial transactions and for the transmission of confidential data (for example tax returns). Logical access control will also include access to entitlements offline, such as social security pay-outs.

Finally, convenience applications include all uses of biometrics where individuals voluntarily participate because they find it advantageous to do so. This would include ambient intelligence applications such as personally-adjusted home lighting or e-toys, but also participation in biometric applications offered by private actors, such as shops, sports clubs or other, where participation is not mandatory.

These classifications are useful for analysis. However, while they are clearly distinct in theory, in practice the different structural and practical applications tend to be applied jointly. For example, in functional terms law enforcement has used biometric identification for several purposes: firstly, to verify the presence of a suspected individual at a scene of crime; secondly, to identify which among several individuals was present at a scene of crime; thirdly, to create a profile of an unknown individual known to have been present at a scene of crime. In other words, it is used for verification, identification and screening. Other applications, for instance e-health, may combine physical access control to the operating theatre with strict logical control of access to medical data.

## 1.4 The Issues

The widespread implementation of biometric applications raises a series of challenges. These will be considered in chapter 3 from a SELT perspective (i.e. social, economic, legal and technological). In addition, there are four issues which feature prominently in the discussion on biometric technologies, namely security, privacy, interoperability and costs, which will be discussed now. Medical implications are examined in chapter 2. The following table summarises the analysis:

TABLE 2: ANALYSIS of the MAIN ISSUES

| | | | |
|---|---|---|---|
| Interoperability (1.4.1) | | | |
| Security (1.4.2) | | | |
| Privacy (1.4.3) | | | |
| Costs (1.4.4) | | | |
| Medical (2.2) | | | |
| **Social (3.1)** | **Economic (3.2)** | **Legal (3.3)** | **Technological (3.4)** |
| Clarity of purpose, function creep and the trust model (3.1.2 + 3.1.4 + 3.1.6) | The economics of biometrics (3.2.1) | The current legal framework (3.3.1) | Evaluation of biometric systems (3.4.2) |
| Interoperability and equivalence of performance and process (3.1.3) | The biometrics market (3.2.2) | The need for new rules (3.3.2) | Challenges, limitations and multimodality (3.4.3 + 3.4.4) |
| The human factor and social inclusion (3.1.5) | Policy issues and policy levers (3.2.3) | Biometrics in court (3.3.3) | Application issues (3.4.5) |

* numbers in parenthesis are report chapters

### 1.4.1 Security

The security of an identification system, i.e. the degree to which it is difficult for a third party to circumvent it, depends on the entire system architecture, not only on the technology used. Biometric security cannot rely on secrecy, as is the case for passwords and personal identification numbers, because most biometrics characteristics of a person can easily be obtained by anyone: faces can be photographed, voices can be recorded, fingerprints can be taken from doors or glasses, DNA can be obtained from a single hair. Security measures must therefore rely on the operating characteristics of the system. As pointed out above, biometric identification systems work with the same four steps as traditional systems: enrolment, storage, acquisition, matching. In each of these steps, there is potential for circumvention.

At the enrolment stage, a person enrols as Mr. X on the basis of the non-biometric system previously used. If he successfully enrols under a fake name on the basis of fake documents, it will be impossible to detect his false identity with the identification system. He has, in fact, acquired a new identity. At storage level, it is possible to access the stored data and to manipulate it. Depending on whether the data is in a central database or on a memory device such as a smart card, one either needs collaboration inside the system, or advanced technological knowledge, or both. At the point of acquisition, the degree of difficulty in faking biometric data (so-called 'spoofing') depends on the biometric used. For example, fake fingerprints in the past could relatively easily circumvent simple systems, but the increasing sophistication of fingerprint techniques (e.g. the addition of tests for liveness) makes it ever harder to provide fake data[12]. Independent of what may be done to circumvent the system during the acquisition stage, the system may also be spoofed at the matching stage. For example, at the time of matching, with sufficient collaboration from a system operator, it is possible to lower the acceptance threshold to a point where detection of intrusion becomes unlikely.

Other factors that need to be considered include whether the stored data is encrypted or not and the choice of method for transmitting data, either from the central database or from the token or smart card (contact or contactless interaction). A number of technical/security precautions well-known from securing data and data transfers ought to be applied. This improves security but at the same time increases costs. In general it is important to do away with the assumption that the use of a biometric identifier is an absolute proof of identity. Biometrics are subject both to errors (see above) and to circumvention. True, they should be more secure than traditional identification systems – after all, this one of the main drivers for the increasing use of biometrics, but they are not perfect. If the possibility of error or fraud is ignored, then the overall security level will actually be lowered, as people will place greater trust in those with a fake biometric ID than they ever placed in those who had a fake paper ID.

### 1.4.2 Privacy

Biometric identification and verification generates digital data. Primarily of course there is the data used as an identifier – for example the fingerprint template. More delicately, it creates a machine-readable trace every time identification is performed. From a data protection point of view, it therefore raises the usual questions: what data are stored, how are they stored (centrally in a database or decentralised on smart cards), who has access to the data, for what purposes can the data be accessed, etc. The answers to these questions, and their compatibility with existing legislation, depend on the system architecture and are only marginally related to the characteristics of particular biometric techniques. In chapter 3.3 we will look more closely at the applicability of data protection legislation and in particular whether the characteristics of biometrics allow the current legislative framework to develop its full impact.

[12] For details on the security concerns of the selected biometric technologies, see the annex

In addition, privacy is closely linked with the question of user acceptability. Apart from the merits of privacy in itself, an identification system where citizens feel that their data is not sufficiently protected and their privacy not sufficiently respected will not be able to obtain the necessary cooperation from the population. We will come back to this issue in chapter 3.1.

### 1.4.3 Interoperability

As for any emerging technology, interoperability plays an important role for the development of biometrics. For example, the more widely a memory device carrying biometric identification can be read, the more useful it is. This applies both on the geographical level, where it is clearly helpful if a passport can be read at both ends of a plane journey, and on the sectoral level, where it makes life easier if the same card can be used for a cash machine and for social security purposes. Note however that this does not necessarily mean that the same biometric must be used: one card can carry multiple biometrics, only one of which at a time is then consulted by the corresponding machine[13].

There is significant work being done at national and international levels to develop standards, which will be useful in promoting open systems development and interoperability. However, contrary to "normal" technologies, interoperability in biometrics may not always be desirable, in the sense that absence of total interoperability may create barriers which could limit transfer of personal data and thus protect against abuse. But since technical interoperability is to be expected in the future, the need for also developing other types of safeguards against abuse grows as well.

Moreover, since individuals have many different biometrics at their disposal, there is the possibility for different applications to make use of different biometrics. Also, systems that are incompatible at the biometric level, say a central database iris recognition system and a memory-device fingerprinting system, can still be compatible at the data transmission level, i.e. they can still exchange data about place and time of performed identifications.

Finally, interoperability at the international level raises the question of the applicable data protection framework. This also shows that it is not only about technical interoperability; interoperability of processes may be more challenging especially when biometrics diffuse more widely in society.

### 1.4.4 Costs

Like any other identification system, biometric identification has a cost. This cost varies enormously between technologies: for example, DNA identification, which requires significant human intervention, is an order of magnitude more expensive than basic fingerprint recognition. But even within one technology, prices will vary enormously between low-end and high-end equipment. Since the choice of the

[13] This is a different issue from the use of multiple biometrics for the same instance of identification/verification, see chapter 2.8

technology and the required level of equipment depend on the concrete purpose for which the biometric identification system is used, it is that purpose which to a large extent determines the costs. The scale of the application is equally decisive, as fixed costs can be spread over more participants in a large-scale implementation. The cost calculation should equally include measures to ensure data safety (encryption, firewalls etc.) and data protection (tracing of data use). Finally, it is important to take total real costs into account: these include in particular the fallback system, which is indispensable in any biometric application (see above), the necessary supervision expenditure to ensure that all categories of the population (children, elderly citizens) are included, and the set-up and running of the enrolment procedure.

Most biometric identification systems are still in a development phase and there is no real mass market, so no significant economies of scale are available yet. This should change once a sufficient number of large-scale applications are up and running. In addition, technological progress relying on advances in information technology should reduce costs over time. However, in the meantime those first applications will have to bear higher costs; afterwards, a rapid decrease in prices can be expected.

A key issue for the costs is of course who pays for them (see also section 3.2). This will depend mostly on the relative negotiating power of application implementers (government, companies and other organisations) and citizens. Since biometrics are supposed to reduce fraud and error, thereby reducing current costs for the implementers, one might argue that they should bear at least a part of the total cost. However, where the negotiating position of the individual citizen is weak, one should not be too surprised to see citizens bearing a large share of the cost.

### 1.4.5 Concluding Remarks

So far, we have provided the framework for a discussion of biometric identification. We have established what biometrics are, which criteria they need to fulfil, for which functional and practical purposes they are used, and we have introduced some of the key issues surrounding the implementation of biometric identification. Before we proceed to the in-depth analysis of the social, economic, legal and technical consequences of biometrics for society in chapter 3, it is therefore necessary to take a closer look at how each of the selected techniques (face recognition, fingerprinting, iris recognition and DNA identification) actually work, and at how their technical differences shape their impact on society. Chapter 2 will also consider the medical aspects of biometrics.

# CHAPTER 2: BIOMETRIC TECHNOLOGIES

In order to better understand the challenges posed by biometric technologies, this chapter provides some background information on the main technological issues of biometric systems, independent of the technology used, including their medical implications. It also presents an in-depth analysis of the four selected biometric technologies (face, fingerprint, iris and DNA), an overview of multimodal biometric systems and a comparison of these four technologies against the seven pillars set out in chapter 1.

## *2.1 Biometric systems: main technological issues*

Generally speaking there are two phases in a biometric system: a learning phase (enrolment) and a recognition phase (identification/verification).

### 2.1.1 Enrolment: root process of biometric systems

Enrolment, which is the very first step of any biometric system, consists of collecting the biometric sample through one or more acquisition cycles, processing the biometric data in order to obtain the reference template and finally storing it for subsequent usage. The efficiency, accuracy and usability of a biometric system depend directly on the enrolment process, since the result of the enrolment should be an accurate, usable reference template embedding the person's identity. There are many issues related to enrolment. These were investigated by an extensive trial, involving more than 10 000 users, which was carried out in the UK (2004). Some of the issues relate to the technology used, some to the format of the templates used and some to the possibility of storage in a central database vs. smart cards or tokens. In addition, during the life cycle of a biometric system it is sometimes necessary to re-enrol considering the natural but also the unexpected/accidental evolution of biometric traits (e.g. face, voice ageing, eye disease, hand injury, etc.).

### 2.1.2 Architecture of a Biometric System

There are six basic steps (see figure 2) of a generic biometric system (with the last two steps only being used during the recognition phase):

- Sample acquisition: first the collection of the biometric data must be done using the appropriate sensor; for example an image capture in the case of iris recognition or a saliva sample for DNA.
- Feature extraction: this step performs the transformation from sample into template. In general, the template is numeric data. (This step can be omitted if full images are used).
- Quality verification: this step establishes a reference image or template by repeating the two first operations as many times as needed so as to ensure that the system has captured and recognised the data correctly.

- Storage of reference template: this step registers the reference template. Several storage mediums are possible (see the following section) and the choice depends on the requirements of the application;
- Matching: this step compares the real-time input data from an individual against the reference template(s) or image(s);
- Decision: this step uses the result of the matching step to declare a result, in accordance with application-dependent criteria (e.g. decision threshold). E.g. for a verification task the result would say whether the user claiming an identity should be authenticated.

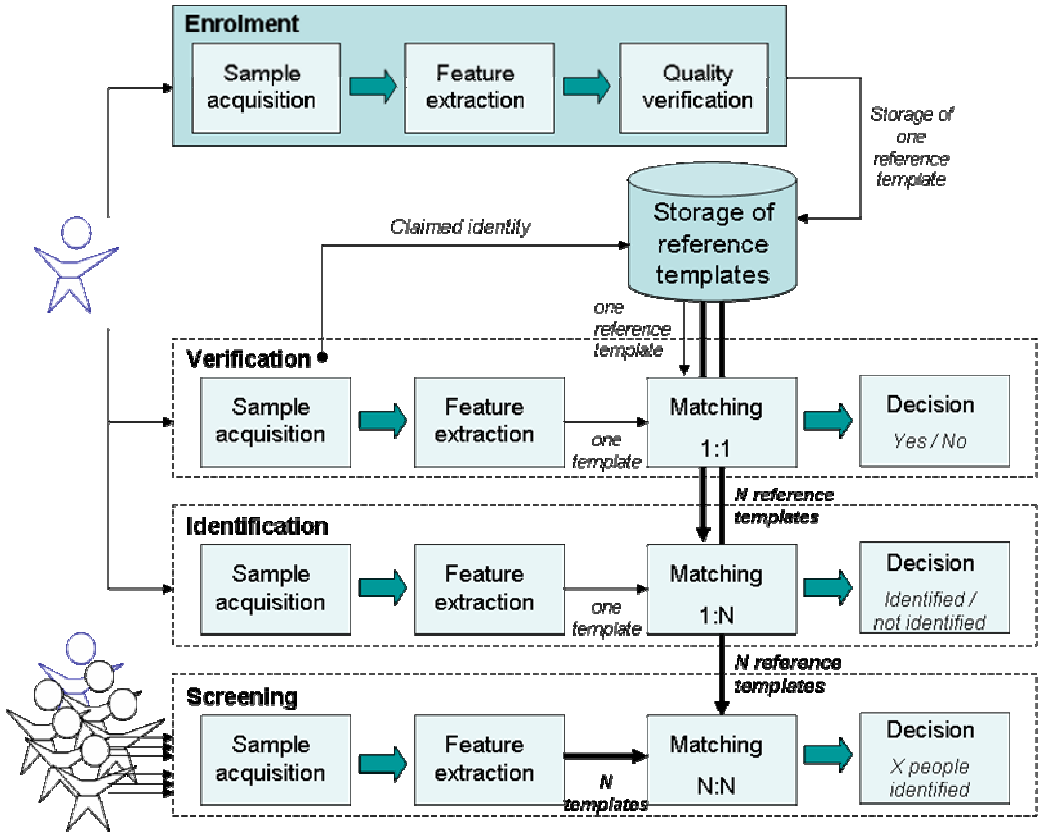


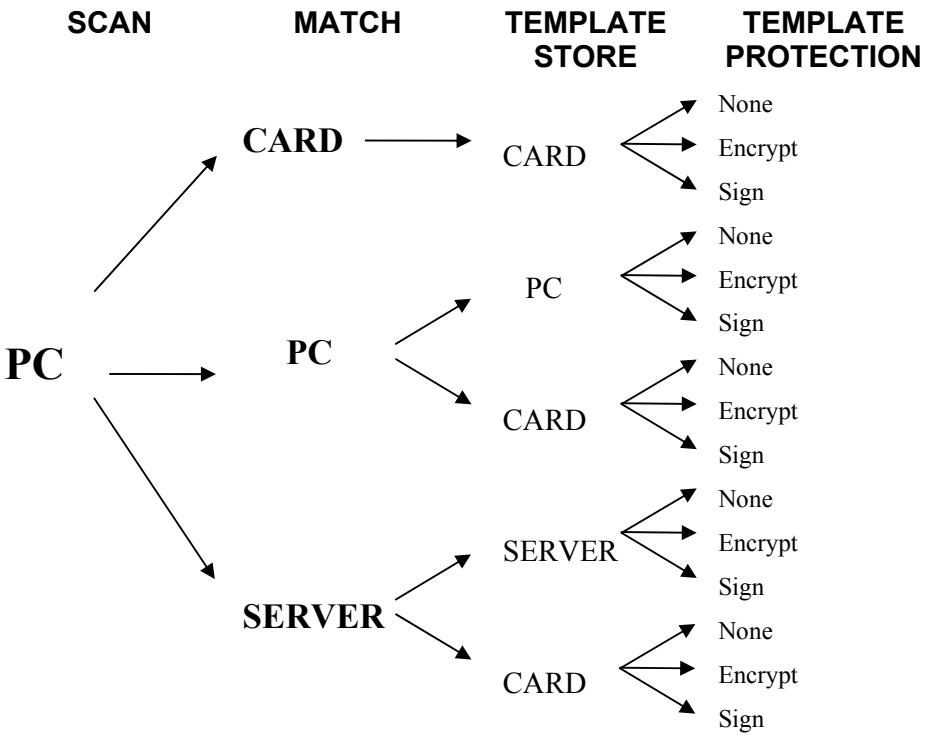

FIGURE 2: Enrolment and main use of biometric systems
- adaptation from Jain et al. 2004

### 2.1.3 Storage and protection of the template

Biometric systems have to scan, store/retrieve a template and match. It is important to note that depending on the design of the system, the match can be performed in different locations: on the processor that is used to acquire the biometric sample data, on a local PC or on a remote server, or on a portable medium such as a smart card (equipped with a strong enough processor). In addition, the reference template may be stored on the same three media leaving us with five different combinations

and resulting in five different levels of 'trust'. Moreover, there can be three different modes of protection that may be used for the template: no protection, data encryption, or digital signature. In total we have at most fifteen possible configurations (see table 1).

TABLE 3: Storage / protection of the template: 15 possible configurations[14]




There are advantages and disadvantages deriving from the use of each combination; the choice of combination is clearly application-dependent (based on risk and requirements analysis).

### 2.1.4 Accuracy of biometric system steps

The evaluation of a biometric system has to be based on the evaluation of all components: the recognition system performance, the communication interface, the matching and decision step and other key factors such as ease of use, acquisition speed and processing speed.

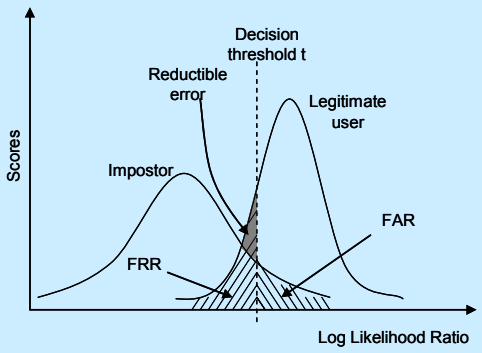
There is however, a method to compare biometric system performance based on the accuracy of the end decision only. As mentioned in chapter 1, in the case of a verification system there are two possible types of error: false non-match (also known as false negative or false rejection, i.e. rejection of a legitimate user) and false match (also known as false positive or false acceptance, i.e. acceptance of an impostor). The corresponding error rates are the **false rejection rate (FRR)** which

[14] http://www.dodait.com/cac/34_Biometrics/BiometricAlternativesBrf.pdf

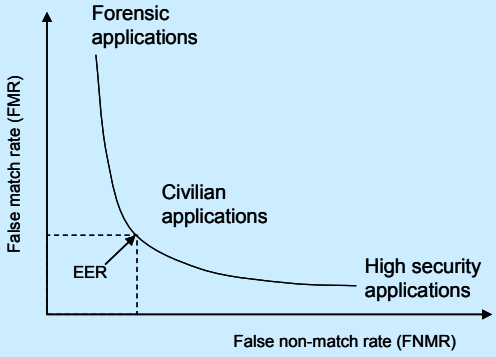
is equivalent to **false non-match rate (FNMR)** and the **false acceptance rate (FAR)** which is equivalent to **false match rate (FMR)**[15]. These error rates vary inversely, so for one technology under fixed operation conditions, lowering one error rate will necessarily raise the other.

Figure 3 displays graphically the distributions of legitimate users and impostors according to the response of the system which in general is a real number (likelihood). The decision threshold must be adjusted according to the desired characteristics for the application considered. This threshold must be calculated afresh for each application, to adapt it to the specific population concerned. This is done in general using a small database recorded for this purpose. High security applications require a low FAR which has the effect of increasing the FRR, while low security applications are less demanding in terms of FAR; FAR can thus be higher and therefore FRR can be lower.

FIGURE 3: Decision error rates and Receiver Operator Characteristic curves




**Curves "decision threshold":**
*The curves show false rejection rate (FRR) and the false acceptance rate (FAR) for a given threshold t over the legitimate user and impostor score distributions. The decision threshold must be adjusted according to the desired characteristics for the application considered.*




**Receiver operating characteristic (ROC) curve:**
*Different biometric application types make different trade-offs between the false match rate and false non-match rate (FMR and FNMR). Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor and user communities alike*

**Main source: (Jain et. al. 2004)**

The decision of acceptance or rejection is thus calculated by comparing the answer of the system to the decision threshold, which can be chosen so as to reduce the global error rates of the system. This global error rate also includes the **failure to enrol rate (FTE),** the **failure to acquire rate (FTA)** and also the **binning error rate**[16]. Other diagrams or curves are used in order to obtain a graphical view of the error rates for their interpretation, analysis and to support the decision making.

[15] A difference exists in the way these two equivalent error rates are calculated and interpreted.
[16] To improve efficiency in systems requiring a one-to-many search of the enrolled database, some systems may partition template data to separate "bins". A binning error (i.e. a kind of partitioning error) occurs if the enrolment template and a subsequent sample from the same biometric feature on the same user are placed in different partitions. Binning errors are assessed by counting the number of matching template-sample pairs that were placed in different bins and reporting this as a fraction of the number of pairs assessed (Mansfield et al., 2002).

Figure 3 shows the ROC (Receiver Operating Characteristic) curve. The point where FAR=FRR, and thus the point where the Equal Error Rate (EER) is obtained, signals the best choice of operation for a specific biometric for common civilian applications.

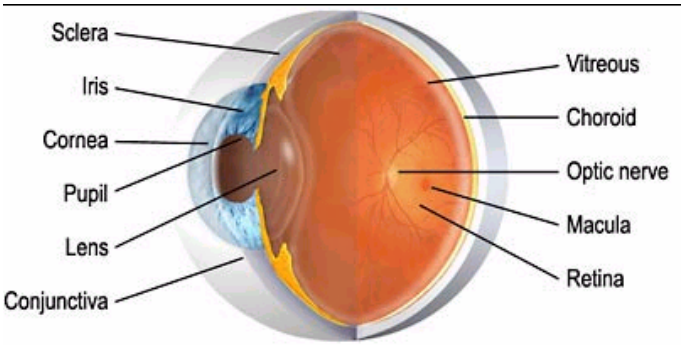
However, biometric systems must be considered as one element of a larger more complex identification module which is in itself part of a larger application. Biometric systems therefore need to be evaluated as a part of a whole application or process.

## *2.2 Medical Aspects of Biometrics*[17]

Biometrics, like other innovative technologies in the past, may raise public concerns regarding possible damage to the human body as well as ethical concerns derived from the use of physiological data. One should not, therefore, underestimate the perception of potential hazards on health and risks associated with the use of biometric devices, including fears about the secondary uses of data acquired. Two types of medical implications have been raised: direct medical implications (DMI) and indirect medical implications (IMI). The former refer to the potential risks of damage associated with the use of biometric devices, and the latter relate to the ethical risk of biometric data being used to reveal private medical information. Both types of implications can be seen as fuzzy quantifications of risks, but DMI refer to physical, measurable potential damaging effects, whereas IMI are about the possibility of extracting medical information that could be used for purposes other than identification and verification.

### 2.2.1 Direct Medical Implications

There are just a few direct medical implications (DMI). One technique that has potential DMI is retinal scanning, which analyses the layer of blood vessels at the back of the eye. The scanner uses infrared radiation and there is a fear it could cause thermal injury on the back of the eye. Excessive heating could also cause damage to the cornea and the lens, although there is not sufficient evidence on these effects when using retinal scanning sensors. It must be noted that, although these techniques do not currently have a prominent place in the market, some firms are showing interest in developing new systems based on retinal scanning. Thus it




[17] This section is based on contributions by Mario Savastano, Ing. University of Naples, IT. Mr. Savastano is a member of the BIOVISION project, responsible for medical aspects of Biometrics.

would be worth monitoring and analyzing the techniques as soon as these break into the market. Other biometric techniques, like three dimensional (3D) face recognition using laser also require monitoring and analysis.

Iris recognition is a more widely used biometric technology. The concerns related to this technique are the same as those for retinal scanning, namely that the eye might suffer thermal damage from prolonged exposure to infrared (IR) radiation. However, to cause actual damage, the radiation would need much higher doses than is usually required by the imaging sensor. It is well known that by looking directly into the sun for some time the eyes may be damaged. Yet, the energy entering the eye during exposure to an IR sensor is far less than that received just standing in sunlight or looking at an incandescent lamp. The enrolment process for iris recognition can be fairly long, (30 seconds to 2-3 minutes[18]). But even during this time period, the radiation absorbed, according to specifications by vendors, is very low and with no significant implications for the eye. No evidence of medical risks has been reported despite the extensive use of iris-based biometrics.

Biometrics requiring physical contact with readers, such as fingerprint and hand geometry, are sometimes perceived as a source of potential germ transmission. People are reluctant to use such readers because of the fear of contamination. However, it appears that this is more a problem of perception rather than a real health risk. It suffices to think of daily actions which are similar in nature, like touching doorknobs, railings or other common objects and the risk of contamination from those. Hand geometry readers could have more potential for cross-contamination than fingerprint readers, but this does not cause widespread health concerns[19]. General counter-measures for cross-contamination (besides regular cleaning) are irradiation with UV light at regular intervals (claimed to kill 99% of bacteria in 10 seconds) or even the use of nanomaterials that prevent the spread of bacteria. It would be inaccurate to assert that contact biometrics are totally innocuous; sensible measures therefore include avoiding their use in environments where there is risk of cross-contamination such as hospitals for example.

### 2.2.2 Indirect Medical Implications

Indirect Medical Implications refer to fears about secondary use of health data, and lead to important ethical considerations. As regards the potential barriers to biometrics implementation, IMI are, indeed, much more relevant than DMI. The ethical debate becomes extremely heated particularly when people's genetic information is at stake. Even if genetic data acquired in biometric processes are not usable for second purposes, for reasons explained below, the general perception is that individuals' DNA could be captured and, therefore genetic predispositions and conditions could be revealed without their consent.

[18] Image is captured three times using different wavelengths. The best image from the three is kept. Usually LEDs (Light Emitting Diodes) are used. Such LEDs are similar to those used in TV remote controls, toys and other consumer products

[19] Studies have shown that although people wash the palms and fingerprints quite well, they mostly fail to wash between their fingers. With hand geometry techniques users have to put their fingers in between the grooves of the reader, therefore touching it with the least washed parts of their hands

DNA is not currently utilised for real-time identification and so these issues have not yet been fully debated. For current biometric applications, IMI relate to the detection of vascular dysfunctions, the interaction with 'iridology', and the detection of emotional conditions.

The detection of vascular dysfunctions has often been associated with retinal scanning (presently of limited use although of increasing interest). Nevertheless, while it is true that the pattern formed by the blood vessels in the retina may provide information about vascular conditions, the known retinal scanning techniques do not give direct information about the retina. Nevertheless as a precautionary measure, further monitoring and analysis should be done whenever a novel biometric system that scans this tissue is put on the market.

'Iridology', the study of iris texture, claims that systematic changes in the iris pattern reflect the state of health of each of the organs in the body, one's mood or personality, and can even reveal one's future. Iridology is considered questionable by scientists[20], who often compare it to palm-reading, and it is not recognised as a medical practice by any Member State. However, due to its relative popularity in Europe, iridology could increase concerns for iris recognition methods and have an impact on its widespread adoption. As a result a number of additional issues are presented so as to disperse fears over indirect acquisition of data that iridologists claim is possible. The first is that the image taken is black and white, thus eliminating much of the basis for eliciting such information. Secondly, in most cases only the image template is stored (and not the full image), and thirdly when the iris image appears on the screen, it is intentionally blurred.

Face recognition techniques raise fears of revealing the emotional state of a person. However, the data acquired during this process is not at present sufficient to reveal such kind of information. Furthermore, users are requested to exhibit strictly neutral expressions for the face recognition sample acquisition process to perform properly. For some biometric technologies, isolated physiological facts can be determined on a probabilistic base. For instance, one study[21] shows that 50% of people with a given type of fingerprint have a certain type of stomach problem. These examples are limited however.

### 2.2.3 IMI from DNA

IMI derived from DNA are a particular source of public concern, and probably the most controversial case. The context of this controversy is obviously influencing

[20] There are a few changes that can be scientifically observed on the iris texture though. The most evident ones are the blanket of chromatophore cells in the anterior layer of the iris during the first few months of life until this pigmentation develops (typical blue eyes of babies) and some pharmacological treatments for glaucoma are reported to affect melanin, and therefore iris pigmentation. Such possible changes in iris colour are irrelevant for the usual iris recognition methods. Freckles can also develop over time in the iris, but they are invisible in the infrared illumination used. Elderly persons' eyes sometimes show a thin white ring surrounding the iris, an optical opacity that develops with age in the base of the cornea, where it joins the sclera.

[21] See http://www.jhbmc.jhu.edu/Motil/finger.html

the public acceptance of technologies that analyse DNA, since people fear the possible manipulation or misuse of their genetic data. The completion of the human genome sequence announced only three years ago (we are in the so-called post-genomic era) and the decision of some governments to store the DNA of citizens for pharmaceutical research[22], and the extended use for DNA profiling in forensics, are the main factors raising strong privacy concerns. Some characteristics inherent to current DNA biometric practices, however, could reassure the general public about the failure of these techniques to perform genetic profiling of individuals. For instance, only extracts of DNA that are not at present connected to any genetic information are actually stored and used to perform the matching process, while the physical individual's sample is not stored at all.

Sampling and analysis do not use sensors (a physical sample of the user is required) and cannot provide real-time identification (the matching is not performed in this mode). Although for these reasons, many do not even consider DNA techniques to be a biometric technology (Chapter 1), there is a high interest in such technologies, as the general claim is they offer the best biometric performance with respect to FAR and FRR. It is only a matter of time that DNA processing becomes faster and fully automatic. Therefore, public concerns have to be taken seriously if DNA-based biometrics are to be implemented in the future.

### 2.2.4 Medical factors affecting Biometrics

Finally, it is worth pointing out some physiological and medical factors that can affect the usability and efficiency of biometrics. In the case of iris recognition, an obvious factor is that of aniridia (absence of iris, a phenomenon found in a proportion of 1.8 out of 100.000 births[23], which affects both eyes for genetic reasons[24]). Similar effects may be caused by laser iridotomy (used to correct angle-closure caused by glaucoma). Blind people can have problems due to their natural difficulty to align their eyes with the camera. A similar case is that of people with pronounced nystagmus (tremor of the eyes). Wheelchair users can face usability barriers due to the usual location of cameras and insufficient height variation possibilities (handheld or height-adjustable cameras can cope with this problem). People that have been operated on for cataracts may need to be re-enrolled, although empirical evidence suggests that relatively few people need to do so[25]. For fingerprint, conditions such as arthritis may affect usability (it may be difficult to position the finger correctly). Skin conditions such as eczema may cause blistering on the fingertips. With face recognition, any kind of surgery that significantly changes the structure of the face, will require an individual to re-enrol.

[22] Iceland was the first country to assemble genetic data of its citizens (DeCODE Genetics was the private firm in charge). Other European countries followed the experience on parts of the populations, on a voluntary basis. The aim is helping pharmaceutical companies to find genetic risk factors of diseases to facilitate the development of new and efficient drugs.
[23] Source: US National Eye Institute http://www.nei.nih.gov
[24] Source: UK Royal National Institute for the Blind http://www.rnib.org.uk/info/aniridia.htm
[25] "Iris recognition as a biometric method after cataract surgery"
Roizenblatt et al. www.biomedical-engineering-online.com/content/3/1/2

Biometrics usually have higher failure rates with the very young and very old. As people get older, ageing processes tend to degrade biometrics. For instance the ridges of their fingerprints wear down and cataracts are more prevalent. Given the increasing number of elderly people in the EU, costs incurred by re-enrolment or updating passports could be considerable. Moreover, regarding DNA-based biometrics yet another problem relates to the fact that DNA methods today cannot distinguish between monozygotic twins. This is not a limitation to forensic applications neither does it influence the mean error rates but it may rule out certain identification applications such as cash machines.

### 2.2.5 Concluding Remarks

While it is true that DMI exist, they are relatively scarce and irrelevant. Most biometric techniques are innocuous to the human health. The techniques representing a risk, even if it is for a small part of the population or in certain extreme conditions, should be assessed and monitored in a precautionary manner, so as not to promote public concern. IMI are however, more important. To cope with these implications, more effort is needed to convey to the public the fact that such fears are unfounded. This would be a special challenge with regard to DNA techniques. One should remember that scientific reality is not necessarily translated into public reality. Finally, biometrics technologies intended for the whole population, should take into account the biological facts that diminish robustness of the systems. In particular, the aged population is increasing and this could affect the success of the deployment of biometrics, causing extra costs or inefficiency.

## *2.3 Face Recognition*

The face is an obvious choice for a biometric as it is the physiological characteristic used everyday by humans in order to identify others. Face recognition is considered less invasive than other biometrics and generally has a higher level of user acceptance. However it is also more challenging technologically and face recognition has lower accuracy rates than other biometric modalities such as iris or fingerprint recognition. Having been chosen by the ICAO as the primary biometric identifier for travel documents, face recognition is guaranteed a wide level of implementation in the future.

### 2.3.1 What is face recognition?

Face recognition refers to an automated or semi-automated process of matching facial images. The image of the face is captured using a scanner and then analysed in order to obtain a biometric "signature"; different algorithms can be used for this and manufacturers have adopted various proprietary solutions[26]. A step-by-step outline of this procedure is provided in the annex. It is important to note that the term face recognition covers several technologies, including 2D, 3D and infra-red

[26] For further details of different techniques and algorithms, see also http://www.biometrics.org

(IR) facial scans, with 2D face recognition being the most common by far and the one proposed for passports and visas.

### 2.3.2 Technology – state of development

Face recognition is a relatively new technology with the first systems being developed in the late 1990s. The most comprehensive independent evaluation of commercial face recognition systems to date is FRVT[27] 2002, sponsored by six US government bodies. From the couple of dozen companies operating at that time, ten chose to take part in the test; a summary of the key results is presented in the annex and the FRVT full report is available online[28]. The results show that face recognition is clearly not yet a mature technology. Its performance ranks far below iris and fingerprint systems. Though the best performing systems are not significantly affected by normal changes in indoor lighting conditions, face recognition is not yet ready for outdoor use. It is unsuitable for large databases and large watch-lists, and even for moderately-sized lists it has a mediocre performance. Accuracy drops when the acquisition and test occur further apart in time, suggesting faces may need regular re-enrolment. Demographic factors greatly affect performance and this is an important consideration for applications where everyone will be expected to participate.

### 2.3.3 Challenges and limitations

*Seven pillars*

Face recognition does well in the areas of universality (everybody has a face), collectability (2D face recognition uses a photograph, which is easy to acquire) and acceptability (people are accustomed to the idea of using the face for identification and the technique is non-intrusive). It struggles with distinctiveness (the patterns of faces show less variation compared to fingerprints or irises for example), permanence (faces change significantly over time), performance (currently face recognition has much lower accuracy rates than the other featured biometric technologies). Face recognition's resistance to circumvention depends on the application. It is not possible to spoof a face recognition system in the way a latex fingerprint might spoof a fingerprint system, but the low accuracy rates of face recognition make it easier for impostors to be falsely accepted.

*Privacy*

Many privacy implications are common to all biometric modalities but there are a couple of issues specific to face recognition that need to be discussed further: the capability for covert capture and the fear of surveillance. Face recognition differs to other biometric modalities in that the cooperation of the subject is not necessary. An image of the face can be captured covertly with a hidden camera. This may lead to both real and imagined privacy concerns. In 2001, the Tampa Bay Police used face recognition technology to screen the spectators that attended the Super Bowl game against a watch-list of known felons. Part of the outrage that followed,

[27] Face Recognition Vendor Test
[28] http://www.frvt.org/FRVT2002/documents.htm

derived from the fact that spectators were unaware the technology was in use[29]. The result was a negative public perception and a misunderstanding of how the technology was being used; people felt they were being identified even though they were being *anonymously* screened against the watch-list (Bowyer, 2003).

Face recognition also holds the potential to scan many faces at a distance, overtly or covertly, leading to fears of surveillance. Current performance levels of face recognition limit the capabilities of a large-scale surveillance system as the technology would face too many difficulties. Face recognition however will no doubt improve in the coming years. Better performance coupled with advances in computer vision could potentially enable an automated system to identify everybody in a crowd using images captured at long distances. This situation is clearly hypothetical but worth considering if one is to take a prospective view.

### 2.3.4 Applications

The previous section outlined certain attributes of face recognition not shared with the main other biometric technologies. They make face recognition suitable for surveillance, large-scale screening and applications where identification occurs without effort from the subject. On the other hand the relatively low level of accuracy limits such applications at present. The annex describes existing and planned face recognition applications further.

The ICAO recommends the introduction of the face as "the primary biometric" on all machine readable travel documents (MRTD). Though this means a digitalised image of the face must be available on documents, it is not compulsory for all countries to implement face recognition technology. The facial image stored on the travel document can be compared to the individual travelling by a human operator, and it is likely that this will occur until the technology performs well enough to be used at border control.

Several face recognition applications or trials are currently underway, with varying degrees of success. User populations for these applications tend to be limited in size and come from only certain demographic backgrounds. Another (claimed) benefit of face recognition is that it could be used to mine existing databases of photographs. Current technology would struggle however with the quality of photographs available.

The distinctive feature of face recognition that is appealing to law enforcement agencies is the option of matching witness descriptions or artist-rendered images to databases of suspects, i.e. the capacity to compare biometric data with non-biometric data within the same system. Though the results are not precise enough to be admissible as evidence, they could provide the police with leads for further investigation.[30]

[29] For press coverage see http://news.bbc.co.uk/1/hi/sci/tech/1500017.stm ; "Welcome to the snooper bowl," *Time*, Feb 12, 2001; "Electronic surveillance: From 'Big Brother' Fears To Safety Tool," *New York Times*, Dec 6, 2001

[30] http://www.fcw.com/geb/articles/2002/0311/web-face-03-04-02.asp

### 2.3.5 Future trends

It is safe to predict that as face recognition technology matures, performance will improve making viable many prospective applications. Face recognition could be combined with other biometric technologies that operate with no user effort (e.g. voice recognition) in order to create systems that recognise users passively. Further into the future, face recognition is likely to expand beyond the confines of identity and verification tasks. Choudhury[31] suggests that distinguishing facial expressions will become increasingly important for 'smart systems' which can dynamically interact with users.

## *2.4 Fingerprint recognition*

The idea that no two individuals have the same fingerprints and that fingerprints patterns do not change significantly throughout life became accepted during the course of the 19th century. This gave rise to the practice of using fingerprints for the identification of criminals. Though undoubtedly law enforcement remains the best known application of fingerprinting, there are many other everyday applications and in 2004 fingerprint recognition accounted for 50% of the biometrics market.

### 2.4.1 What is fingerprint recognition?

A fingerprint consists of the features and details of a fingertip. There are three major fingerprint features: the arch, loop and whorl. Each finger has at least one major feature. The minor features (or minutiae) consist of the position of ridge ends (ridges are the lines that flow in various patterns across fingerprints) and of ridge bifurcations (the point where ridges split in two). Fingerprint matching done on the basis of the three major features is called pattern matching while the more microscopic approach is called minutiae matching. These are the two main approached to fingerprint recognition (O'Gorman, 1999: 45-46).

### 2.4.2 Technology – state of development

Since fingerprint technology is one of the oldest automated biometric identifiers, supported by strong demand from law enforcement, it has undergone extensive research and development. But fingerprint recognition is still a challenging and important machine pattern recognition problem (Maltoni et al., 2003: 2).

One of these challenges relates to the question of interoperability. Fingerprint recognition normally consists of a closed system that uses the same sensors for enrolment and acquisition, the same algorithms for feature extraction and matching and clear standards for the template and for instance, the enrolment procedure (e.g. FBI standard is nail-to-nail). Take the example of fingerprint sensors. There are

[31] Source: http://vismod.media.mit.edu/tech-reports/TR-516/node10.html

many different vendors on the market that have all proprietary feature extraction algorithms that are strongly protected, although there are some (proprietary) sensor-independent recognition algorithms on the market.[32] Different sensors using the same technology (e.g. solid state) produce different fingerprint raw image data, in the same way as sensors using different technologies (e.g. optical and solid state) deliver raw images that are significantly different. Sensor interoperability is a problem that hitherto has hardly been studied and addressed; it will become increasingly important as fingerprint scanners are embedded in consumer electronics (Ross et al., 2004).

### 2.4.3 Challenges and limitations

*Seven pillars*

Fingerprint recognition has a good balance related to the so-called seven pillars of biometrics. Nearly every human being possesses fingerprints (*universality*) with the exception of hand-related disabilities. Fingerprints are also *distinctive* and the fingerprint details are *permanent*, although they may temporarily change due to cuts and bruises on the skin or external conditions (e.g. wet fingers). Live-scan fingerprint sensors can capture high-quality images (*collectability*). The deployed fingerprint-based biometric systems offer good *performance* and fingerprint sensors have become quite small and affordable. Fingerprints have a stigma of criminality associated with them but that is changing with the increased demand of automatic recognition and authentication in a digitally interconnected society (*acceptability*). By combining the use of multiple fingers, cryptographic techniques and liveness detection, fingerprint systems are becoming quite difficult to *circumvent*. (Maltoni et al., 2003: 11)

When only one finger is used however, universal access and permanent availability may be problematic. Moreover, everyday life conditions can also cause deformations of the fingerprint, for instance as a result of doing manual work. It is estimated that circa five per cent of people would not be able to register and deliver a readable fingerprint. This is significant when implementing large scale applications of millions of people. This will not only lead to serious delays (decrease in task performance) or annoyance (decrease in user satisfaction), but also makes fingerprinting not fully universally accessible (Sasse, 2004: 7).

*Security*

A security issue specific to fingerprint recognition is liveness testing. People leave images of their fingerprint on everything they touch so it is reasonable to assume that an impostor may have access to a copy of a victim's print. It is therefore crucial to prevent systems from accepting artificial fingerprints. Older systems could be spoofed using fake prints made from gelatine. But liveness detection procedures (e.g. 3-dimensional imaging, temperature measuring) are increasingly being integrated in fingerprint readers making fingerprint recognition less vulnerable to

[32] http://www.biometricgroup.com/reports/public/reports/finger-scan_extraction.html

spoofing (Mainguet et al. 2000).[33] Spoofing also becomes harder when multiple fingers are used.

### 2.4.4 Applications

Fingerprint identification of criminals for law enforcement continues to be one of the major applications domains for this technology. The biggest fingerprint central database in Europe is EURODAC, used for asylum requests. In New York, fingerprints are taken to prevent fraudulent enrolment for benefits. Using fingerprint recognition to secure physical access is another popular application. Moreover, fingerprint readers in electronic devices opens up a whole range of new digital applications that are based on online authentication. Finally, decisions have been taken for the future integration of fingerprints (with other biometrics) on travel documents and passports.

### 2.4.5 Future Trends

A fraction of the population faces difficulties in being enrolled and verified through fingerprints and this limiting factor needs to be taken into account for large scale applications. Public perception of fingerprints also needs to be taken into account; there are negative associations due to their use by law enforcement and there is also a fear of contamination from contact readers (cf. Section 2.3 on medical implications).

As fingerprint readers can be cheaper and far more portable than those required for other biometric technologies, it is likely that fingerprint recognition will experience a large diffusion effect, with digital devices.

## *2.5 Iris Recognition*

### 2.5.1 What is Iris Recognition?

The iris is the externally-visible, coloured ring around the pupil. It is a physical feature of a human being that can be measured and thus used for biometric verification or identification. The human iris is well protected as although it is externally visible, it is an internal part of the eye. Iris patterns are both highly complex and unique (the chance of two irises being identical is estimated at 1 in $10^{78}$) (Daugman, 2004) making them very well-suited for biometric identification.

[33] On artifical fingers, see for instance (Sandström, 2004) and "Gummi bears defeat fingerprint sensors",The Register, 16 May 2002;
http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/

### 2.5.2 How does it work

An iris 'scan' is a high-quality photograph of the iris taken under near-infrared (near-IR) illumination.[34] Though visible light can also be used to illuminate the eye, darkly pigmented irises reveal more pattern complexity under near-IR light. Iris recognition systems generally use narrow-angle cameras and ask the user to position their eyes correctly in the camera's field of view. The resulting photograph is analysed using algorithms to locate the iris and extract feature information, in order to create a biometric template or 'IrisCode'.

### 2.5.3 Technology – state of development

The technology is mature enough to be used commercially although all the relevant patents belong to one company (Iridian) which may prove to be a problem for further innovation in the field. However, there is ongoing research (mainly in Asia) on alternative methods and the original patents will expire within the next 5-10 years.

The system works well in identification mode and requires less frequent re-enrolment compared to other technologies, making it ideal for large-scale identification. It may thus be attractive for government applications (electronic identity, border-control). It is also extremely efficient in verification applications (physical access control, time and attendance control) and due to convergence, it may find its way into point-of-sale and wireless and mobile applications once cost effectiveness of the wireless devices has been enhanced.

All iris recognition systems worldwide today deploy algorithms developed by Daugman. Current commercial iris scanning systems are relatively fast, flexible (in terms of operational conditions) and very efficient. They may operate at a range of about 10-20 cm although there exist research systems that operate at the extreme range of 5m. Verification time can be very fast; for example the time needed to search a database of 1 million IrisCodes on a 2.2 GHz PC would be approximately 1.7 seconds.

### 2.5.4 Challenges and limitations

*Seven Pillars*

Iris recognition performs very well against the so-called 7 pillars. All humans (including blind people) possess irises (*universality*) with some exceptions (e.g. people with aniridia, which is the absence of an iris). Iris patterns are scientifically proven to be *distinctive*. The patterns are also *permanent* from infancy to old age with the exception of the effects of some eye diseases. Existing sensors can capture high-quality images (*collectability*) although several trials may be necessary. The iris recognition system offers excellent *performance* even in identification mode with huge databases of enrolled users; however, the necessary infrastructure is still costly. The *acceptability* of iris recognition is relatively low. Finally, while the first

[34] Near-IR wavelengths lie just beyond visible red light on the electromagnetic spectrum.

systems were easy to fool with a picture of an iris placed at the appropriate distance, new systems are more expensive but quite difficult to *circumvent*.

*Privacy*
When considering privacy issues it should be noted that the enrolment process necessarily requires the user to opt-in since it can not be done without consent. The data collected in this way can be used for no other purpose than for identification and authentication of the individual and so we may assume that the technology cannot be used for any other purpose (Big Brother or otherwise). The technology is also ideally suited for use with smart cards due to the relatively small size of the template (512 bytes) which may be easily help on a smart card and manipulated so as to deliver 'on-chip' biometrics. This system would be also sufficiently secure against theft or loss of the smart card since even if someone could access the IrisCode inside the smart card chip the code could be sufficiently changed when re-issued so as to prohibit unauthorized use while allowing the rightful owner continue to use the secure application. Moreover, it is impossible to re-engineer the IrisCode to produce the digital picture of the iris.

### 2.5.5 Applications

Some of the major applications of iris recognition currently are: immigration control/border crossing (using verification, identification or watch-lists), aviation security, controlling access to restricted areas/buildings/homes, database/login access. There is further scope for using this technology in other government programs (entitlements authorisation), automobile entry/ignition, forensic and police applications or any other transaction in which personal identification currently relies on passwords or secrets.

The largest deployment so far is currently in all 17 border entry points (air, land and sea ports) of the United Arab Emirates (UAE). Immigration Control checks all incoming passengers against an enrolled database of about 420000 IrisCodes of persons who were expelled from the UAE (the captured IrisCode of an arriving passenger is matched exhaustively against every IrisCode enrolled in the database). After 3 years of operation and with an average 6500 passengers entering every day - totalling 2,1 million passengers already checked - and some 9500 identified as being on the list and travelling with forged identities, the system is described as very fast and effective (Daugman et al., 2004)

The same system is also being trialled as a 'positive' application in Schiphol airport (NL), Frankfurt airport (DE), several Canadian and 10 UK airports during 2004. Furthermore, on the Pakistan-Afghanistan border, the United Nations High Commission for Refugees (UNHCR) uses such a system for anonymous identification of returning Afghan refugees.

### 2.5.6 Future Trends

Despite the very good accuracy rates achieved, which are necessary for high-security applications, and the lack of a negative connotation (not associated

with criminals and law enforcement as fingerprints are), the high costs of the technology deployment combined with the fear of some kind of lock-in to the technological platform and the user perception of discomfort are putting a brake on the diffusion of iris recognition. Some of the initial patents for iris recognition expire in 2004 and 2005, and it is likely that following this, iris recognition will diffuse more rapidly.

## *2.6 DNA as a Biometric Identifier*

### 2.6.1 How is DNA used as a biometric identifier?

DNA (deoxyribonucleic acid) is the well-known double helix structure present in every human cell. A DNA sample is used to produce either a DNA fingerprint or a DNA profile. For this study and with the current knowledge on the DNA, it is very important to observe the following points[35]:

- only 2-3% of the DNA sequence represents the known genetic material;
- almost 70% of the sequence is composed of non-coding regions, i.e. we do not know the function of these regions;
- almost 30% of the sequence is composed of non-coding repetitive DNA, and only 1/3 is tandemly repetitive, the rest (2/3) is randomly repetitive.

DNA identification is based on techniques using the non-coding tandemly repetitive DNA regions, i.e. the 10% of the total DNA that bears non-sensitive information.

In general DNA identification is not considered by many a biometric recognition technology, mainly because it is not *yet* an automated process (it takes some hours to create a DNA fingerprint). However, because of the accuracy level of the process and because we consider it as a possible future biometric trait we have analysed it further together with the standard biometric technologies.

### 2.6.2 Technology – state of development

DNA testing is a technique with a very high degree of accuracy. The statistical sampling shows a 1-in-6-billion chance of two people having the same profile (Burgess, 2004). Nevertheless, using DNA techniques it is impossible to distinguish between identical twins (the probability of identical twins is approximately 1 in 250 or 0.4%)[36]. According to Bromba (2004), the accuracy of DNA is considered as lower than the one of the iris or retina recognition. Moreover, the possibility of sample contamination and degradation also impacts the accuracy of the method.

### 2.6.3 Challenges and limitations

*Seven pillars*

DNA is present in all human beings (universality) and with the exception of monozygotic twins, it is the most distinct biometric identifier available for human

[35] http://www.college.ucla.edu/webproject/micro7/lecturenotes/finished/Fingerprinting.html
[36] http://www.keepkidshealthy.com/twins/twin_statistics.html (in the US)

beings. DNA does not change throughout a person's life, therefore the permanence of DNA is incontestable. It performs well for the applications where it currently used (forensics, paternity tests, etc.) though it would not be suitable for every application. DNA tests are difficult to circumvent under certain conditions (supervised sample collection with no possibility of data contamination). If sample collection is not supervised however, an impostor could submit anybody's DNA. We all leave DNA traces wherever we go (a single hair can provide a sample) and so it is impossible to keep DNA samples private.

DNA faces several other challenges. Several hours are required in order to obtain a DNA fingerprint. The public is fairly hostile to DNA usage and storage. Further privacy and security concerns are discussed fully below. In conclusion, DNA performs well on the aspects of universality, distinctiveness, permanence, performance and resistance to circumvention, while it is weak on collectability and acceptability.

*Privacy and Security concerns*
DNA collection in the past was regarded as invasive sampling (e.g. finger prick for blood). However, DNA sampling methods have evolved to allow less invasive sampling (e.g. collection with a bucal swab of saliva sample or of epidermal cells with a sticky patch on the forearm). Thus, the new sampling methods are not considered to violate the social expectations for privacy (Quarmby, 2003).

The main problem with DNA is that it includes sensitive information related to genetic and medical aspects of individuals. So any misuse of DNA information can disclose information about: (a) hereditary factors and (b) medical disorders. A DNA profile however is just a list of numbers so it is non-informative and neutral. In addition, in forensics the selection of DNA markers is performed with the aim to be neutral and endeavours to locate DNA markers away from or between genes rather than being part of gene products. Hence, DNA markers are not established in order to be associated with any genetic disease. Race and ethnicity are actually cultural, not biological nor scientific, concepts. Nevertheless, DNA can tell a person what parts of the world some of their ancestors came from[37].

The concern with the DNA sample is that it enables to establish sensitive information related to genetic aspects and this is directly related to security. The two main security problems are the security of DNA system (access rights, use of information only for the overriding purpose), and the implementation of security mechanisms in order to ensure for instance a high level of confidentiality and the security of DNA database (access rights, length of information retention). It seems essential to define the conditions under which the samples can be banked (anonymous/anonymised/coded/identified storage) and to guarantee data protection. So, a quality assurance plan and safety regulations of banking (certification of authorised personal, responsibilities listing, safety measures, etc.) are primordial requirements (Godard et al., 2002).

[37] http://www.adoptiondna.com/what-is-dna.php

### 2.6.4 Applications

Each person has a unique DNA fingerprint and it is the same for every single cell of a person. A DNA fingerprint, unlike a conventional fingerprint cannot be altered by surgery or any other known treatment. Apart from its use in medical applications (e.g. diagnosis of disorders), DNA is widely used for paternity tests, criminal identification and forensics. It is also used in certain cases for personal identification as the following two examples illustrate. In the US, a pack, known as DNA PAK[38] (Personal Archival Kit) is sold with the aim of conserving a sample so that an individual can be identified in the case of kidnapping, accidents or natural disaster. Another US company, 'Test Symptoms@Home' sells several products and services based on DNA. One such product is a personal identification card[39] which exhibits general data, such as name, weight, sex, etc, a fingerprint picture and an extract of DNA profile based on the same loci used by CODIS database. Despite these examples, commercial applications for DNA are very limited; privacy fears and low user acceptance will undoubtedly be a bottleneck for the use of DNA in large-scale applications.

### 2.6.5 Future Trends

Progress in DNA testing will come in two areas: current techniques will improve, offering more automation, precision and faster processing times, and new techniques will be developed (e.g. by exploiting the electronic proprieties of DNA[40]). Today the time required for a DNA test is in the order of 4-5 hours. Recent experiments though, cited in the annex, suggest that it may be possible to cut this time by half. Nowadays it is impossible to distinguish identical twins. In future however it may be possible to do so either through technical improvements in current DNA testing or through a different approach. One such alternative is to study the DNA of the micro-organisms each person carries, such as viruses, bacteria, or other parasites (Crow, 2001).

A joint partnership between a US and a Taiwanese company[41] currently exploits DNA technology for security solutions and provides several products based on plant DNA technology for anti-counterfeit or tracking purposes, such as DNA ink[42] with a real-time authentication (DNA test pen) or DNA marker integrated into textile materials. For this study, an interesting application of the DNA ink would be to use it for the authentication of passports or visas. Though this is not a direct use of DNA to identify a human, it is a potentially interesting application.

DNA from plants is easier to study than DNA from animals and humans and likewise DNA from bacteria is easier to study than DNA from plants. From this we may infer two likely future trends. The first is that other types of DNA may supplant human DNA for individual identification (e.g. identification through analysis of the micro-organisms carried by each individual as mentioned above).

[38] http://www.yellodyno.com/html/dnahome.html
[39] http://www.testsymptomsathome.com/GTI85_productfeatures.asp
[40] http://physicsweb.org/articles/news/8/3/8/1, http://physicsweb.org/articles/world/14/8/8/1
[41] http://www.adnas.com/products.htm, http://www.biowell.com.tw
[42] a scientific view of DNA-based ink is provided in Hashiyada (2004)

The second trend is that that current applications based on plant DNA or on animal DNA are likely to exist in the future for human DNA.

## *2.7 Multimodal Biometric systems*

Biometric systems relying on a single technology are currently deployed, with various levels of success, in many different application contexts (airports, passports, physical and logical access control, etc.). However, by combining more than one modality, enhanced performance reliability and even increased user acceptance could be achieved. Combining less reliable technologies in sequence could strengthen the overall system performance and combining them in parallel could increase the flexibility of the system by providing alternative modes for the verification/identification process.

### 2.7.1 Using multimodality to achieve improved efficiency

Unimodal biometric systems can be subject to many types of errors. Studying the source of such errors will help the design of multimodal systems that can achieve improved performance characteristics.

Some errors may be due to *noise* associated with the acquired data. Noise may be produced in different ways: (a) by sensor performance (e.g. image out of focus); (b) by poor ambient conditions (reflected light during facial image acquisition); or (c) by user behaviour/status (an incorrectly placed finger). As a consequence, the biometric input may be incorrectly matched and the user falsely rejected. By combining appropriate technologies together such noise may be minimised and the end result could be fewer false rejects.

Another type of error relates to *intra-class variability*. Biometric data will naturally vary from one data acquisition to another. This intra-class variability may be stronger for some individuals, especially when monitoring behavioural biometric features - such as signature, voice or gait. This usually results in variation between the data acquired and enrolled data which affects the matching process and may lead to system failure. Again, combining technologies with mixed intra-class variability could result in systems which exhibit overall better performance characteristics.

Other types of errors relate to the distinctiveness of individual biometric features. By combining two less distinct features, an improved overall performance may be achieved (Jain et al., 2004a). Another error effect that multimodal system design can minimise relates to forging and 'liveness' attacks (e.g. fake fingerprint – Matsumoto et al., 2002). In this case, combining biometric technologies in sequence is likely to counter such attacks since a lot more effort will be required to spoof the combined system.

As a result, multimodality could significantly enhance the performance of authentication systems, compared to unimodal systems.

### 2.7.2 Using multimodality to enhance the usability of systems

Two (or more) modalities could be combined in parallel to produce a system that would allow more flexible use. For example biometric systems built for both fingerprint and face recognition, could allow the use of only the facial image for verification when users have problems enrolling their fingerprints and vice-versa. Moreover, this procedure could prove extremely useful to those users who have temporarily lost the ability to provide one of their biometric traits (for example, a temporary eye problem that rules out an iris scan). The same could apply in cases where people refuse to use a specific modality (for religious or health purposes, for instance). A multimodal system therefore allows enhanced flexibility by providing alternatives for the identification process. As such, it also has the potential to be more socially inclusive.

In brief, when designing a multimodal system, the following choices must be addressed:

- *Which modalities are going to be combined*? The choice once again is mainly driven by the application requirements. In addition to the need to enhance performance or usability of the system, other factors such as available resources (including necessary processing power) and costs (of the combined technologies) should also be considered. For example, if a mobile platform with a camera (i.e. a smart phone) is used, voice and face may be the natural combination.
- *At which stage should technologies be combined?* When the modalities are combined in sequence, the fusion of the information provided by the different modalities can be done at different levels (Kittler et al., 1998):
  (a) at the feature level, by combining the features extracted in a single input,
  (b) at the decision level, by combining the decisions of separate biometric systems. The last option may be problematic if the systems disagree. In this case it may lead to further errors (the "bad" performance of a system will degrade the combined multimodal system), or
  (c) at the score level, by combining scores generated by the different systems. Fusion at the score level is more widely used. In this case, the combination considers the scores produced by the system before making a final decision. Overall performance is increased provided that the fusion scheme is adequately chosen (Garcia-Salicetti et al., 2003; Ly Van et al., 2003 and Sanderson et al., 2003). In some cases, the two modalities that are combined may be correlated (for example lip movement and voice recorded together when a person is speaking, minimising the possibility of fraud). In such cases, it is interesting to fuse the information at an even earlier stage, namely just after feature extraction and to build a unique system taking as input a combination of these features (Brown et al., 2002).

Independent of the procedure chosen to design and develop efficient multimodal systems it is essential that further research on such systems is conducted. Several

research projects (see box 1) are evaluating multimodal biometric systems but a major problem is the lack of available multimodal test data.

BOX 1: EC funded research project on multi-modality

Two projects are mentioned both involving mobile handheld platforms which is a new, promising but also complex orientation in the use of multimodal biometrics. Indeed, mobility introduces more noise in captured data, lower quality of data because of cheaper sensors, as well as increased intra-class variability due to changes in capture environments:

a) FP6 IST project SecurePhone[43] "Secure Contracts signed by Mobile Phone" which explores face, voice and signature simultaneously.
b) "Multimodal Face and Speaker Identification" research project (Hazen et al., 2003) which explores multimodal biometrics combining face and voice on a handheld device.

There are few multimodal databases available: M2VTS[44](Pigeon et al., 1997), XM2VTS[45] (Messer et al., 1999), BANCA[46] (Bailly-Bailliére et al., 2003), DAVID (Mason et al.), SMARTKOM[47] ), most of which are the outcome of past European projects. Most of these databases contain few biometric modalities, usually face and voice, and it is only recently that a database (BIOMET) including five biometric traits has been built[48]. Developing multimodal databases is more complicated, time consuming and expensive than developing unimodal ones and as a result such databases contain the data of only a few hundred individuals. This in turn makes it difficult to extrapolate the success or failure of a multimodal algorithm or method which is tested to be used in large-scale deployment (thousands or millions of people). Furthermore, current data protection legislation limits the cross-border sharing of such data.

Finally, there is currently no independent evaluation of multimodal systems available. One of the aims, however, of the BIOSECURE European Network of Excellence[49], is to carry out such an evaluation.

## 2.8 Comparing the selected biometric technologies

All of the technologies presented in the previous sections have a number of benefits and drawbacks which make them better suited for specific applications. Comparing technologies out of context whether on performance or usability or any other criterion is misleading as it does not correctly reflect that biometric identification is only part of a system. There is also very little reliable, comparable and recent data available. However, by having an overview of the likely merits or limitations of

[43] http://www.secure-phone.info/
[44] http://www.tele.ucl.ac.be/PROJECTS/M2VTS/
[45] http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/results/
[46] http://www.ee.surrey.ac.uk/Research/VSSP/banca/
[47] http://www.phonetik.uni-muenchen.de/Bas/BasHomeeng.html
[48] a research project by GET (Groupe des Ecoles des Télécommunications, France)
[49] http://www.biosecure.info/

each technology, one may reach conclusions about which applications are likely to emerge or what kind of multimodal combinations would function better in a specific setting. The best way to achieve this is by comparing modalities against all seven pillars of biometric wisdom rather than on the basis of the accuracy of the final decision stage alone.

It is imperative in this exercise to fully understand the assumptions that govern any such comparison. For instance, the collectability criterion may be interpreted differently depending on whether the whole enrolment process is considered or just the stage of feature acquisition; performance depends on whether we are considering verification, identification or screening. With this in mind, this section presents a comparison of the selected technologies against the seven pillars, focusing on the enrolment process and including cost and market share.

### 2.8.1 Seven Pillar analysis

The "Seven Pillars of Biometric Wisdom" provide a framework with which to evaluate biometric technologies. The information presented in sections 2.3-2.6 is summarised below (table 1). The colour scheme (green for positive, red for negative) allows an immediate impression of the areas of strength and weakness for each technology.

TABLE 4: Selected technologies Comparison against the seven pillars

| Biometric trait \ Pillars | Universality | Distinctiveness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|---|---|---|---|---|---|---|---|
| Face | **H** | **L** | **M** | **H** | **L** | **H** | **H** |
| Fingerprint | **M** | **H** | **H** | **M** | **H** | **M** | **M** |
| Iris | **H** | **H** | **H** | **M** | **H** | **L** | **L** |
| DNA | **H** | **H** | **H** | **L** | **H** | **L** | **L** |

High, Medium, and Low are denoted by H, M, and L, respectively

This table, adapted from (Maltoni et al., 2003), shows overall better results for iris and fingerprint. Face recognition shows a mix of strengths and weaknesses; its strength in universality, collectability and acceptability make it more popular than its performance would suggest. DNA performs well in most areas, but in two areas (collectability and acceptability) it faces serious difficulties which at present prevent its use as a biometric outside forensic investigations. The following two sections draw a more detailed comparison between the four technologies on the enrolment process and performance data.

### 2.8.2 Enrolment comparison

*Universality of biometric trait*

Clearly a person can only enrol if they have the required biometric trait. For the majority of people this will cause no problems, but there will always be people unable to enrol. This could be because they do not have the biometric in question (e.g. no iris, no fingertips, no hand) or because they have the biometric but it is hard to capture (e.g. the ridges of the fingerprint are too fine). The table below summarises the **universality** of the four biometric traits we have studied while more details on factors impeding enrolment can be found in the annex.

TABLE 5: Availability of selected biometric features

| Biometric trait | Universality |
|---|---|
| Iris | High |
| Fingerprint | Medium |
| Face | Very high (enrolment always possible) |
| DNA | Very high (enrolment always possible) |

*Distance of enrolment*

The table below presents the **distance of enrolment,** which may be used to show whether user consent is required. For example, when contact with a sensor is necessary, it is also assumed that the user grants consent. Long distance acquisition could be done with or without user consent, leading to fears of surveillance.

TABLE 6: Distance of enrolment of selected biometric features[50]

| Biometric trait | Distance of enrolment |
|---|---|
| Iris | From 10 cm to 1 m |
| Fingerprint | ~ 0 (user in contact or near contact with sensor) |
| Face | **2D/3D –** A few metres at present, though could potentially be done at longer distances (tens of metres) |
| | **Thermal** – uses IR camera, works also in the dark |
| DNA | Extreme contact; uses body sample (saliva, blood, hair etc.) however, as we leave DNA traces wherever we go, it will be hard to control who has access to this data as DNA testing becomes cheaper and quicker. |

### 2.8.3 Performance comparison

While it is again repeated that such comparisons only have a relative value since performance has to be placed within the context of the purpose of the complete process, it is instructive to have a overview of nominal values for accuracy (and error rate) and throughput rate both resulting in suitability for generic applications.

[50] Source: www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf

*Accuracy*

The qualitative **accuracy level** shown here has been defined by the OECD's Working Group on Security and Privacy and is based on measurements for false match and non-match rates, equal error, failure to enrol, failure to acquire rates[51]

TABLE 7: Laboratory defined selected technologies accuracy level

| Biometric trait | Accuracy level |
|---|---|
| Iris | Very high |
| Fingerprint | High |
| Face | Low |
| DNA | High |

The following table for the **error rate** expresses the accuracy quantitatively.

TABLE 8: Selected technology error rates as reported in large third-party tests

| Biometric | Face | Finger | Iris |
|---|---|---|---|
| FNMR % rejection rates | 4 | 2.5 | 6 |
| FMR1 % verification match error rate | 10 | <0.01 | <0.001 |
| FMR2 % identification error rates for dB size > 1 mil. | 40 | 0.1 | N/A |
| FMR3 % screening match error rate for dB sizes=500 | 12 | <1 | N/A |

Where FNMR is also FRR and FMR is also FAR and N/A is non-available data.

The results are very good for iris recognition, acceptable for fingerprint and poor for face recognition. It should be noted however that the next independent evaluation of face recognition will occur in August/September 2005[52] and it is likely that results will show significant improvement. An accuracy rate of 98% is considered excellent. Data for DNA is not available from independent evaluations of biometric technologies as it is still a lab-based technique.

*Throughput*

A factor which strongly determines the deployment of a technology is throughput, i.e. the time required for the process per person. It is important to note that there is a difference in time due to the existence of both experienced and inexperienced users. Throughput is particularly pertinent for large-scale applications such as border control. Currently, the time required for DNA matching does not allow its use in real-time applications. Table 7 shows the mean, median, and minimum transaction times from an empirical study carried out in 2001 (Mansfield et al., 2001). Time is calculated using the time differences logged between consecutive transactions.

[51] OECD Working Party on Information Security and Privacy - Biometric-based technologies JT00166988, June 2004

[52] http://www.frvt.org

TABLE 9: User transaction times (in seconds)

| Biometric trait | Transaction Time (seconds) | | |
|---|---|---|---|
| | Mean | Median | Minimum |
| Iris | 12 | 10 | 4 |
| Fingerprint optical | 9 | 8 | 2 |
| Fingerprint chip | 19 | 15 | 9 |
| Face | 15 | 14 | 10 |
| DNA | 4 or 5 hours | | |

It is worth noting that this information dates from 2001 and further independent research is needed in order to obtain more up-to-date results.

*Suitability for applications*
Accuracy levels and throughput are important for determining the types of application that each technology can be used for. For large scale identification applications, high levels of accuracy and throughput are required. Consequently, based on current results, face recognition is not yet suitable for identification applications if it is not used as part of a multimodal solution. DNA may be used for identification purposes (though not in real-time). Finally, iris and fingerprint technologies are suitable for both verification and identification applications.

### 2.8.4 Cost and market comparison

*Cost comparison*
The **cost** components of any biometric system include:

- Hardware and associated software to capture the biometric;
- Research and testing of the biometric system;
- Installation, including implementation team salaries;
- Mounting, installation, connection, and user system integration costs;
- User education, often conducted through marketing campaigns;
- Alternatives for users unable to enrol
- Exception processing, or handling users who do not pass the biometric test;
- Productivity losses due to the implementation learning curve;
- System maintenance.

Additionally if there is a centralised database of biometric images/templates

- Back-end processing power to maintain the database;

Though independent data is not available[53] on the relative cost of biometric technologies, it is possible to make a very crude classification, based on several sources. It is estimated that fingerprint and face implementation have a medium

[53] Sources: http://www.bromba.com/faq/biofaqe.htm; OECD 2004 as before; An Overview of Biometrics 19th October 2004 SC3, Scarlet Schwiderski-Grosche www.isg.rhul.ac.uk/msc/teaching/sc3/sec3slides/SC3-2004-3.pdf

cost while iris deployment introduces high costs mainly due to the higher costs for the acquiring sensors. Finally, costs for DNA identification systems are very high mainly due to the need for skilled human intervention.

Figure 4: Comparative Market Share by Technology (2004)

*Market comparison*

Recent comparative market share data reveals which technologies have been implemented most widely thus far. Market share for 2004 show the current dominance of fingerprint recognition but the subsequent table with market share data from 2002-2004, illustrates that the share of other biometrics is increasing at the expense of fingerprint.

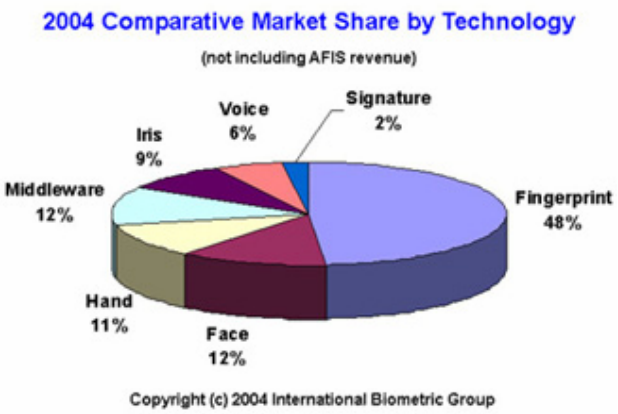



TABLE 10: Comparative data of selected technologies market share (02-04)

| **Biometric trait** | **2002** | **2003** | **2004** |
|---|---|---|---|
| Iris | 5.8 % | 7.3% | 9% |
| Fingerprint | 52.1% | 52% | 48% |
| Face | 12.4% | 11.4% | 12% |
| Others | 29,7% | 29,5% | 31% |

The comparisons made in this section raise two questions. First, why does face recognition have the second largest market share despite performing worse than other leading technologies in most of the areas surveyed? To answer this we must take into account social, economic and practical aspects. Indeed, it is the ICAO's first choice for biometric passports for mainly such reasons[54]. The second question relates to the discrepancy between the strong technical performance of iris recognition and its relatively low market share (9% in 2004). This can be explained by the comparatively high cost of the technology and the existence of patents on the techniques and algorithms which are stifling competition.

Moreover, it is worth noting the strong presence of hand recognition in the biometrics market. Although it has not been fully analysed in this report, the accompanying text box provides a brief overview of this technology.

[54] According to ICAO's Berlin resolution, face recognition benefits include: *facial photographs do not disclose information that the person does not routinely disclose to the general public; the photograph (facial image) is already socially and culturally accepted internationally; the public are already aware of its capture and use for identity verification purpose; it does not require new and costly enrolment procedures to be introduced, etc*.

BOX 2: Hand geometry recognition systems basic Information

Hand geometry recognition relies on measuring the structure of the hand. The acquisition stage takes measurements of almost 100 points on the top of the hand (size of knuckles, length of fingers, etc.) and computes a mathematical formula based on those measurements to create the template. The cooperation of the individual is required at this stage. Users tend to find hand recognition systems simpler to use because the readers are more intuitive. In addition, such systems do not hold negative connotations; thus facilitating user acceptance.

The hand's lower level of distinctiveness compared to other biometrics makes it suitable for verification and medium-scale identification applications. Compared to other biometrics, the accuracy of hand geometry is somewhat lower but it produces a very low false reject rate. The relatively simple and cost effective setup are also major strengths of hand recognition systems as is the fact that it performs well in both internal and external environments and generates less privacy concerns.

The hand is a popular biometric for certain applications; its most widespread use is for physical access control and for time and attendance applications (e.g. S.Francisco Airport employees' access - 30 000 enrolees). It is also utilised for border control, e.g. frequent traveller programme at Tel Aviv's Ben Gurion airport and the US Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) programme used at nine airports.

Recent research has developed new recognition methods aimed at increasing performance. Finally, some projects are studying hand recognition as a promising candidate for web-access.

## *2.9 Other Technological issues*

Biometric identification/verification systems are already used in many applications that require stronger security through stronger identification. For instance, such applications are enabling users to:

a) Control physical access to high-security areas;
b) Protect sensitive data by controlling (physical and/or logical) access to them;
c) Help improve password maintenance, auditing, reporting and record keeping;
d) Provide a high degree of identity certainty (especially in online transactions);
e) Help create and maintain data bases with singular identity;
f) Enhance their privacy protection through the use of biometric encryption.

Their ability to increase trust in identity authentication is their greatest advantage. Law enforcement makes wide use of biometrics and security-controlled environments have benefited from their use as well. In addition biometrics are beginning to be used to enable strong remote access identification, which is regarded as necessary for the development of the Information Society. Their potential diffusion in everyday life applications is another area where expected benefits should be considered. These are regarded as enhancing convenience in a win-win situation for the user and service provider. In the health sector in particular, the possibility to use biometric technologies to protect personal data is a breakthrough application.

The decision whether or not to use biometric technologies in a security solution as well as which one to select from the available technologies, should consider state-of-the-art risk assessment practices, cost/benefit analyses and the potential

effects on issues such as convenience of use and privacy. The best way to acquire experience as to the use of a biometric solution remains a real test case. Manufacturers and integrators of biometric systems have been conducting successful trials mainly in non–European countries (Africa, Asia) and now also in Europe. However, these have been generally uncoordinated and the results achieved have not been widely diffused, nor are they directly reusable. In addition, most of them were not a sufficiently large-scale deployment to be considered as case studies.

While biometric technologies are being used in a variety of applications, there are many questions that need addressing related to their technical and operational efficiency, especially for large-scale deployment. There are still a lot of problems related to the acquisition environment which needs to be controlled in most of the techniques. Hand geometry is the most reliable of the mainstream technologies in terms of the sampling process. In addition it is regarded as a non-invasive technology. However the hand's level of distinctiveness does not make it a suitable choice for border control. Voice is a biometric technology that has potential for the future. There are many strong points in using voice as an identifier; it is after all a natural way to distinguish identity even through telecommunication. However, the effect of ambient noise on accuracy, the fact that voices are not clearly unique, the likely changes over the lifespan of a user and the perceived ease of falsification make this choice less valuable.

Although voice and possibly gait recognition offer the potential to operate without user cooperation or even awareness, face recognition is clearly the choice of biometric technologies for most passive/covert applications. Some of these may offer convenience but perhaps others could threaten privacy. At the moment, face recognition is limited by its performance. As this obstacle is removed however, it will certainly raise questions that need to be answered related to issues of acceptance and legality of surveillance applications, data protection principles, or linking to other information without user consent to draw commercial advantages. In this case and considering society as it is today, for some people the convenience will outweigh the possible fear of surveillance and for others the reverse will be true.

Independent of the technology used, there are general issues to consider. Users and integrators need to be aware of the variability of the threshold chosen for a specific application and how this may be affected by operating conditions. They should also be aware that biometric identification is only a part of the whole security system and therefore could in some cases not increase the overall security at all. But mostly they need to be aware that widespread adoption of biometric technologies (even beyond security applications) is truly dependent on other issues that will be facilitated by the adoption of these technologies that are highly discriminative. The following chapter will put some of these issues in perspective.

# CHAPTER 3: SELT APPROACH

Chapter 3 deals with the Social, Economic, Legal and Technological aspects of biometrics, therefore called SELT approach. The following contributions are authored by external experts. The views expressed do not necessarily reflect those of the European Commission.

## *3.1 Social Aspects of Biometric Technologies*[55]

By Julian Ashbourn[56]

### 3.1.1 Introduction

Out of the many different social issues to be discussed when reflecting upon the implementation of biometrics[57], the following main themes will be touched upon:

- **A)** Clarity of purpose in relation to technology implementations
- **B)** Interoperability and equivalence of performance and process
- **C)** Biometrics as an enabler for other aspirations
- **D)** Human factors, social inclusion and exclusion
- **E)** Impact upon the trust model between citizen and state

It will be argued that there are many factors outside of the technical design or provision of systems which must be considered if current aspirations are to be realised in an ethical, responsible and sustainable manner. In the current rush to introduce biometrics and related technology to a number of processes in the public sector, there is a danger that such matters will not be fully understood or catered for. There is an additional danger that incorrect assumptions are made as to the real value of a biometric identity verification check and what this actually means. Therefore, Europe faces a challenge to understand better the longer-term importance of the implementation of biometrics in order to ensure its benevolent deployment. Such matters need to be taken fully into account.

### 3.1.2 Clarity of purpose in relation to biometrics implementations

One of the concerns often expressed in relation to public sector implementations of strong identity verification technology is that of function creep, i.e. that technology and processes introduced for one purpose will quickly be extended to other purposes which were never discussed or agreed at the time. For example, let us consider the new generation of ICAO recommended travel documents, which will incorporate a chip, and up to three biometrics. What precisely is the purpose of

[55] Authored by Julian Ashbourn, chairman of the IBF International Biometric Foundation and creator of the AVANTI non-profit on-line biometric resource, this section is a brief summary of the report on "Biometrics: social issues and implications", to be found online at www.jrc.es

[56] See also (Ashbourn, 2002a), (Ashbourn, 2002b), ( Ashbourn, 2003).

[57] For additional background information on biometric technology, including relevant links to government and industry, please see the non-profit Avanti web site at www.avanti.1to1.org

introducing these technologies to the ICAO travel document? If it is to verify that the individual presenting the document is the same individual to whom it was originally issued, then let us be clear about that purpose and develop our technology infrastructure accordingly. This would be a distinct purpose that may be easily articulated and that most likely would be accepted by the majority of law-abiding citizens. Similarly, if a biometrically equipped national identity card is primarily for the purpose of verifying that the individual presenting it is indeed the authorised holder, then let us be clear about that purpose. Identity verification via the use of a token, be it a passport, national identity card or a commercially issued token should be contained as a specific function.

In many instances, an important distinction needs to be made between identity verification and entitlement. The entitlement or benefit associated with the transaction in question should not be confused with the identity verification function.

Similarly, the identity verification function should not be extended into areas that are not directly concerned with, or expressly necessary for the transaction. In the case of a travel document being presented at a border crossing point for example, then the identity verification function might be a self-contained transaction, the result of which enables a trained officer to reach a decision about entitlement. Many would be of the opinion that the same transaction should not be extrapolated into areas of general law enforcement or other public and private service areas which have nothing whatsoever to do with the distinct immigration process. This could give rise to general public confusion around such matters and will reflect poorly upon government departments seeking to introduce such technologies. Clarity of purpose should be a key factor in deliberations and, furthermore, clarity of purpose should be properly articulated and communicated in relation to every single programme under consideration. Broad and emotive statements around "fighting terrorism" or "making the world a safer place" are not the most adequate labels with which to introduce these programmes.

### 3.1.3 Interoperability and equivalence of performance and process

This is an area which, even at this relatively late stage in related developments, is seldom understood. Many consider the use of the word 'interoperability' to refer to purely technical matters. The greater interoperability however, lies in the interoperability of process and, where applicable, supporting legislation. This is especially relevant to international situations such as border control and the use of nationally issued documents in other countries. Let us consider for example a biometric identity verification check which returns a negative result. Is this result understood and interpreted in the same way throughout Europe? Or between Europe and the Americas? Or in the Asia Pacific region? If not, what are the consequences of such regional interpretation?

Bearing in mind that a failed verification transaction does not necessarily mean we are dealing with the wrong person – there are many types of potential errors and

many reasons for them. A great deal of confusion could ensue in this respect when usage starts to scale upwards. From a travel perspective, it raises interesting questions with respect to multi-segment journeys which cross several geographic boundaries and where the same individual might be treated quite differently at different points along the way, irrespective of their legitimate entitlement to cross the borders in question. From a social services and entitlement perspective it also raises interesting questions, both within a single member state, or between member states. However, even this scenario assumes a common level of performance (of the biometric identity verification transaction) which will certainly not be the case in practice.

Equivalence of performance across multiple nodes is a factor, which has not been properly understood, nor addressed. How is the biometric technology at individual points of presence calibrated? To what specification? Who has control over this? How is realised performance measured? How is this coordinated between nodes? In this respect, we must also take into consideration non technical factors such as the physical and technical environment, user psychology (Ashbourn, 2002b) and human factors such as age, ethnicity, gender, disabilities and so forth, all of which will be proportionally different at different points of presence. This will lead to possibly significant differences in realised performance across nodes.

This in turn will lead to differences in the user experience and therefore user perception. Habituated users of related systems within the public sector will quickly notice differences in both realised performance and local administration response between points of presence. If the broader situation appears uncoordinated, with little equivalence of process in the way the individual is treated by the local administration, this will itself have a societal impact as citizens begin to question the effectiveness of such systems. There are ways of assuring equivalence of realised performance across nodes, which take environmental and human factors into consideration. However, equivalence of process and response are matters which must be addressed by the agencies concerned.

### 3.1.4 Biometrics as an enabler for other aspirations

Some initiatives which publicly focus upon biometrics and tokens (such as identity cards for example) seem to be less focussed on identity verification in relation to specific transactions than on collecting citizen information for inclusion in various databases, for various reasons. This is currently an area of concern to many, especially where there are aspirations to share this data not only between government agencies, but between countries. Furthermore, the distinction between official and commercial databases and data management is by no means clear, with many suggestions of private sector involvement.

When data is shared between databases and between countries (whether specifically “pushed” or simply made available via the granting of third party access) this calls into question many aspects of data protection and privacy. In such cases, individuals have no control over their personal data, for what purpose it is being used, or who has access to it. The provisions of national data protection acts become meaningless when data crosses national borders. Furthermore, the ability

of the individual to challenge incorrect assumptions with respect to their own data is highly questionable – assuming that they even have knowledge of such a situation.

There may be legitimate reasons for establishing databases of citizen information, but these should be clearly articulated, as should the detail of how such databases will be used and for what specific purpose. We should not confuse this broader data issue with the provision of biometric technology. Furthermore, aspirations to include biometric data in such databases should be considered very carefully, especially with regard to the specific purpose and use of this data. In some instances this may be very clear. For example, if biometric data were included in a passport agency database in order to guard against multiple applications, then the majority of citizens would understand and support such usage, provided they were confident that this same data were not automatically shared with other agencies without their knowledge. If the precise purpose of holding such data is not clear, or considered ethical and responsible, then this may create a negative impression among citizens. Similarly, the blurring of government agency functionality, for example between immigration and law enforcement, may well be considered negatively by citizens. It is therefore important to be very clear about the purpose of introducing a biometric and exactly how this relates to existing and proposed databases, including any proposed sharing of data.

### 3.1.5 Human factors, social inclusion and exclusion

The importance of human factors such as age, ethnicity, gender, disabilities and so raises the possibility of inclusion or exclusion from widespread applications and, crucially, assumptions and processes which might ensue as a result. There are many reasons why, for a given individual, it may be extremely difficult to consistently give a live biometric sample or to otherwise participate in an automated biometric identity verification process. Resulting errors from such difficulties will not necessarily mean that we are dealing with the wrong person or that any attempt at fraud is being pursued. An individual who managed to enrol into a given system may repeatedly fail biometric identity verification checks, or simply fail to interface with the technology involved (such as a kiosk or automated barrier) for a variety of reasons.

Some of these reasons may be immediately obvious, such as physical disabilities for example and, if exception handling processes have been properly conceived, these might be dealt with appropriately. Other disabilities may be less obvious, such as memory retention or learning difficulties, degrees of autism, personality disorders and other psychological affects. There are also physiological issues such as degenerative illnesses, which may gradually reduce an individuals ability to consistently interface with the technology and associated process. The proportion of individuals so affected will no doubt vary according to region and the nature of the system under consideration, but, in some cases may be materially significant, perhaps leading to incorrect assumptions.

In addition, we shall most likely discover a number of individuals whose biometric trait is sufficiently indistinct, or otherwise unusual, to cause problems in enrolment

and, or subsequent identity verification. Fingerprints might be weak or the skin texture not ideally suited to the sensors being used. Facial features may be obscured or skin tone may be causing problems with specific cameras and local lighting or other environmental conditions. Individual eyes may prove difficult to enrol into iris recognition systems. Medical conditions such as arthritis may make it difficult for individuals to use hand geometry devices. Also, there may be behavioural issues which make it difficult for individuals to consistently provide a biometric. Many such conditions may be discovered at the time of enrolment, if our registration processes are properly considered and implemented.

Moreover, we shall have to consider exception handling processes for individuals who have difficulty with automated processes. The proportionality of this factor will become increasingly important as systems scale upwards and large numbers of individuals are enrolled into various systems and schemes. If the failure of an automated biometric identity verification check results in denial of service, then a proportion of individuals are likely to find themselves disenfranchised in this context. The impact of this from a societal perspective will depend upon how well such factors have been considered in advance, together with the nature and practical delivery of associated exception handling processes.

### 3.1.6 Impact upon the trust model between citizen and state

This is a very important point, especially when viewed in the context of modern history (i.e., the last 100 years). In many countries who would consider themselves civilised and perhaps of a democratic nature, the trust between citizen and state plays a key role. Citizens offer their trust to government and, in doing so, empower them to manage national and international affairs on their behalf. If this trust breaks down, a breeding ground is created where a variety of situations might develop, from underground economies to outright challenges to government and civil unrest. In many countries, part of this trust is inherent in the concept of being considered innocent until proved guilty and in enjoying personal privacy and anonymity. These fundamental concepts of trust seem now to be challenged by certain governmental aspirations. There is a risk that the emphasis changes to ordinary citizens being almost treated as criminal suspects and the right to privacy and anonymity being withdrawn.

The issue is exacerbated when the administrations of foreign countries have an undue influence on a given country's procedures. It may be true that, in the short term, citizens simply go with the flow and accept what many of them will see as the sacrifice of personal freedoms in order to support policies which, they have been lead to believe, will create a more secure world. However, in the medium and longer terms, the reality of the situation (such as it may be) may become self evident and, depending upon popular perception, this may lead to an erosion of trust which will not be in the interest of government. This is a very serious issue which should be taken fully into consideration with respect to current aspirations. We should be in no doubt that we are tampering with the very fabric of society and should treat this fabric with the care and respect it deserves.

## 3.2 Economic Aspects of Biometric Technologies[58]

By Jonathan Cave

### 3.2.1 Introduction

Economic transactions require *trust*. The secure provision of identity can help build the needed trust by clarifying the assignment of legal liability and any necessary recourse to the courts. In addition, identifying oneself can signal goodwill. Moreover, personalised data tied to identities provides convenient summaries that may help firms to tailor-make their goods and services or to offer customers the most appropriate choices, improving the efficiency of the market. More generally, identity *indexes* transaction history or other data.

Identity also serves as a *capital* asset (e.g. credit ratings) - formed through investment and subject to depreciation. Ownership of identity capital may be split or diffused (e.g. credit rating agencies with different accounts and amounts of information). This increases the need to attach the data to the person seeking credit.

These functions of identity were known in economics for a long time, but identification was not really an economic issue – face-to-face or closed-system transactions lacked significant misidentification risk and identity fixation in remote transactions or open systems tended to be a legal matter. The value of identity was also approached obliquely – primarily via analysis of reputations. Recent changes in technology and practice call for fresh economic perspectives. Increasingly 'virtual' transactions - where parties may never be able directly to verify each other's identity - have increased the value of identity and made identity theft a more pressing concern. Technical 'solutions' offer identification of differing strengths; their interoperability affects the compartmentalisation of economic identity and its externalities.

The impact of biometrics on economic outcomes will be discussed: optimal and actual identity, the emergence of standards, and costs and benefits. A second section surveys the present state and likely evolution of market demand and supply. Finally, the issues which policy makers need to address as well as the means to address these issues are explored.

[58] Authored by Jonathan Cave, Senior Lecturer at the Department of Economics, University of Warwick, Coventry, UK, and research leader with RAND Europe, Cambridge, UK, this section is a brief summary of the report on "Biometrics: economic issues and implications", to be found online at www.jrc.es

## 3.2.2 Economic aspects

### 3.2.2.1 Optimal identity

In cash transactions parties need not be identified; it is only necessary to verify the right to exchange goods and services for money. However, uncertain or contingent transactions may need more. Buyers may need to prove creditworthiness or certify how purchases will be used, sellers may need to establish provenance or certify quality, origin, etc. via retrospective (e.g. professional qualification) or prospective (e.g. seller warranty) identity. Sometimes it suffices to prove membership of a specified class (adults, physicians); other cases require identification of specific individuals or their legal representatives.

Even if biometrics provides more certain identification it is not necessarily cost-effective or 'optimal' because its additional costs may exceed the benefits of increased certainty of identification. The quality of a particular implementation may be too high for at least one party. Some – regardless of monetary cost – may be too strong for the purpose for which they are employed due to privacy concerns or legal restraints on information collection. Permissible accuracy may be limited – for example, it is essential to establish that voters are eligible and have not already voted, but equally essential not to identify them further. Unless the means and degree of biometric identification are included in negotiations there is no reason to expect the level of identification to be optimal; there may be too much or too little identification or use of secure channels.

Generalised use of one or several large and widely-used "strong identification" systems provides an enormous installed base to cover e.g. security and RTD costs and scope for data mining to detect fraud, thus lowering costs and increasing security. It also limits identity compartmentalisation to control risks. However, even apart from increased data protection concerns, its very strength makes errors harder to correct. 'Hardening' outer boundaries may reduce overall security if internal precautions are relaxed. Identity theft may be less frequent but more severe and identity theft may give way to outright 'denial of identity service' attacks.

Furthermore, to the extent that biometrics provide cheaper, stronger and/or faster identification, they 'tilt the playing field' against those who cannot or will not participate. If the vast majority migrate to a biometric solution, alternative channels may disappear, excluding or imposing costs on the minority. Those with privacy concerns may be unable freely to opt out without losing access to goods, services or societal interactions to which they are entitled – harming those on the 'inside' as well. Due to network effects, any system whose benefits depend on user interactions will be damaged by changes that raise barriers among users.

### 3.2.2.2 The emergence of standards

Biometric implementations have technical and dynamic efficiency effects common to network technologies. Identity is *complementary* to economic transactions, so equilibria may be unstable or non-existent. Economies of scale and interoperability favour winner-takes-all ("tipping") equilibria. This works by three channels:

- Market adoption depends on *expectations* – a technology expected to become a standard is likely to do so.
- Competitive forces are likely to produce a single (or unified) standard approach, especially with greater interconnection among sectors and participants, so early leads are difficult to overcome.
- "Sunk costs" of adopting standards can strand those making the 'wrong' choice with obsolete investments and reduced benefits. This risk makes firms wait to adopt, particularly where value depends on availability of interoperating and complementary database, communication, sensing, payment, etc. systems. This in turn inhibits investment in developing such complements, and partially accounts for private sector reluctance to adopt biometrics despite falling direct costs.

This tendency to "tipping" is reinforced by pressures for compromise solutions. If interoperability were irrelevant, it would be possible to match each application to that biometric offering the best combination of costs, accuracy, etc. But even closed identity management systems need to interoperate[59] and multiple identity systems impose substantial burdens. Even when 'optimal' biometric solutions differ by application area, there are strong pressures to adopt imperfect compromise solutions.

Another mechanism which might damage competition could be strategic use of intellectual property rights (IPR). A firm holding key patents need fear no competition; if it chooses to allow competitors to license its technology, it can do even better, encouraging entry of efficient rivals and extracting further rents from their innovations. Ultimately, such strategies are self-defeating; they encourage bypass competition and antitrust action, keep prices high and limit market growth and prevent the 'medicine of competition' from driving costs further down. But, as recent iris scan algorithm patenting disputes show, such self-defeating tactics still persist[60]. Further ramifications include patent 'thickets' and 'clusters' to deter innovative rivals.

There are two alternatives to the emergence of *de facto* (proprietary) standards as a result of "tipping", IPR or accident: voluntary industry agreements (typically open); and mandated national or international standards. Open standards are more likely to solve the coordination problem and enhance competition by lowering entry barriers and stimulating innovation of complementary products. However, they may take longer to achieve and can mask collusion. Mandated standards can be established quickly – perhaps too quickly if they are based on uncertain assessments (e.g. ISDN) or forestall price and quality competition. Regulators may be captured by better-informed industry players, amplifying the anticompetitive effect of proprietary standards.

[59] With other biometrics in combined systems and with data, payment, CRM, etc. in integrated applications.

[60] The main patent is due to expire shortly. The patent holder guarded its rights jealously, launching attacks against actual or potential rivals even in the waning days of the patent.

#### 3.2.2.3 Costs and benefits

Decisions about biometrics rest on estimates of costs and benefits, relative to alternative means of identification, which offer both advantages (ease of issue or revocation, no problem of template aging, low entry barriers) and disadvantages (vulnerability, 'hidden cost' of lost or multiple passwords). Early adopters have high direct costs, but enjoy increased chances of 'winning' the standardisation race, incentives for further development and IPR and 'learning curve' reduction of future costs, including indirect costs[61].

On the benefit side, available data tend to fall into three categories:

1. Costs of problems biometrics should solve.
   Annual UK costs for identity theft[62] are estimated at €1.95 Billion (10% of all fraud, and growing). In the US, where it quadruples annually, identity theft affected 28 million citizens and cost €55.5 Billion in 2003. However, the degree to which biometrics reduces theft and the possible displacement of fraud remain uncertain.
2. Cost savings from immediate deployment.
   Such data are often proprietary or commercial. They should be presented as lifetime cost of ownership and adjusted for changes in financial, physical, IT and human capital and impacts on internal processes.
3. Estimates of willingness-to-pay
   These estimates provide a lower bound on consumer surplus from biometrics. Better functionality is accompanied by falling costs: the two effects offset in terms of price but should be added to estimate welfare gains. Biometrics also let risk-averse consumers save on costly hedging or insurance or make use of more secure or competitive channels.

### 3.2.3 The biometrics market

#### 3.2.3.1 Demand

In the recent past, three applications have constituted the bulk of the biometrics demand. Firstly, physical access control has been the dominant application since the advent of biometrics, but is rapidly being supplanted by IT applications. It had 42% of the biometrics market in 2000, was dwindling but revived strongly since 9/11. Here the dominant trend is expansion to monitor time, attendance or physical location. IT applications had the second-largest share of the market (25% in 2000), growing with biometrics' inclusion in laptops, the development of specific interface standards and biometric implementations in converged computing/communications equipment. The third largest area for biometrics was financial services (15% in 2000), which is likely to grow due to changes in fraud types, financial identity management and banking itself.

[61] For instance, automated identity management can produce personnel savings – or raise the cost-effectiveness of skilled personnel. Conversely, there may be increased demand for skilled staff to enroll participants or decreased capability to perform other tasks at point of verification.
[62] For US data, see e.g. http://www.consumer.gov/idtheft/stats.html. For the Cabinet Office report (2002), see http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf.

However, the demand for biometrics is rapidly shifting, due to new implementations. Government and other public sector applications will be leading the sector in volume, new technology adoption, project scale and prominence. After 11 September 2001 transport and immigration (biometric passports) have become key issues, with an emphasis on international interoperability. The public sector is also a leading client in health, where biometrics is increasingly used to prove entitlement and link patients to electronic health records.

Other sectors likely to emerge as significant parts of the market are retail and other payments (already being trailed in wide range of applications), telecommunications services (integrated with other services and linked to individual data), and transport (including private transport).

#### 3.2.3.2 Supply

The biometrics sector follows the 'experience curve:' a few leading firms, many subsequent entrants and consolidation to a few survivors. The shakeout is well underway; despite strong demand growth, mergers and bankruptcies dominate recent market reports. The cycle is more advanced in fingerprint, while newer technologies (iris) still have many small firms pursuing diverse approaches (albeit with tight control of key patents). Concentration is high even during expansion, leading to persistence of dominant firms with specific national and/or sectoral attachments and possible distortion of biometric development.

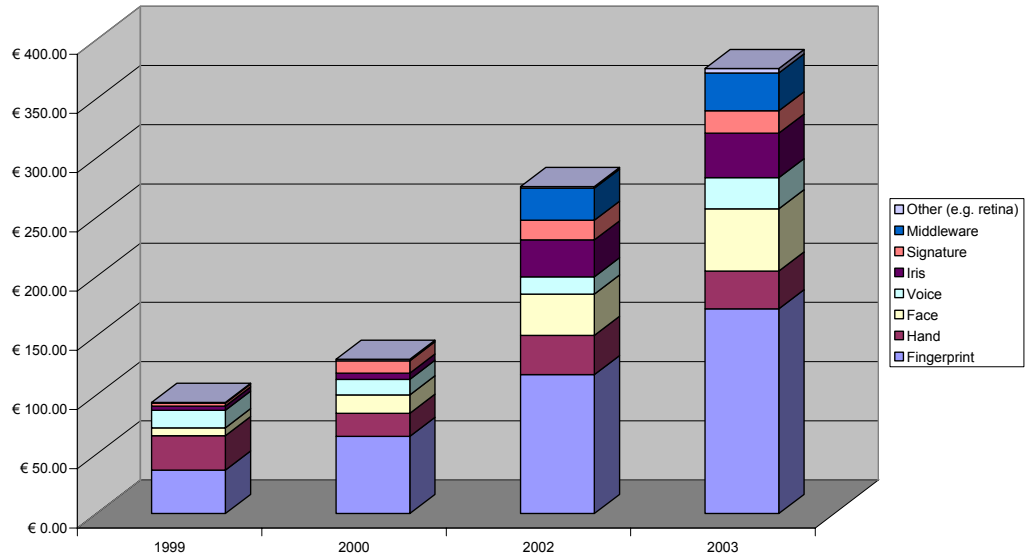
The tendency to concentration is reinforced by specific factors. Firstly, as eventual uses of the technologies are unclear, fixed testing costs are fairly high, which raises entry barriers. Secondly, early public or private customers seek 'assurance,' which favours incumbents and firms with a large installed base. The key role currently played by very large public procurements can generate an enormous installed user base, which encourages subsequent clients and suppliers of complements to standardise on the incumbent firm/approach. Thirdly, the threat to competition is enhanced by the 'layered' structure – hardware, middleware, application, all of which must work with each other. Market power in one layer can extend to others.

#### 3.2.3.3 State of the market

The industry began and is thriving in the US, but Europe's share is growing rapidly, particularly in banking. Recent European government initiatives will boost demand even more. Available data suggest consistent dominance by fingerprint, with hand geometry and voice recognition dwindling and iris growing.

Supporting these data are overall growth and the growing non-US market (where hand recognition is rarely used). Strong revenue growth in fingerprint is likely to continue as cheaper scanners are bundled with computers but other biometrics such as facial recognition and iris are also showing strong growth (See Figure 5).

FIGURE 5: Revenues by Biometric Technology




Over time, hardware will become cheaper, interoperable and commoditised. Algorithms will remain proprietary and distinctive and continue to improve, so IPR will remain profitable. Middleware, which mediates functionality and interoperability, is likely to be convergent, less profitable and ultimately provided by open-source and/or compatible free software.

Application service providers will dominate the growth phase – initially providing solutions but ultimately supporting users and 'intermediary' layers, possibly before acquisition by integrators. Value-added resellers and original equipment manufacturers provide important transitional competition, but the market is likely ultimately to belong to specialised security or diversified ICT integrators. Relationships are likely to be strategic and/or collusive partnerships. Ultimately, biometrics may be wholly subsumed by technology (e.g. PCs), integrated ICT and/or security markets.

## 3.2.4 Policy

Six major issues which might require action by policy makers emerge from the above analysis. In a second step, we will present the levers which policy makers have at their disposal to address these issues.

### 3.2.4.1 Issues

The first is possible *market failure* – competition may be undermined by 'tipping' or capture – of a single market layer or a set of connected segments. This applies to biometrics *per se* and broader IT, transportation, health informatics, etc. market segments, in many of which strong network, interoperability and complementarity

effects can lead to some dominance. The consequences are those usual to competitive failure; allocational inefficiency, retarded or distorted RTD and associated spill-over effects on employment, competitiveness, etc.

A second, somewhat narrower concern is the *development and competitiveness* of biometrics and the 'identity industry'. Biometrics shares many characteristics with other high-tech industries (risk, possible slow take-up, limited capital access, threatened obsolescence, high-tech skill dependence, critical importance to other rapidly-growing sectors), but stands out because of its importance to security, eGovernment and other public objectives.

The third concern is the tension between *standards* 'lock-in' (Arthur, 1983; David 1985) and diversity. Market competition on its own may fail to produce timely and appropriate levels of standardisation or may get 'stuck' in an inferior standard.

Fourthly, *intellectual property rights* (IPR) are obviously important to the competitive health of the market, but pose particular problems relating to interoperability and network effects. Compatibility requirements may reward IPR holders with market power even without beneficial innovation – especially when customers value stability, 'assurance' and compatibility above other characteristics. The first product to be adopted may well become the *de facto* industry standard. On the other hand, IPR may encourage beneficial 'bypass' innovation.

A fifth point is that biometrics is a key element of government *security* policy. Yet governments have poor records in managing large IT procurements, and political sensitivities combined with rapid technology development and the importance of international interoperability make value for money even harder to ensure. For instance, it is not obvious who (if anyone) 'owns' liability for flaws in a technology or its implementation. On the basis of empirical evidence, open-source systems seem to be at least as secure as proprietary systems and sometimes much more secure[63].

Finally, the use of one's identity itself is changing from a 'private good' belonging to the individual and useful in a limited range of close interactions to a form of social capital used in a vast range of poorly-observed and uncontrolled interactions and based on data scattered throughout many networks. Difficulties in preventing access to one's identity and its possible abuse in ways that are not immediately obvious makes 'identity' a *public good* – not least because protection of individual rights and freedoms may require public provision of strong identity.

#### 3.2.4.2 Policy levers

These issues can be addressed by several policy levers. The first is *procurement policy*. Large government contracts are often the first major demand component, underwrite private financing and create industry leaders in a short space of time. Thus they drive new technologies. The advent of mass-market biometrics coincides with security, eGovernment and eParticipation initiatives. However, the public

[63] Compulsory licensing provides a limited 'third way' but is costly and legally complex to operate.

sector's 'launching customer' role is extremely difficult; it requires appropriate specification, smart contracting and active partnerships with suppliers in the face of untested technology. Because biometrics is intimately connected with sensitive policy areas it may challenge the two pillars of European public procurement: equal treatment and transparency. Tools include 'pre-competitive engagement' multiple-sourcing, design competitions, IPR options in contracts, open standards requirements and insistence on open and transparent supply chain management. Interoperability generally makes it impossible to divide procurement among many firms in advance of open standards, but procurement can be structured to leave even 'losers' with valuable IPR and to provide opportunities for integrators, licensees, etc. to participate in future development.

A second policy lever is *standardisation policy* – there is a potential role for mandated open standards with protection for 'equivalent' alternatives or for incorporation of open standards requirements in procurement, licensing and other policy decisions.

As a third lever, *competition policy* must take account of both tipping tendencies and the need for innovation. In general, incompatibility makes product innovation 'too fast.' Another danger is *foreclosure* e.g. when an integrated provider deliberately makes its equipment incompatible with rival offerings or when the holder of a key patent effectively controls all those who use it. Competition policy can act via merger and access pricing regulation. The treatment of industry standards consortia is also important; they might manipulate standards, exchange cost information or refuse to licence to 'outsiders'.

The fourth policy domain is *intellectual property rights* (*IPR)*. There is obvious scope to use mutual recognition and compulsory licensing to control adverse effects or private IPR. A more radical alternative would be a public goods route (e.g. General Public Licence) supporting an open source RTD policy, where access to research results is open, usage rights are granted freely and even derivative innovations may be bound to the public domain. Economic returns may be sought in selling related goods and services or in selling enhanced versions.

TABLE 11: Summary of the interaction between issues and levers.

| | | Policy domains | | | |
|---|---|---|---|---|---|
| | | Procurement | Standards | Competition | IPR |
| Issues | Market failure, sector health | ✓ | | ✓ | ✓ |
| | Standards | ✓ | ✓ | | ✓ |
| | IPR | ✓ | ✓ | ✓ | ✓ |
| | Security | ✓ | | | |
| | Public identity | ✓ | | | |

## *3.3 Legal Aspects of Biometric Technologies*[64]

By Paul de Hert

### 3.3.1 Europe is ready for biometrics

With computer systems recognising fingerprints or voice, we have gained a powerful tool to verify the identity of an individual and thus ensure essential levels of security. The technique to use human characteristics in identification processes is often referred to as biometric recognition. Biometric technology is no longer an embryonic development, but has become the core of national and international security and immigration policies and is gaining importance as a product for the private sphere.

With the exception of DNA analysis, blood and breath sampling regulated in Traffic bills and (to a lesser degree) fingerprint sampling there is relatively little legislation in Europe with regard to biometrics. Biometrics use in private transactions is based on consent. Governmental use of biometrics is only starting and when biometric enrolment becomes obligatory, for instance in the context of identification schemes such as electronic passports and identity cards, new legislation will be needed.

Analysis of the current human rights framework and the data protection framework shows a flexible legal environment that allows for much discretion for public and private actors implementing biometric schemes. Biometrics deployment does not threaten procedural rights, such as the presumption of innocence, stated in Article 6 subsection 2 of the European Convention on Human Rights. Also, the sampling of biometrical data respects the right not to incriminate oneself as defined in the European case law. According to the European Court of Human Rights the right not to incriminate oneself, that is regarded as an aspect of the general right to a fair trial enshrined in Article 6 subsection 1, means that a suspect cannot be forced to supply evidence for his conviction and consequently the prosecuting authority has to collect evidence without exploiting evidence obtained by force or pressure. Taking bodily samples, even against the will of a suspect, is not considered a limitation of this right.

Also important is privacy, a fundamental right included in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Interference by the executive power on the rights and freedoms of the individual should not be permitted unless there is a clear legal basis to do so. The requisite in Article 8.2 of the Convention that a law restricting privacy must be ‘necessary in a democratic society’ brings us to the difficult relationship between individual rights

[64] Authored by Paul de Hert, Professor at the faculty of Law, University of Leiden, this section is a brief summary of the report on "Biometrics: legal issues and implications", to be found online at www.jrc.es

and collective interests. Because with most biometric technologies no penetration of the body's surface is required, it is assumed that the use of these technologies will not be deemed unreasonably intrusive when properly motivated (and based on a legal regulation) or based on consent. Therefore every application – such as the choices of the EU legislator for two biometrics in the passport and Visa system – must provide a satisfactory balance on four criteria: reliability, proportionality, the presence of a fallback option and prior knowledge or consent. Even if arguments against current EU legislative can be found, when these four criteria are met, decisions will for instance, suffice the European Convention on Human Rights.

The text of the Constitution of the European Union and previously, the European Union's Chapter of Fundamental Rights, include next to privacy protection the rights to data protection and human dignity, which are not covered in the European Convention. Although the data protection framework has some important consequences for the way biometrics are implemented, fundamental choices such as the choice for centralised biometrical databases, are seemingly left untouched by it. Data protection lacks 'normative' content. It is in the first place designed to 'channel' the application of new technologies. However, certain 'technical' problems with the data protection framework are identified, such as the question whether templates are considered to be personal data, the question on whether biometrical data is sensitive data and in general problems with the application of Article 15 of the Directive 95/46 on Privacy Protection[65], already in force.

### 3.3.2 Fundamental concerns about human rights and power remain

The deployment of biometrics by public and private actors raises numerous concerns that are not or not adequately addressed by the current human rights framework and the data protection framework; for instance concerns of power accumulation, concerns about further use of existing data, concerns on specific threats proper to biometrics, concerns related to the use of the technology in the private sector, concerns about the failure to protect individuals from their inclination to trade their own privacy and concerns for costs.[66]

These concerns are genuine. Policymakers and civil society demand decisions that are well informed and based on careful consideration of reality. However, there are no empirical data about the current performance of the existing systems as there are no precise data about why new systems and facilities are needed.

[65] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[66] Biometrics seemingly often come for free. Private actors demand biometric samples in exchange for certain advantages and certain governments, such as the U.S., are investing huge amounts of money in identification schemes *and* in financial instruments to accelerate the use of security devices in U.S. society (tax write-of formula, grants, demonstrations of biometric security options for schools). Legal concerns emerge when biometrics come for free. Human rights and data protection law requires the processor and controller to be the first arbiter of the necessity to process biometrical data. How can this demand be properly met in a non-critical environment?

The concerns are also genuine because European policymakers and civil society know that the longer a technology is used, the more entrenched in life it becomes. They feel that the current (legal) system gives too much leeway to new technological developments that are conceived without proper regard to a human rights perspective. They also feel the American pressure and know about America's mass installation of surveillance technologies (metal detectors, scanners, CCTVs, iris recognition systems, alarms, locks, intercoms, and other forms of surveillance, detection, access control and biometric equipment) in schools, government premises, stores, offices, workplaces, recreation areas, streets and homes; and other public places, without understanding all the purposes behind this security build-up. Common sense pushed people to adopt a critical attitude (that regrettably is hardly echoed in the current legal framework), refusing to accept simple answers about safety and protection when there is little evidence that security technology actually makes us safer. They have heard about the paradox of technology.[67] They realise that law enforcement often use new technological security tools on poor and non-white people, and fear social outrage about discriminating practices.

Adding up the specific threats created by the use of biometrics with the common privacy threats, explains why when allowing biometric images to be processed, one gives up complete control over information that maps distinctively onto one's physical person. Should in addition, someone's biometric data become available on public networks (e.g. unauthorised release) or distributed or exchanged commercially (e.g. misuse) further risks emerge, to the point where it is difficult to imagine any proportionate gains in security or comfort.

This ethical assessment leaves no room for the view that: "data protection will do for biometrics". Next to privacy and data protection, the right to have human dignity protected should be taken into consideration. Applying data protection principles implies the presumption that biometrics can be processed or that biometric data can be made available to others (even commercially). Already today, some American firms present their customers the option to make a commodity of their fingerprints in exchange for the faster acquisition of cheeseburgers. The choice is portrayed as a casual decision with little or no moral impact, and customers are not encouraged to consciously consider its repercussions. It is easy to imagine people providing biometric samples under time pressure, without precaution. The example of the European dancing club which uses biometrics for access control, demonstrates that monetary or other rewards can have a similar effect in making biometric enrolment look trivial.

The answers to such concerns must be formulated with reference to the basic features of the democratic constitutional state. From this perspective, opacity/privacy (prohibiting) rules should guarantee those aspects of an individual's life that embody the conditions for his/her autonomy (or self-determination, or freedom, or "personal sovereignty"). Privacy and human dignity must preserve the roots of the individual's autonomy against outside steering or against disproportionate power balances in vertical, but also in horizontal power relations.

[67] Technology that is said to do good also produces unintended negative consequences and does not live to the promises of those that develop and sell it.

This is so since such interference and unbalanced power relations are not only threatening individual freedom, they are also threatening the very nature of our society.

The fundamental task should be first to consider whether biometrics *should be allowed* and *when*. Developing concepts such as 'biometrical anonymity' or 'a right to property on biometrical data' might be instrumental to achieve this objective. Defining specific biometric prohibitions may be another, more familiar approach. Some possible options are incriminations for theft and unauthorised use of biometric data, and prohibitions. For instance by forbidding the non-encrypted processing and transfer of biometric data or by prohibiting the use of biometrics that generate sensitive data when alternatives exist or the use of financial rewards to promote participation in biometric identification programs, or on 'centrally' storing easy to misuse full "raw images".

Once legitimate use is identified by the legislator (the first task), enhancing available transparency tools need be considered (the second task). It is only after having identified legitimate forms of biometrical processing, that one should define the rules and conditions which any *allowed* use of biometrics should respect.[68] With regard to this second task, there is a need to establish both common principles and language of privacy for biometrics, including principles such as: equality of access to the network; absolute accuracy of targeting by surveillance systems; systems to ensure the accuracy of the data held within the surveillance systems; mechanisms for amending the false, inaccurate or modified data; systems to protect individuals from their inclination to trade their own privacy. This biometrics framework should be established based on appropriate risk assessment which distinguishes between legitimate and illegitimate use of biometrics.

### 3.3.3 Procedures based on biometric evidence shall be unfavourably received

Biometric evidence is likely to be accepted without too much resistance in European Courts. Notwithstanding some differences, all systems in Europe tend to include most forms of evidence. Also, although the principle is elaborated in a different way, the rules governing evidence in all European countries have a tendency to ban only categorically unreliable or illegal (illegally obtained) evidence. In countries belonging to the different traditions some form of corroboration is required as a limit on the freedom of the judge. In the Netherlands, for instance, one confession is not sufficient (art. 341 Code of Criminal Procedure) for a conviction. This evidence has to be corroborated by other evidence.

However, some authors assess critically the impact of DNA-analysis on legal systems that employ the rule of free assessment of evidence. We saw earlier that within such systems all means of evidence are equal; the judge can thus choose

[68] "Assessment of the principle of proportionality in these questions of visas and free movement of persons, therefore, begs the question of the fundamental legitimacy of collecting these data and does not only concern the processing procedures (modes of access, storage period etc.)" (Article 29 Working Party, Opinion No 7/2004 - 11224/04/EN WP 96, adopted on 11 August 2004.

freely what kind of evidence is relevant to help assess the possible guilt of the defendant. Since DNA-analysis offers stronger security and more reliability than older evidential techniques, which may be flawed by subjective elements, there is the danger that judges within such systems of freedom of evidence will be tempted to attach increased role to DNA-evidence (obviously when properly obtained and processed by certified institutions). This might be detrimental to the system of free evaluation of proof based on a possible intimate conviction of the judge.

This warning can, be generalised to all biometric technologies and to all systems of evidence in Europe. Whenever investigations become complex and the methods of investigation become formalised, the outcome will be harder to evaluate by the court *and* the defence. To prevent experts taking over the position of the judges, the legal recognition of an automatic right to counter-expertise is needed and, like in civil cases all over Europe, parties should have the right to meet the expert and be heard.

## *3.4 Technical Aspects of Biometric Technologies*[69]

By Bernadette Dorizzi

For a long time, the use of biometrics was limited to forensic applications. Recently, however, it has become possible to digitize, store and retrieve biometric patterns and have them processed by computers. Large scale deployment can thus be envisaged in, for example, passports, voter ID cards, national ID cards, and driving licenses, which will reduce waiting time at border controls, or for welfare disbursement. Biometrics provides a challenging solution to increased security needs, as it bases authentication on aspects that are specific to each individual. However, biometrics is only one element of a larger system that involves: the use of sensors to acquire a biometric sample; the transmission of this data from the sensor to a computer; the access to a database of stored templates in order to find a match; and the decision and subsequent action. Biometrics should not be considered alone but as part of global system that must be designed and evaluated in its entirety (Dorizzi et al., 2004).

### 3.4.1 Different well-known modalities

Different modalities can be considered; fingerprints, iris scans are currently the most reliable methods, but users often consider them intrusive. Users are more familiar with methods using face, voice or handwritten signatures, but these are not yet sufficiently efficient for use on a large scale. In view of this, combining several methods would seem more appropriate, but this has still to be validated. Moreover, there will always be a compromise between the level of accuracy you can obtain through a given modality, (as biometric systems will always produce a certain level of error) and the level of constraints you can impose on the user, especially during the enrolment phase. Indeed the more constraining the acquisition of the patterns, the more accurate the results of the biometric system. Of course it is the application's purpose that mostly impacts user acceptability; requirements to ensure safe air travel need not be the same as those used to access an office or a home.

#### 3.4.1.1 Iris

Of all existing biometric techniques, the one encoding the iris patterns (Daugman, 1995) is the most precise one, possibly at the expense of a rather constraining sample acquisition process (the camera must be infra-red, the eyes must be at a very precise distance and angle from the camera). These elements provide a very good quality initial image, which is necessary to ensure such a high level of performance.

[69] Authored by Bernadette Dorizzi, Professor at Institut National des Telecommunications (INT), FR, this section is a brief summary of the report on "Biometrics: technological issues and implications", to be found online at www.jrc.es

On the other hand, they may make enrolment time consuming and call for user training (Jain et al., 2004). This method is also relatively expensive and unavoidably involves the scanning of the eye, which can initially prove off putting to users. Its reliability, however, means it can be successfully used both for identification and authentication (verification), an advantage which few other techniques can offer.

#### 3.4.1.2 Fingerprinting

Fingerprinting, is currently the method which offers the best compromise between price, acceptability and accuracy (Maltoni et al., 2003) and a lot of systems based on this modality are already operational. However, the latest evaluation results[70] show that their performance relies heavily on the quality of the acquired images, particularly during the enrolment phase. Moreover, it seems that a few percentages of the population cannot be enrolled through fingerprinting (manual workers, people with too wet or too dry hands etc.), though this can be reduced with the use of prints from two or more fingers, and adequate specific enrolment processes for people who have problems. While the existence of a great number of different sensors associated with various technologies is in general beneficial to performance due to the coupling of sensor and algorithms which is optimized by the designer of the biometric system, it also induces interoperability problems. Fingerprinting is, in general, fairly well accepted, even if it has some forensic connotations and it allows both identification and verification.

#### 3.4.1.3 Face recognition

Currently face recognition is considered to be relatively inaccurate due to the presence of a lot of variability (from 1.39% to more than 13% EER[71]). This is due to changes that occur to people over time, like ageing, or simply related to external environmental conditions (poses, facial expressions, illumination, textured background). Therefore this method's performance varies considerably, depending on the recording conditions and the context of application (static images or video, with or without a uniform background, or constant lighting conditions).

Face recognition is not efficient enough at this moment to deal with Large Scale Identification but it can be useful in the context of verification or limited access control with constraining acquisition conditions (during enrolment the background must be uniform and the user must face the camera at a fixed distance. As regards sample acquisition using a video camera, no system can be considered as sufficiently developed[72] (Phillips et al., 2000) but there are promising technological innovations that use 3-D modelling to cope with the problem of pose (Xu et al., 2004 and Chang et al., 2003). This obviously means an increase of the cost of the global system (use of sophisticated 3-D scanners in place of standard medium-cost cameras). However, due to the fact that this modality is well accepted by the user, and that it has been introduced as a standard in travel documents by the ICAO, a lot

[70] FINGERPRINT VENDOR TECHNOLOGY EVALUATION, 2003 http://fpvte.nist.gov/
[71] EER is Equal Error Rate when False Accept and False Reject rates are equal FAR=FRR
[72] FERET Database. NIST 2001 http://www.itl.nist.gov/iad/humanid/feret/

of research is being conducted to improve the systems' accuracy. A big increase in performance can be expected in the next 5 years but this modality can never be expected to be as accurate as fingerprinting or iris scanning due to its intrinsic variability and behavioural character. Nevertheless for convenience, applications (like physical access control or personalisation of environment) which impose limited FAR (False Acceptance Rate) constraints, the use of face recognition is still very interesting as it can be transparent. It would, however, have to be used in association with other methods, in order to reduce error rates or be used against a pre-selected database (trained to use).

#### 3.4.1.4 DNA

Except for identical twins, each person's DNA is unique. It can thus be considered a 'perfect' modality for identity verification. DNA identification techniques look at specific areas within the long human DNA sequence, which are known to vary widely between people. The accuracy of this technique is thus very high, and allows both identification and verification. Enrolment can be done from any cell that contains a nucleus; for instance taken from blood, semen, saliva or hair samples which is considered intrusive by many users. However, DNA as a biometric for identification uses a very small amount of non-coding genetic information which does not allow deciphering a person's initial genetic heritage. At present, DNA analysis is performed in specialized laboratories and is expensive and time-consuming (roughly 4 or 5 hours for the whole procedure). Moreover, the complete lack of standardization means interoperable systems are a long way off. Moreover, DNA techniques are currently being used by Law enforcement. Thus, any wider deployment of DNA-based biometric techniques in the future, if these do indeed become quicker and cheaper, will always face acceptability problems.

It seems, therefore, that it will be a long time before DNA printing becomes a real-time biometric authentication method. However, a Canadian laboratory recently announced a proprietary DNA extraction process which takes only 15 minutes and needs only simple equipment. According to (Crow, 2001), who foresees that DNA analysis could be done in real time, future technical improvements will be of two types: firstly more automation and more accuracy in the existing processes, and secondly the building of new systems (that only require very small amounts of material to provide an identification).

### 3.4.2 Evaluation of biometric systems

At first, comparing the error rates of the different systems in each modality and in a restricted number of environments per application, using estimates of FAR (False Acceptance Rate) and FRR (False Rejection Rate) one may reach conclusions as to performance. In fact, the performance of the systems is highly dependent on the test conditions (laboratory conditions with a small database and relatively good quality data). Moreover, fair evaluation should include forgeries (natural or simulated) in the database and this is very rarely done. Fingerprinting and face recognition are subjected to independent international evaluation annually[73] (Blackburn et al.,

[73] FINGERPRINT VENDOR TECHNOLOGY EVALUATION, 2003 http://fpvte.nist.gov/

2002) which now aims at testing more operational situations. Unfortunately, no openly-available evaluation on iris recognition is being conducted.

Table 12 below (also table 8) gives what we consider to be the most accurate information available on biometric performance (Jain et al., 2004) (at least order of magnitude estimates of the performance of the state of the art systems).

TABLE 12 (table 8): Selected technology error rates

| Biometric | Face | Finger | Iris |
|---|---|---|---|
| FTE % Failure To Enrol | n/a | 4 | 7 |
| FNMR % rejection rates | 4 | 2.5 | 6 |
| FMR1 % verification match error rate | 10 | <0.01 | <0.001 |
| FMR2 % identification error rates for dB size > 1 m | 40 | 0.1 | N/A |
| FMR3 % screening match error rate for dB sizes=500 | 12 | <1 | N/A |

Typical biometric accuracy performance numbers reported in large third party tests. FNMR (also FRR) and FMR (also FAR). N/A is non-available data.

More generally, in the evaluation of operational biometric systems, criteria other than performance have to be taken into account, e.g. robustness, acceptability, facility of data acquisition, ergonomic aspects of the interface, enrolment and identification time. When choosing a practical fingerprint system, for example, the robustness of the sensor, the possibility of wrong or clumsy manipulation, and dirtiness, must be considered (Maltoni et al., 2003). It should also be remembered that a relatively large part of the population will be unable to enrol with any chosen method. Alternative processes will always have to be found for any specific application.

### 3.4.3 Challenges and limitations

#### 3.4.3.1 Resistance of the system to forgeries

Fraudulent reproduction of biometric data is possible; this depends heavily on the modality, application and resources being considered and availability of the data to be reproduced. Different questions should be considered when deciding whether a biometric system can be fooled. Is it technologically possible to reproduce biometric data artificially? How easily available is the data? (Is the person's cooperation needed or not?) Is it possible to design biometric sensors that can detect impostors?

While it is not easy to for example get a good three dimensional image of the finger it is relatively easy (using a dentist's kit) to get latent fingerprints left by a person on different surfaces and objects and use them to reconstruct a fake finger (still not very reliable). There are also behavioural tests of 'liveness'; some rely only on software, but some require special hardware which distinguishes by physical means living from dead tissue. Nonetheless, a fake finger that would fool all the vitality

FERET Database. NIST 2001 http://www.itl.nist.gov/iad/humanid/feret/

detectors in a fingerprint sensor could still be built, given sufficient resources, as pointed out in (Maltoni et al., 2003).

#### 3.4.3.2 Biometric data storage

Biometric data may be stored on portable media such as smart cards if they will be used in verification mode. This ensures that the data cannot be used without the user's own authorization, contrary to what happens with data stored in a central database. Biometric verification/identification can also be realized through remote access, by transmission of the biometric image or template through a network to the device that will process the decision step. This requires a highly secure connection. Watermarking could be used in this case to ensure that the transmitted data have not been corrupted.

Of course, smart cards can be lost or stolen. For this reason, the data they contain must be encrypted and backed-up. However, if the information is stolen, it is necessary to be able to revoke it and to produce another template which could be used for further identification. Revocation is easy when dealing with pin codes or passwords but not with biometric traits as we cannot change our irises or our fingerprints.

Cancellable biometrics (Kumar et al., 2004) is a new research field and some preliminary propositions have been made. It is possible to generate new facial images for a person by filtering the original image. The coefficients of the filter are randomly generated thanks to a PIN code. Changing the PIN code means changing the filter, and therefore, changing the facial image generated. It has been demonstrated that for face recognition this process does not affect the result of recognition, if the matching algorithm relies on correlations. More research is needed to confirm these results on other face recognition methods. The use of such filtering is not straightforward for fingerprints or iris recognition, because it affects the quality of the images and the accuracy of the minutiae detection (fingerprint) or texture analysis (iris). For iris recognition, one solution is to extract a shorter code from the 2048 bit length code and to use only this information in the matching process.

#### 3.4.3.3 Biometrics as a way to increase privacy, anonymity and security.

Biometrics, depending on the way they are deployed, could enhance the security and the privacy of the users. Biometric Encryption can thus be used. The fingerprint of one person can be used to produce a PIN which for example allows access to a bank ATM. The coded PIN has no connection whatsoever to the finger pattern. The finger pattern only acts as the coding key of that PIN, any PIN. What is stored in the bank's database is only the coded PIN. The fingerprint pattern, encrypted or otherwise, is not stored anywhere during the process. Moreover, the successful decoding of a PIN confirms a person's eligibility for a service without having to reveal any personal identifiers; since only the user can decode the PIN (indicating also physical presence), the transaction can go ahead. There is also an indirect benefit to privacy. A user can continue to have a multitude of PINs and passwords, and thereby achieve "safety through numbers", rather than having one single

identification which links everything. However, there are still technical problems with Biometric encryption. Some (Uludag et al., 2004) solutions have been already proposed and some patents (Soutar et al., 1999) applied for, but further research is still needed. The fact that biometric patterns are never exactly the same from one data acquisition to another, renders the production of a private key, which has to be similar at each stage, very difficult.

### 3.4.4 Multimodality

The use of several modalities can be considered in order to:

1) *Improve the efficiency* of the overall system.
   A single modality biometric system can be subject to a high level of errors. Some errors can be due to *noise* associated with the acquired data, or to *intra-class variability* (from one data acquisition to another). In addition, biometric systems may be attacked with forged data, or genuine data of a dead person. Using several different modalities together aids in dealing with such unimodal problems, especially when complementary biometrics such as behavioural and physical, which may be discriminative or not, are used (Jain et al., 2004a). Indeed, multimodality has a clear impact on performance and attacks by impostors. For instance, by combining fingerprint with hand shape or face the use of fake fingerprints may be circumvented, since faces and hands are more difficult to fake than fingers.
2) Provide alternative paths, thus *enhance system flexibility*.
   Different modalities can also be used in parallel allowing the use of the system for different objectives; for example a biometric system built for both fingerprint and face recognition, could use the face in verification mode, if the user has a problem enrolling a fingerprint. Moreover, in case some biometric trait is temporarily unavailable the other one could be used to allow access. If the user has, for example, a temporary eye problem that makes the iris scan impossible, in a multimodal system fingerprints could be used instead. The same would apply in cases where people refuse to use a specific modality (for religious or health purposes, for instance). A multimodal system therefore allows flexibility by providing alternatives in the identification process.

### 3.4.5 Application Issues

"Mass Identification" applications (border control, National ID cards, Visas etc.) which demand a high level of security (very low FAR) must be distinguished from domestic, or personal applications (personal access to PCs) for which the constraints are low FRR and friendly interfaces.

Mass identification involves: (a) Storage of the data on a central database; (b) High accuracy level; and (c) User constraints for high quality enrolment. In this case, the size of the population may be a problem, when considering access times to a database, and the fluidity of the entire process etc. Interoperability is another issue: if a border control system is to be used in several Schengen area entry points, either the same system has to be used by all Schengen States, or the different systems

must be interoperable (which means that software and hardware on multiple machines from multiple vendors must be able to communicate). Interoperability between different systems is achieved by using common standards and specifications. At the moment, the standardization of the data formats (for iris and face recognition, and fingerprints) is rapidly becoming an important concern with the ISO- SC37 commission. It seems that standardization constraints are essentially suitable for verification systems (1:1) but they increase the processing time of large-scale identification, which can be detrimental to the systems. Very few tests have been conducted so far dealing with real interoperability issues, which thus remain a fundamental concern.

In the second type of applications, the focus is on transparency and comfort for the user. In this case, non-intrusive biometrics may be used such as video recording, from which a sequence of images can be obtained, providing different types of correlated information such as gait[74], voice in correlation with the face images. None of these modalities is efficient enough to be used alone. However, the complementary aspect of the information that the joint use would provide, will be an important tool to ensure final reliability in the identification of people.

## References (Chapter 3)

**(Ashbourn, 2002a)** Ashbourn, J. Biometrics: Advanced Identify Verification: The Complete Guide, Springer-Verlag. 2002 ISBN 1-85233-243-3

**(Ashbourn, 2002b)** Ashbourn, J. BANTAM User Guide: Biometric and Token Technology Application Modeling Language. 2002 ISBN 1-85233-513-0

**(Ashbourn, 2003)** Ashbourn, J. Practical Biometrics: From Aspiration to Implementation, Springer Professional Computing. 2003 ISBN 1-85233-774-5

**(Blackburn et al., 2002)** Duane M. Blackburn, Mike Bone and P. Jonathon Phillips. *Facial Recognition Vendor Test 2002*. DOD, DARPA and NIJ, 2002 http://www.dodcounterdrug.com/facialrecognition/frvt2002/ frvt2002.htm.

**(Chang et al., 2003)** Chang, Bowyer and Flynn "*Face recognition using 2D and 3D Facial Data",* IEEE international workshop on analysis and modeling of faces and gestures, pp. 187-194, October 2003.

**(Crow, 2001)** James F. Crow ,"*DNA Forensics : Past, Present and Future*", 2001

**(Daugman, 1995)** J. Daugman, "*High confidence recognition of persons by rapid video analysis of iris texture*"**,** European Convention on Security and Detection, pp. 244 -251, 16-18 May 1995.

**(Dorizzi et al., 2004)** B. Dorizzi, P. Lamadeleine, C. Guerrier, J.L. *Les Jardins : Biométrie : Techniques et usages*, Revue des sciences et techniques de l'ingenieur, Avril 2004

**(Jain et al., 2004)** Anil K. Jain et al : "*Biometrics: A grand Challenge*", Proceedings of International Conference on Pattern Recognition", Cambridge, UK., August 2004

**(Jain et al., 2004a)** A. K. Jain & A. Ross, *Multibiometric Systems*, Communications of the ACM, January 2004/Vol. 47, N°1

[74] Baseline Algorithm and Performance for Gait Based Human ID Challenge Problem, http://gaitchallenge.org

**(Kumar et al., 2004)** B.V.K. Vijaya Kumar and P.K. Khosla, Marios Savvides, "*Cancelable Biometric Filters For Face Recognition*", International Conference of Pattern Recognition, ICPR 2004, Cambridge.

**(Maltoni et al., 2003)** Maltoni D., Maio D., Jain A.K., Prabhakar S., *Handbook of Fingerprint Recognition*, Springer, 2003.

**(Phillips et al., 2000)** P.J. Phillips, H.J. Moon, S.A. Rizvi, and P.J. Rauss. *The FERET Evaluation Methodology for Face-Recognition Algorithms.* T-PAMI, 22(10):1090–1104, October 2000.

**(Soutar et al., 1999)** Colin Soutar, Danny Roberge‡, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar « *Biometric Encryption* »™, Bioscrypt Inc. , The content of this article appears as chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nichols, McGraw-Hill (1999)

**(Uludag et al., 2004)** U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "*Biometric Cryptosystems: Issues and Challenges*", Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92, No. 6, June 2004.

**(Xu et al., 2004)** C. Xu, Y. Wang, T. Tan and L. Quan, "*A New Attempt to Face Recognition using 3D Eigenfaces*". In 6th Asian Conference on Computer Vision (ACCV), Vol. 2, pp.884-889, 2004.

For further information:
The host papers to the four summaries presented here

- Ashbourn, Securing Our World – a study with particular reference to border control
- Avanti non-profit web resource ( www.avanti.1to1.org )
- BBC News, "Long lashes thwart ID scan trial", 7 May 2004, http://news.bbc.co.uk/2/hi/uk_news/politics/3693375.stm
- R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, *Guide to Biometrics.* Springer, 2003.
- Jain-29. C. Wilson, M. Garris, and C. Watson, "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints" NISTIR 7110 , May, 2004 http://www.itl.nist.gov/iad/893.03/pact/ir_7110.pdf
- NIST report to the United States Congress, "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability." Available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf , Nov. 2002.
- P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J.M. Bone, "FRVT2002: Evaluation Report" http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf
- Wayman et al Biometric Systems – Technology Design and Performance Evaluation ISBN 1-85233-596-3
- The Biometric Consortium web resource ( www.biometrics.org )
- US Dept of Homeland Security ( www.dhs.gov/dhspublic )
- The International Biometric Foundation ( www.ibfoundation.com )

# CHAPTER 4: BIOMETRICS in 2015 - A scenario exercise

## *4.1 Introduction*

The introduction of this report presented the four scenarios: (i) Biometrics in Everyday Life; (ii) Biometrics in Business; (iii) Biometrics in Health; (iv) Biometrics at the Border. In this chapter, the scenarios are analysed and placed in context.

BOX 3: SCENARIO METHODOLOGY

Scenarios are considered to be one of the main tools for looking at the future but it is important to clearly situate what their objective is. Normally, their objective is not to predict the future but to present plausible futures in order to understand what might happen in the future. Scenarios are used to stimulate discussions on the major technological, economic, social and political factors that are to be taken into account when thinking about possible futures. In theory, the number of possible futures is almost infinite, but usually, scenario exercises reduce them to a manageable three to five 'futures possibilities' (Godet, 2000 and Gavigan et al., 2001, Wilkinson 1998).

There is no single approach regarding scenarios, but scenario exercises are commonly the outcome of group work, group discussions and/or scenario workshops (Massini et al., 2000). About 15 people were involved in the biometrics scenario activity: the IPTS authors of this report who held numerous internal discussions and then discussed and tested their ideas with the external experts that contributed to the report (see acknowledgments).

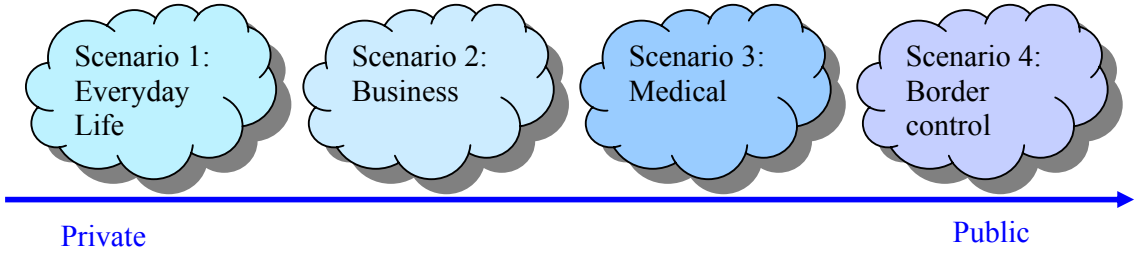
Since there are different types of scenarios, it is important to specify which type of scenario is being developed. The biometrics scenarios presented here are *trend or reference* scenarios. They start from the present and work forward on the basis of to be expected trends and events. They are intended to be realistic rather than for instance normative or extreme (Massini et al., 2000). Normative scenarios are for instance, the IPTS/ISTAG scenarios on Ambient Intelligence (ISTAG 2001). They present a desirable vision of the future and the necessary steps to realise that vision (back-casting). An example of trend scenarios are the MUDIA scenarios on how (online) media are expected to evolve in the future (Punie et al., 2002).

The objective here is to open up the scope of thinking on the future of biometrics, beyond the current passport and visa application plans. One of the themes of this report is the so-called "diffusion effect", i.e. as biometric technologies become better, cheaper, more reliable and are used more widely for government applications, they will also be implemented in everyday life, in businesses, at home, in schools, and in other public sectors. The scenarios therefore try to envisage what the results of this diffusion effect might be.

The four scenarios are carefully selected to encompass key environments for the introduction of biometrics. These environments differ for instance, in terms of the role played by governments and public authorities; in fact they can be placed on a

continuum, as shown in the figure below, with private actors predominant in the first two scenarios and public actors in the last two. The everyday and business scenarios have limited government involvement. The medical environment, particularly in Europe, is a public/private environment that is carefully regulated, not least as a result of the government's budgetary involvement in health provision. The fourth scenario, biometrics at the border, is not only regulated but also under strong control of public authorities.

FIGURE 6: Four Biometric Scenarios Developed




These differences between the four scenarios can also be viewed with respect to the issues of privacy and security. The use of biometrics at the border has clear security purposes which are likely to take precedence over privacy. This is clearly not the case in the everyday scenario where privacy, particularly in the home, is legally and socially protected. The implementation of biometrics in business will also have to take into account privacy and data protection rules. But the protection of personal data may be strongest in the case of the biometrics in health, given the sensitive and thus private nature of medical data. The objective is not to detail all these issues but rather to raise awareness that these differences exist and that they will have an impact on how biometrics can be implemented.

These four scenarios thus present different contexts for the use of biometrics. The choice of biometric technology for each situation is based on the analysis outlined by Chapter 2. Nevertheless the specific examples should be seen as illustrative rather than a prediction of how and where each technology will be used. The scenarios are neither mutually exclusive nor all-encompassing but they do present some of the major domains for biometrics applications in the future: work, private life, government and health.

## *4.2 Scenario on biometrics in everyday life*

The everyday life scenario describes a day in the life of a traditional nuclear family. It is a middle-class dual-income household with two children, a teenager and a toddler. As both parents work, the grandparents provide support in managing the household. The scenario is presented as a diary entry by the teenage son, Constantin. He is in trouble at school because he has spoofed the cafeteria's biometric entry system in order to help out a friend. His mother, who is called to the school to discuss this, has a car with a fingerprint scanner to start the engine. Grandmother goes to pick up the youngest son but the nursery's multimodal biometric system falsely denies her entry. On the other hand she has no problem

with the face recognition system used on the buses. At home, there is a common digital storage space called the virtual residence, where password access is replaced by an iris scanner. There is also a biometric toy that recognises registered users. Household appliances can also use biometrics to secure access, such as the cooker (which uses hand geometry). Finally, unauthorised use of computer games is made more difficult via biometric authentication, in this example, using a fingerprint.

1. Spoofing physical access/entitlements:

The scenario shows that spoofing biometric systems is clearly possible. It does not only depend on the biometric technology – though certainly some technologies (e.g. iris) are more difficult to circumvent than others – but also on the way the technology is implemented (e.g. thresholds and hardware). In the case of the school cafeteria entry system, cheap iris scanners make the system easy to fool. To be able to discover spoofing, systems need to check for irregularities such as double entry attempts (manually or automatically). This is easier to do within a closed system which has a small local database, like the one at the school, compared to a large-scale database containing millions of stored templates.

2. Biometrics to replace keys (for convenience and security)

The fingerprint scanner in the car is installed to prevent unauthorised use and theft. It is a local system that only needs to verify a limited number of authorised users (and Constantin, the son, is not one of them). Enrolment will probably need to be managed by the car owner. The system is installed/bought for security reasons. Insurance companies can stimulate the demand for such systems. For users it is convenient since they always have their keys with them (i.e. the finger) but in the case of breakdown, alternative procedures need to be available. These may however take some time, as suggested in the script. It may for instance be the case that spare keys are available at home or at an authorised dealer or garage.

3. Physical access and security thresholds

The biometric technology for access to nurseries needs to be highly secure. Therefore, the nursery combines two biometric technologies, in this case face and voice recognition. Templates will probably be stored in a central database but within a closed system. The threshold for false acceptance is set low at the expense of a higher false rejection rate. This may mean that regular (e.g. yearly) enrolment is necessary since people's biometrics may change (slightly) over time. Face recognition seems to be particularly sensitive to this problem but more generally, regular enrolment is an issue for all technologies. Being falsely rejected may cause user annoyance and user frustration, and as a result, may negatively affect the quality of a submitted biometric trait (e.g. granny's voice) as it is not pleasant to be wrongly rejected by an automated system. In the end, human intervention needs to be available as a fallback procedure.

The public transport face recognition system is used to check if people are entitled to use it (i.e. have they paid the correct ticket?). The threshold is set in favour of convenience, i.e. allowing more false positives. In contrast with the nursery where

there is a central database, templates for the public transport system will most likely be stored on a smart card. The less likely alternative would be that buses connect wirelessly in real time with a central database for matching.

4. Digital access

Biometric access to digital spaces can replace knowledge-based password access. Secure access to a shared digital space also makes personal digital territories possible within that common folder (e.g. Beslay & Punie, 2002). Another issue here however is related to usability. Taking a biometric scan – be that fingerprint, face or as in the case of the scenario, iris – requires a clear positioning of the biometric trait on the scanning device for a good result. Scanning devices are not always designed in a user-friendly way (e.g. making sure the user knows what to do, where to focus or how to push) nor are people always in the position to provide the trait in the prescribed way, as illustrated in the scenario (the father is short-sighted). The iris recognition system is bought off-the-shelf and is installed and managed by the end-user.

5. Biometric toys

The biometric toy is introduced to illustrate the possibility of alternative uses and business models that are not inspired by security, safety and convenience. It shows that biometrics can be used in a playful way as well. Biometric technologies can enable the recognition of people in a natural way. They are part of the repertoire of so-called natural interfaces that envisage human-machine interactions becoming more similar to the way humans interact with each other in the real world (via speech, gesture, touch, look, etc.).

Biometric toys could contribute to the wider acceptance of biometrics in society, not only because children would in this way already be acquainted to them and would learn to use biometrics when there are still young but also because such localised and off-line applications have less privacy and security concerns. It may be necessary however to pay special attention to raising awareness and education because there is a fear that the use of biometrics by children may desensitise them to the data protection risks that they may face as adults through the use of their biometrics.[75]

6. Biometrics for safety vs. reluctance to use them

The use of the cooker is protected by a hand geometry reader to avoid accidents with children. The choice of the hand as well as other biometrics that are based on touching (e.g. finger) may appear as natural in the kitchen but at the same time may be less suitable there, since hand and fingers get dirty while cooking. This also affects the biometric sensors. Contactless biometrics such as face could be more suitable here.

[75] Data Protection Working Party - Working Document on Biometrics, 01/08/2003 http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf

The example also shows that people can be reluctant to use certain but not all biometrics. They may be accustomed to using biometrics and they may not be against them as such but they just get tired of using them all the time, or rather, of enrolling again and again for each stand-alone application that one can imagine.

7. Biometrics for Digital Rights Management

Biometrics might be useful for digital rights management (DRM) to replace code and/or password protected files. It can be assumed however that people, especially youngsters, will look for possibilities to bypass these systems. The example shows that fingerprint spoofing may be possible, but also that it takes some time to do, especially when taking into account that the newer generation fingerprint sensors have a liveness detection functionality.

To summarise, the everyday life scenario illustrates that people can be confronted with biometrics in many different ways in their lives. They are used to secure access – that is to prevent unauthorised access – to both physical and digital places but also to check entitlements. The can be installed – voluntarily or not – for the protection of both physical (e.g. car) and digital goods (e.g. DRM). They might be used for safety purposes (e.g. cooker) but also for toys.

It is clear that biometric technologies are never 100 percent secure. Choices need to be made between different biometrics. But mutually important is the implementation. Thresholds need to be set and decisions need to be made, usually in the form of trade-offs. Finally, some usability and user acceptance issues are raised. People may accept biometrics for certain aspects and reject them for others.

## *4.3 Scenario on biometrics in business*

Biometrics in business encompasses the use of biometrics by companies. This can be for internal and external purposes (e.g. with employees internally and with clients, other companies or third parties externally). The scenario is presented as a memo to senior management of a large multinational supermarket chain that has embraced the use of biometrics but is concerned that it is not reaping the expected benefits. The memo raises several issues, such as a biometric access system to the company premises and secure electronic payments enabled by a third party. Customers also make use of biometrics in order to access shops. The sharing of biometric databases between companies is highlighted as a new use of biometrics to be pursued.

1. Staff access to company premises

Biometric access to company premises may be installed to allow only authorised people to enter, but it can also be used to in order to manage people more effectively. In this case, it is used for checking working hours. The memo implies that with the older system of punch-cards, punching could be done by someone else. With biometric authentication, this becomes much more difficult.

The staff entrance situation also highlights the importance of human factors when using biometrics. Alternative procedures need to be foreseen for the cases where biometric access is refused and these procedures might be neglected, as humans tend to do when it is more convenient for them. The scenario foresees human monitoring of the system to ensure correct use. Another usability issue is raised with the example of sweaty hands, showing that both physical and psychological factors can decrease the performance of biometric applications.

2. Electronic payments

Electronic payments require strong authentication. Biometrics can add an additional layer of security to the process, which is particularly desirable when large amounts of money are concerned. To enable this, banks may want to have biometric authentication that is managed by them, in order to verify and guarantee correct enrolment and regular re-enrolment. Enrolment may be local while the database is centralised. Adding a biometric to the transaction also enables stronger control *a posteriori* in the case that something goes wrong, since the person who transferred the money can be identified.

3. Companies and their customers

The use of biometrics in stores shows that companies will probably need to convince customers to enrol and participate in their biometric systems, especially if it is not clear what the added value for the customer is. For the companies, one of the reasons to invest in biometrics might be to identify and know customers better, so that more products can be sold and logistics can be improved. Companies however, will have to address bottlenecks in terms of accessibility, privacy and customer acceptance. Customer reluctance may be tackled by offering a financial benefit (e.g. price reductions, enrol and win, promotions) or by providing strong privacy protection (pseudonymous biometric system).
The supermarket chain's initial idea was to use biometrics to provide people with a personal greeting when they entered the shop. But this initiative was withdrawn because it was perceived to be very privacy invasive. As noted in the memo, customer preferences have been monitored for many years via loyalty cards but that may be less visible compared to biometric identification.
Companies may also need to think about how to deal with customers that cannot provide the biometric feature and as a result, are excluded from these benefits.

4. Sharing of enrolment and databases

The implementation of biometric applications in the business environment might be quite cost-intensive and laborious, and as a result, might make biometrics less feasible for smaller enterprises. To tackle this, it is imaginable that companies will want to collaborate and create virtual networks for sharing biometric investments and biometric applications. Why not share the enrolment process, rather than each company organising its own enrolment? Why not share biometric databases, rather than each company setting up and maintaining its own database? Also for customers, this might be interesting since a network of companies can offer a single

enrolment. This raises however many questions in terms of security, privacy, liability, maintenance, etc.

It is not explicitly mentioned in the scenario but the biometric experts consulted for this report made clear that there is currently little knowledge on the potential of biometrics in business outside the well-known security and safety schemes. Convenience can be a driver but it is not clear if it will provide enough reason to invest in biometrics.

## 4.4 Scenario on biometrics in health

The biometrics in health scenario presents a series of emails between doctors in two different countries, describing various applications that exist in each. Adele Mattsson, the first doctor, describes how biometrics have been implemented for physical access and network access and mentions an example of an unsuccessful application. Vasily Nowak replies with a description of an electronic health card and identity checks in the maternity ward. Adele's second email offers a subjective opinion on the applications and biometrics in general.

Prior to discussing the script, a few general points can be made on this scenario. Positive identification is essential in the health sector. Retrieving medical histories, administering medicine, handing out prescriptions, carrying out medical procedures, all rely on the correct identification of the individual. In addition there is a strong need for privacy which stems from the sensitive nature of medical data. These two requirements make the health sector a likely field for the application of biometrics[76].

1. Physical access:

In the first situation, biometrics are used in order to limit access to restricted areas to authorised staff alone. Missing medical supplies are an acknowledged problem faced by hospitals and clinics; there therefore seems to be a cost incentive to introduce biometrics as a solution. Hospital administrators can estimate the cost of missing supplies and compare this to the cost of introducing a biometrics-based system or a non-biometrics-based system. It is therefore possible to evaluate the benefits of introducing such a system. As the application operates within a closed environment with a limited number of users, there are no issues of interoperability and high performance levels might be achieved. One point to note here is that biometrics are just one part of the overall technological solution; the scenario describes how systems also make use of other elements such as RFID tags and smartcards.

2. Network access:

A frequently proposed use of biometrics for the health sector involves access to electronic health records; biometrics can be used to ensure that only authorised

[76] See for instance a prospective view on eHealth being a prominent application area in the transition towards a socially inclusive and sustainable knowledge society: http://fiste.jrc.es/pages/ehealth.htm

people have access to sensitive medical information. This application draws on many of the advantages of biometrics: a biometric cannot be lost or forgotten and it cannot be lent to an unauthorised person. Adele mentions in her email that people need many different passwords for the different systems they have to access: patient records, appointment schedules, financial records. People commonly use the same password for all systems or write passwords down. The solution is a single-sign on system where one biometric is used as a password for all systems. This application offers convenience and leads to greater security as people use the system correctly.

*Choice of biometric technology*

The choice of biometric technology always depends on the context within which it will be deployed. In the medical sector, there are additional factors to take into account, e.g. fingerprints will not work in environments where users wear latex gloves, face recognition will not work with surgical masks, voice recognition will not work in noisy environments. On the other hand, in the case of network access, if a doctor is accessing files with a laptop from remote locations iris recognition will be unsuitable because the scanners are both expensive and bulky. Cross-contamination through contact readers is an issue of particular importance within a hospital environment and the scenario mentions some ways of minimising this risk.

3. A failed application

The third situation describes an example of a failed application. The specific details are not the issue, but the script tries to emphasise the point that biometrics are not a panacea for all ills. They are a tool with certain benefits and drawbacks, which may be used as part of a wider application in answer to a specific problem. Applications need careful design to fit in with working practices and other practical considerations.

4. Maternity ward

Maternity wards are a field where biometrics have already been tried out for security reasons in order to prevent people taking someone else's infant. Once again it is a small-scale closed system (limited users and no issues of interoperability). Biometrics are a natural solution for confirming and linking the identities of mothers and children and there has been public support in areas where this has been implemented as people perceive the benefits.[77]

5. The health card

The health card, described next, is a complex issue. Both private health insurance companies and public authorities have a vested interest in ensuring that only those eligible for treatment receive it. Biometrics could be instrumental in tackling fraud in the health sector and in fact there are several instances where biometrics have already been introduced in order to cut down on health insurance fraud.[78] There are

[77] Trials have been carried out in Bavaria (Germany) and Madrid. Source: Sasse
[78] For examples see http://www.nwfusion.com/news/2004/121304biometrics.html,

two ways a biometric health card could be implemented: with or without a centralised database.

6. Tele-care or home healthcare

A great benefit of biometrics is the ability for remote authentication. This potential is mentioned in passing in the script but is worth reflecting upon. So far security worries as well as technological limitations have stopped the widespread adoption of eHealth applications. For home healthcare in particular, it is important to be able to remotely identify patients. Biometrics offer the power to do this and could therefore enable many interesting applications that would otherwise not be able to make it off the drawing-board.

## 4.5 Scenario on biometrics at the border

As part of the international drive for greater security at border control, the ICAO has recommended the introduction of biometric identifiers on machine readable travel documents (MRTD). The European Parliament has voted in favour of proposals for biometrics on passports and visas, in accordance with ICAO recommendations. Taking the introduction of biometrics on MRTD as a given, the aim of the fourth scenario is to highlight issues raised by the implementation of biometrics at the borders. The story presents a father, daughter and grandfather, making a trip around the world, with stops in Dubai, Beijing and Bangkok. By focusing on three destinations and three family members, the scenario illustrates the use of biometrics in different countries, by different age groups. We follow the family through the process of obtaining visas to the journey itself. The analysis presented here briefly discusses the topics raised.

1. Visa applications

*Closed vs. open systems*

Visa applications are a closed system and therefore each country (or group of countries in the case of the Schengen States) can choose a proprietary technology and store only biometric templates rather than full images. In contrast, passports are an open system as they have to be readable by foreign border control authorities. In open systems, interoperability is an issue of particular importance and for this reason the ICAO has recommended storage of the full biometric image on passports.

*A few dominant technologies*

Some countries may choose not to have visas (in our example this is the UAE) while others may implement whichever biometric technology they see fit. If different countries use different technologies, it will lead to inconvenience for citizens as they will have to go in person to enrol their biometrics at the embassy of the country for which they are obtaining a visa. Sovereign states will want to select the biometric technology that best fits their needs, but at the same time they may want to avoid costly enrolment procedures at local embassies by using a biometric

available on the passport. It is likely that these two factors will lead to a few dominant technologies being used for all border control applications.

2. Correct enrolment

The importance of correct enrolment is emphasized for the visa application, but the point is equally valid for any type of enrolment (passport, ID card, driving licence, etc.). An application is only as secure as its weakest point; if it is possible to make a fraudulent enrolment, the application quickly loses its value. For this reason the ICAO has suggested using biometrics in order to verify the identities of supervising staff and to confirm they have the authority to carry out the tasks they perform.[79]

3. Schengen zone

Although biometric controls will be introduced at external borders, the scenario shows that the Schengen Agreement continues to apply within the EU. The Schengen acquis is going to be further developed within the institutional and legal framework of the EU, including the use of biometric data for checks at external borders.

4. Confirmation of presence

An article from the in-flight magazine draws attention to a different benefit of biometrics – the ability to confirm an individual's presence. Biometrics in fact are the only automatic tool that can verify the presence of a particular individual. Passwords and security cards can be shared or lost, but biometrics are an integral part of the individual. This unique property could have many applications. In the story, Schiphol Airport has introduced biometrics in order to authenticate the presence of airport control tower staff.

5. Iris scanner at Dubai and the watchlist

The scenario imagines that at Dubai a watchlist is used instead of visas, i.e. a database where the biometric data of certain individuals is stored. In our example the watchlist contains the details of people who have been banned from the country and therefore should not be allowed entry. Passengers are checked against this database and if they do not match a record, they are allowed to enter the country.

6. Advanced Passenger Information (API)

API is used to carry out a type of watchlist operation in advance of travel (for further details see reference below[80]).

[79] Biometrics Deployment of Machine Readable Travel Documents – Technical Report, ICAO

[80] API: Data on each passenger (as contained in the machine readable zone of the passport) is captured by the airline during the check-in process overseas, formatted by the airline's reservation/control system and transmitted to the centralized Customs system, where it is checked against inter-agency data bases and watchlists. The results of these checks are then downloaded to the airport of arrival, where they are distributed to both Immigration and Customs. The accomplishment of this part of the process prior to arrival of the flight substantially reduces or eliminates the time-consuming data entry and computer processing required during the examination of each passenger from a flight on which API data was not transmitted. http://www.icao.int/icao/fr/atb/fal/api_f.htm

7. Revocation of biometrics

An important question which has not yet been answered is whether biometrics can be revoked, i.e. if a person needs to change identity or finds that his/her biometric data has been compromised, what can be done to revoke that person's biometrics. This question will assume even greater importance as biometrics diffuse into everyday life.

8. An example of DNA tests

There may be reluctance on the part of citizens to share biometric data, particularly of a sensitive nature such as DNA, with third countries outside the EU. For those who travel for leisure, there will always be the option to avoid countries where they do not feel comfortable with visa application procedures. For business travellers however, there may not be the luxury of choice. Decisions taken unilaterally by one country, may therefore affect a large portion of citizens.

9. Face recognition – controlling conditions

The success of biometrics at border control will depend largely on the method of implementation. The face has been chosen by the ICAO and EU as the primary biometric identifier. But face recognition is currently one of the less accurate biometric technologies. It suffers from technical difficulties with uncontrolled lighting and it therefore may be necessary to install the face recognition readers in booths where lighting conditions are carefully controlled. Measures, such as this one, may lead to improvements in accuracy but also to an increase in costs.

10. Difficulties at Bangkok airport

Biometric applications can and do go wrong sometimes and therefore secondary or back-up procedures are required to deal with these cases. The scenario shows just one such example. Iris recognition systems are believed to be able to match any person to their record by the third attempt. This may be true for regular users but Gerard the grandfather suffers from glaucoma. It has been shown that glaucoma can cause iris recognition to fail as it creates spots on the person's iris. When the machine rejects Gerard for the third time, officials take him aside for secondary procedures. This situation draws attention to several potential pitfalls for biometrics. Currently border control staff are skilled employees who use personal judgment in deciding who needs further questioning. There is a danger that these skills could be sidelined if border control starts relying heavily on automated biometric checks. Furthermore there has to be a recognition that biometric tests are statistical by nature which means that there will always be a possibility however small that innocent individuals fail the verification. Secondary procedures must take this into account.

11. Queues

Biometrics at border control may be suggested as a way of automating the procedure, thus scaling back staffing requirements. The reality is that for the foreseeable future, border control staff will have an important role to play in supervising biometric checks, particularly early on in the implementation when

travellers are still getting acquainted with the technology. Secondary procedures will always have to exist to deal with cases where the biometric check fails. Frequent traveller programmes are sometimes cited as an example where biometrics can improve passenger turnaround times, but they work with a limited user base of passengers who travel often and are therefore adept at using biometric readers. Furthermore the travellers who may most need assistance (children, elderly people, disabled people, people without biometrics, etc.) are unlikely to be part of current frequent traveller schemes. Thus existing performance data may not accurately reflect the difficulties that may arise when biometrics are implemented on a large scale.

## *4.6 Concluding Remarks on scenario exercise*

The scenarios naturally place biometric applications at the centre of attention but it should be noted that in a future digital society, biometrics will be part of a larger IST (or Ambient Intelligence) environment that includes RFIDs and other digital technologies. As the cost of biometric technologies comes down and people grow accustomed to using them through border control and other government applications, it is likely there will be a diffusion of biometrics into everyday life. Tomorrow's diffusion effect provokes today's need for discussion.

The critical issues raised by the scenarios can be categorised under three headings: privacy, security and usability.

**Privacy**

The final email of the medical scenario makes the assertion that biometrics can undermine or protect privacy depending on the application and the implementation. The medical scenario demonstrates how biometrics can enhance privacy of medical records by replacing an easily-compromised system of passwords with a theoretically more secure biometric and smart-card combination. Similar situations occur in the everyday scenario with the use of biometrics to protect the teenager's diary and each family member's file-space. The medical scenario also suggests that a biometric template might be used as a key in a database of medical data so that a medical record can only be retrieved with someone's biometric. These applications show the positive side of biometrics.

On the other hand, biometrics can threaten privacy. The business scenario alludes to the potential for profiling with biometrics. Biometrics such as face, gait or voice recognition that may in the future allow humans to be identified passively (without requiring their consent), have provoked surveillance fears in some privacy campaigners. A policy question for the future will be deciding on the appropriate safeguards (legislative or not) to deal with such issues.

The business scenario also shows the use of biometrics for auditing working hours. In this case employees may resent or even obstruct the use of biometrics. In general, the principle of proportionality should apply when designing applications. The question to be answered is whether the use of biometrics is justified in the context

or whether some other means of authentication could equally well fulfil the requirements.[81]

**Security**

The fundamental question from a security point of view is: how secure do systems need to be? For a particular application is it more important to prevent impostors (low false accept rate) or to let through the right people (low false reject rate)? This question is broached by the everyday scenario when comparing the access system at the nursery to the season ticket for the bus. At what cost are we willing to achieve high security? The cafeteria system at the school installs cheap iris readers to save on costs resulting in a system that can be spoofed. Arguably for a school cafeteria, the additional security provided by better readers does not justify the cost. In contrast, for the medical sector it will be crucial to ensure that it is not possible to spoof access systems. If spoofing is possible, then a biometric system loses much of its security value and cannot guarantee privacy.

Security is not just determined by technical factors such as thresholds, hardware and prevention of spoofing. All parts of the procedure have to be equally secure, including enrolment, storage of the biometric template (if using distributed storage), maintaining and updating the database (if using central storage) and secondary procedures for when biometric tests fail. Secondary procedures are shown in three of the scenarios, at the nursery (the grandmother is checked against paper records), in the business (the employee has to go to a different gate when trying to gain access) and at border control (the customs officer has to receive confirmation of Gerard's visa from the embassy). Human factors have to also be taken into account; if biometric applications secure all other means of fraud, insider attacks may become more prominent.

**Usability**

The usability of biometric systems will greatly influence their success and acceptance. For universal applications (such as the health card) where all citizens are obliged to enrol, biometric systems will need to consider the needs of everyone, in particular people with disabilities, elderly people, children, etc. This is a very different proposition to a frequent flyer programme for example, where users fit a fairly specific socio-demographic and socio-economic profile.

In both the public and private sector, biometric applications will have to take into account working practices. The medical scenario for example, shows an example of an application which fails because it disregards the practicalities of the environment in which it is being implemented.

Secondary procedures also come under the category of usability. A person who fails a biometric test may either be an impostor or an honest person falsely rejected. For security purposes it is important that the secondary procedures are rigorous, but

[81] Reference: UK Biometric Working Group http://www.cesg.gov.uk/

at the same time, the border control and everyday scenarios show the embarrassment and agitation that this rejection may cause in a law-abiding person. With current performance levels, the number of people falsely rejected may be 1 in 100 or even 1 in 10 depending on the application and the implementation of the technology. This stresses the need for user-friendly secondary procedures.

# CHAPTER 5: CONCLUSION: The diffusion of biometrics

## *Security and privacy*

In pursuit of the Lisbon strategy to become an inclusive, dynamic, competitive and secure knowledge-based society, the European Union needs to provide its citizens and consumers with a 'trusted' online environment. Identification systems are key interfaces between the real world and the digital world, though often, they are invisible to users. Biometric technologies provide a strong mechanism for authentication and therefore can promote the development of a 'trusted' Information Society. Therefore, deploying biometric technologies is consistent with the Lisbon targets. This comes at the right moment as it will supply for the increasing need for identification in modern societies that are becoming more mobile, flexible and networked.

However, biometric technologies are still under development. Although some applications, in particular for law enforcement, have been around for a long time and have been developed on a large scale, it is only recently that advances in technology have both enlarged the field of possible applications and lowered their cost to a point where it now seems plausible that biometrics may be used for many more purposes. Fingerprint, iris, face and DNA – the four biometrics selected for detailed analysis within this study – have different strengths and weaknesses, making each of one more suitable for certain applications than for others; however, they all can be expected to spread in the foreseeable future.

The diffusion of biometrics is currently led by government applications with the aim of improving public security, such as the inclusion of biometric data in passports, but it will go far beyond these specific uses. As citizens get used to biometric identification in their dealings with border control and customs officials, the association with criminal behaviour will diminish and people may be more prepare to accept the use of biometrics for other purposes as well – for physical access control to private property and for logical access control (online identity), and even simply so as to enhance their convenience or for fun.

Of course, the main reason for introducing biometrics is to increase security and the sense of security. Although increased efficiency in law enforcement does not directly improve security, it can be argued that the use of biometrics acts as a deterrent to criminal, illegal or anti-social activities. In this respect, overblown claims about the performance of biometrics may actually prove helpful.

Nevertheless, since biometric identification is not perfect, neither is biometric security. There will be many false rejections (e.g. travellers with valid documents rejected by the system) depending on the threshold, which will create irritation. More importantly, there will be cases of false acceptance, i.e. allowing intruders access to the system by accident, and there may be scope for circumventing the

checks ("spoofing"). As the sense of security increases, the scope for fraud once inside the system will increase, too. Besides, criminals are likely to respond by changing tactics: if the only way to receive cash is with a live finger, using violence to get someone's fingerprint could replace stealing a credit card.

Beyond the use of biometrics for physical or logical access control, one other important attribute of biometrics is that they can allow confirmation of presence, i.e. by asking a person to provide a biometric sample it means that person is physically present. This can be useful for places such as airport control towers, medical operating rooms or drugs dispensaries.

Biometrics could also deliver improved convenience for the citizen in their everyday life based on the principle that they are always with you and can therefore be effortlessly used at any time. For this purpose it is necessary that they be intuitive to use and non-intrusive during enrolment and data acquisition, regardless of which biometric is used. Such applications could range from fancy e-toys for children to rapid supermarket check-out for their parents.

Then again, if biometrics are established as the only means of access, they have a great potential for inconvenience, too. If biometric access is faster than traditional means during the introduction period, but once established resumes the same speed as previous techniques (because now everybody uses it, or because the increased efficiency is used to cut back on staff), people will end up with an obligation to use biometrics without any corresponding advantage; they will perceive biometrics as an inconvenience. This will be particularly true for those whose biometric samples are prone to problems – which can be a significant percentage of the population. In addition, the more biometrics are used for everyday convenience, the more data or samples may be diffused and become compromised, thus making life more difficult.

Whether secure and convenient or not, the implementation of biometrics raises great privacy-related fears, such as fears of a "surveillance society" or "function creep". The worry from this perspective is that biometrics will become the common mode of identity recognition, biometric data will be linked to all other personal data, it may be subsequently shared with third parties for all kinds of other purposes, and sensitive information will be prone to abuse. In order to allay these fears, a reinforced legal framework for privacy and data protection may be needed; one that adequately addresses the new technological possibilities of biometrics, thus preventing biometrics from becoming a tool in the service of surveillance. The particularly strong need for effective privacy and data protection provisions regarding biometrics reflects the fact that our biometric data are an inseparable part of us, whilst any document is merely an item at our disposal – there is nothing separating the individual and his/her biometrics.

On the other hand, a key feature of biometrics is that they have the potential to enhance privacy. This is because biometrics, if properly used, can establish identity without connecting this identity to other data sets such as social security number, driver's license etc. Moreover, in verification mode biometric systems are able to authenticate a person's access rights without revealing his identity. Better

protection against identity theft also protects the privacy of those who avoid becoming victims. Moreover, since we carry all our biometrics are with us at all times, it is easier to use multiple biometrics to compartmentalise our personal information – we might not be able to remember ten secret codes, but we are able to provide ten different biometric samples to separately access ten different systems.

## *Other key aspects (SELT)*

Security and privacy are the obvious challenges presented by the deployment of biometrics. In addition, a group of experts provided insights on the social, economic, legal and technical (SELT) implications of biometrics for society. From their contributions, the following subjects emerge as the key characteristics of the transition to the biometric society.

### Social

The spread of biometrics and therefore the replacement of weak or no identification by strong identification may reduce the scope for privacy and anonymity of citizens. Implicitly, this may challenge the existing trust model between citizen and state. Currently, the technical limits to government efficiency provide an important pillar of citizen's freedom and autonomy. If governments become more efficient at identifying citizens in all kinds of situations, that trust model is likely to change.

Therefore, it is important to be clear on the purposes of introducing biometrics and realistic about their performance. Concerning the former, one has to consider the possibility that "function creep" will set in over time, i.e. that biometrics will be used for purposes other than those envisaged – and agreed – at the time of introduction. For example, currently separate biometric databases could be connected at some later stage. Concerning the latter, if biometrics are sold as a magic wand against all threats to society, expectations are bound to be disappointed and citizens might come to feel cheated. In that case, the automated decision-making, i.e. the delegation of control from human to machine, may be resented even more than it would otherwise.

Another crucial point to keep in mind is that biometrics can not work alone, but need a fallback procedure. For various reasons, including disabilities, age or sickness, a significant number of individuals might not be able to participate in an automated biometric identity verification process. Clear and equivalent procedures, i.e. with comparable security and ease of use, and without stigma, need to be foreseen for these people – if your fingerprint is not easily legible, that should not make you a second-class citizen.

### Economic

Biometrics provide strong identification. However, economic theory tells us that the strongest available identification is not always the optimal solution, as identification imposes a cost, which will only be compensated by the benefits of identity if these benefits are large enough. Moreover, an assessment of costs of

biometrics should not only look at the cost of technologies but also encompass the complete identification process, including for instance, the costs of (human) backup procedures.

In addition, strong identification changes the risk profile of circumventing the system: a stronger wall against illegal entry into an area or system will make additional inside measures less efficient, thus leading to their disappearance, which means that once the outer wall is breached, all doors are open to the intruder. As a result, identity theft for example may simultaneously become less likely and more serious.

In terms of the market development, the biometrics market has a number of characteristics which make a competitive market equilibrium unlikely. It is a network industry with strong complementarity, a tendency to "tipping", a few large launch projects establishing considerable first-mover advantage, and ample scope to use intellectual property rights to reduce or even prevent competition. Therefore governments, as launch customers with strong bargaining power, should use their public procurement policy to ensure that the market does develop into a competitive one, for example by using intellectual property in the public domain, such as open source software, or by spreading their procurement among several competitors, thus forcing interoperable solutions to emerge.

## Legal

The current legal environment in Europe is flexible and does not hinder the introduction of biometrics. However, it contains very few specific provisions with regard to the impact of biometrics on privacy and data protection. Existing data protection legislation does influence the implementation of biometrics, but it lacks normative content and some interpretation problems remain. Hence, new legislation will be needed when new applications become mandatory or biometrics become widely used.

Such legislation should be based on two pillars: opacity and transparency. On the one hand, opacity rules (privacy rules – prohibiting use) should prevent inappropriate collection of biometric data and lay down the conditions under which the use of biometrics should be allowed. On the other hand, if use is allowed, transparency rules (data protection rules - regulating use) should set out how the data can be processed and how the processing can be traced. Currently users are not encouraged to consider the repercussions of the enrolment process, even if strong identity is not required. An evaluation of whether a biometric application is appropriate and how it will operate should always consider local storage (for instance on a smart card), proportionality, whether a less intrusive method exists, reliability and consent. In this context, data encryption should be mandatory.

There is one further consideration for the increasing use of biometrics in law enforcement. In judicial processes, parties should have the right to meet the expert and be heard, an automatic right to counter-expertise is needed, and the likelihood of errors must always be contemplated.

### Technical

Biometrics are different from paper documents or secret codes. They cannot be lost or stolen (though they can be copied) and they cannot be revoked. Many (face, voice) are in the public domain. A biometric match is never 100% certain; the match depends as much on the threshold of acceptance as it does on the two sets of data to be compared. Individuals making verifications and those being verified need to be aware of the variability of the threshold and how that may vary according to the application. They should also be aware that the biometric technology itself is merely a part of the whole security system, which will work well only if the acquisition environment is properly set up, the storage is secure and the enrolment process is sufficiently controlled.

BOX 4: DG INFSO planned actions

The Directorate General for Information Society and Media of the European Commission has planned a number of actions to facilitate decision-making processes for the large-scale deployment of biometrics in Europe

- Stimulation of systematic exchange of information amongst the Member States on relevant deployment activities (pilots, trials, etc.). A dedicated web portal for this purpose will be launched in mid-2005.
- Establishment of an authoritative technical body on biometrics at European level: the body should advise European policy makers in taking informed and coherent decisions.
- Stimulation of the creation of a network for testing and certification of biometric devises and technology: The lack of commonly agreed quality standards still forms a major obstacle in the wider adoption of biometric solutions. Thus, the anticipated network will share and develop common frameworks and methodologies for biometrics assessment.

## *Recommendations*

The overall message from this study is very clear: the introduction of biometrics is not just a technological issue, it poses challenges to the way our society is organised, and these challenges need to be addressed in the near future if policy is to shape the use of biometrics rather than be overrun by it. To address these challenges, many issues have been identified in this report that may require action. We propose the following five major recommendations as the most urgent ones to be dealt with:

1. **Ensure clarity of purpose**
   The purpose and the limitations of any application must be clearly set out in order for biometrics to become acceptable to citizens. Legislators can allay citizens' fears by providing appropriate safeguards for privacy and data protection, in particular preventing so-called "function creep". Since there is more potential for abuse in biometrics than in traditional identification systems, especially if their use becomes widespread, the existing safeguards may need to be adapted in order to guarantee that the accepted principles of privacy, human rights and data protection maintain their effective force. This means in particular

that it should be considered whether the legal framework will need specific provisions on biometrics.

2. **Promote privacy-enhancing use of biometrics.**
   Whilst biometrics certainly raise fears related to the erosion of privacy, they also have the opposite potential to enhance privacy, because they are able to authenticate a person's access rights without revealing his identity. In addition, by using multiple biometric features it is possible to keep various sets of personal data separate from each other. The more policy encourages such privacy-enhancing uses of biometrics, the more biometrics will become acceptable to the public at large.

3. **Allow for the emergence of a vibrant European biometrics industry**
   The large-scale introduction of biometric passports in Europe provides Member States with the great opportunity to ensure that these have a positive impact. As the launch customer of the largest-scale implementation by far in Europe they can ensure the emergence of a vibrant European industry by insisting on interoperability and open standards. Avoiding automatic market dominance by the passport supplier and concentration of key intellectual property rights in a few hands will not only lower barriers for entry, but also ensure that the forthcoming competition will provide improved products and thus the creation of stronger global industrial actors.

4. **Provide for flexibility**
   A biometric identification system must be able to deal with all kinds of implementation problems. This involves: setting up appropriate fallback procedures for those with difficulties in providing biometric samples; developing the necessary ease of use for all involved groups including elderly people, children, overweight, very tall, disabled, ill, ethnic minorities etc.; and ensuring appropriate supervision and procedures to deal quickly and efficiently with the non-negligible numbers of false rejections. All these elements will have to be included in calculating the cost of an application.

5. **Conduct large-scale trials**
   Large information technology projects always have substantial 'infancy' problems, whether implemented by the public or the private sector. The large-scale deployment of biometrics for identification will not be any different. Law enforcement use of large-scale biometric databases cannot contribute sufficiently to enhancing our expertise, since the number of operations is limited, they are not time-constrained, and they work with significant human involvement. Thus at this stage there is a need for more field trials with a heterogeneous sample population (not just frequent flyers). On the basis of such field trials, the actual running costs would also become much clearer and thus could provide sufficient data to allow a realistic cost-benefit analysis.

# ANNEXES

## *Table of Contents (Annexes)*

# ANNEX 1: SELECTED TECHNOLOGIES IN DETAIL

## *A.1 Face recognition*

The face is an obvious choice for a biometric as it is the physiological characteristic used everyday by humans in order to identify others. Face recognition is considered less invasive than other biometrics and has a higher level of user acceptance. However it is also more challenging technologically and face recognition has lower accuracy rates than other biometric modalities such as iris or fingerprint recognition. Having been chosen by the ICAO as the primary biometric identifier for travel documents, face recognition is guaranteed a wide level of implementation in the future.

### A.1.1 What is face recognition?

Face recognition refers to an automated or semi-automated process of matching facial images. The image of the face is captured using a scanner and then analysed in order to obtain a biometric "signature"; different algorithms can be used for this and manufacturers have adopted various proprietary solutions[82] (OECD, 2004). A step-by-step outline of this procedure is provided below.

Different types of face recognition

The term, face recognition, is used as though it refers to a single type of technology but in fact it constitutes a heterogeneous group of technologies which all work with the face but use different scanning techniques. Most common by far is 2D face recognition, using images captured by a standard camera. 2D face recognition is easier and less expensive compared to other approaches, but the technical challenges are greater (systems cope badly with variations in face orientation and lighting conditions) leading to lower accuracy rates. Research has also been carried out using 3D images resulting in reduced sensitivity to factors such as makeup and changes in illumination but with the disadvantage that the scanners are more expensive and the 3D images are not backwards-compatible with existing photo databases. An alternative approach is to use infra-red (IR) radiation to scan facial heat patterns though this is not a prime area of research.

### A.1.2 How does it work

There are four steps in face recognition. Steps a) and b) constitute the enrolment procedure. The information is then stored either in a centralised database or on a distributed storage medium such as a smart card. For identification or verification, steps a) and b) must be repeated followed by steps c) and d).

**a) Acquiring a sample**

The first step is generic for all biometric technologies; it consists of a sensor taking an observation. In the case of 2D face recognition, the sensor is a camera and the observation is a photograph or series of photographs. This acquisition can be

[82] For further details of different techniques and algorithms, see also http://www.biometrics.org

accomplished by digitally scanning an existing photograph or by taking a photograph of a live subject. As video is a rapid sequence of individual still images, it can also be used as a source of facial images, though at present the standard of image quality makes this less suitable.

**b) Extracting Features**
The generic second step is to extract the relevant data from the captured sample. For face recognition there is the added difficulty that first the face has to be located within the acquired image. This can either be done manually by marking the location of the eyes or through the use of software. Once this has been accomplished, the features of the face can be extracted. Algorithms used for this process are mostly proprietary and will depend on the manufacturer. The outcome is a biometric template, which is a reduced set of data that represents the unique features of the enrolled user's face.

**c) Comparing templates**
The nature of the third step will depend on the application at hand. For identification purposes, this step will be a comparison between the biometric template captured from the subject at that moment and all the biometric templates stored on a database. For verification, the biometric template of the claimed identity will be retrieved (either from a database or a storage medium presented by the subject) and this will be compared to the biometric data captured at that moment.

**d) Declaring a match**
The face recognition system will either return a match or a candidate list of potential matches. In the second case, the intervention of a human operator will be required in order to select the best fit from the candidate list. An illustrative analogy is that of a walk-through metal detector, where if a person causes the detector to beep, a human operator steps in and checks the person manually or with a hand-held detector.[83]

### A.1.3 Technology – state of development

The first prototypes for face recognition systems were developed in the early 1990s. In 1993, the US Department of Defense set up the FERET (FacE REcognition Technology) programme, to evaluate algorithms and sponsor research in face recognition[84]. When the programme ended in 1997, face recognition systems were just prototypes in universities and research labs; by the end of the decade 24 systems were commercially available[85].

The most comprehensive independent evaluation of commercial face recognition systems to date is FRVT 2002 (Face Recognition Vendor Test), sponsored by six US government bodies and supported internationally by the UK Biometric Working Group, the Australian Customs Service and the Canadian Passport Office.

[83] National Institute of Justice 2003, see http://www.nlectc.org/training/cxtech2004/2004CXTech_NIJ_Biometrics.pdf
[84] For further details on FERET, see http://www.frvt.org/FERET/default.htm
[85] Source: http://www.frvt.org/DLs/FRVT_2000.pdf

Ten manufacturers took part in the test and comprehensive results are available in the FRVT 2002 report[86].

Prior to presenting a summary of results, it should be noted that more than two years have elapsed since the completion of FRVT 2002 and in the intervening time period, there has been great interest and investment in face recognition. FRGC (Face Recognition Grand Challenge), launched in May 2004 and directed by the US National Institute of Standards and Technology, aims to improve performance in face recognition by an order of magnitude. The next independent evaluation, FRVT 2005 is planned for August/September 2005 and it will determine whether the objective of this challenge has been achieved[87].

FRVT 2002 tested system performance in verification, identification and watchlist experiments. It took into account some demographic factors (sex, age and the interaction between the two) but did not consider ethnicity[88]. The table below offers the main results. A comparison of face recognition performance against other biometric technologies is available in section 2.9.

**Face recognition results from FRVT 2002 report.**

For verification under indoor conditions, the best-performing systems had an error rate of 10% at a false accept rate (FAR) of 1%. At an FAR of 0.1%, the top two systems had error rates of 18%. Under outdoor conditions, performance is still very low, with an error rate of 50% at an FAR of 1%.

Identification and watch-list tasks are both much harder than verification and accordingly performance suffers. In the watch-list task for example, the detection and identification rate was 77% for a watch-list of 25 people and 56% for a watch-list of 3000, both at FAR of 1%.

FRVT 2002 looked at effect of database size on performance and found that identification performance decreases linearly with respect to the logarithm of the database size; a similar effect is seen with watch-list size.

Systems struggled with non-frontal facial images, but performance was improved by use of morphable models to pre-process the image. This holds promise for developing systems that can deal with subjects when they are off-centre.

The study found two primary effects of demographics on performance. First, face recognition systems perform better on male subjects than on female ones (the difference on the identification task was 6-9%). Second, recognition rates for older people were higher than those for younger people. For each additional year of a subject's age, performance improves on average by approximately 5% points. In contrast, performance drops by an approximate 5% points for each year of the time interval between acquisition of the image and testing.

Based on the results shown in the text box above, face recognition is clearly not yet a mature technology. Its performance ranks far below iris and fingerprint systems.

[86] http://www.frvt.org/FRVT2002/documents.htm
[87] For further details, see http://www.frvt.org/FRGC/
[88] Images were provided from the US Department of State's Mexican non-immigrant Visa archive.

Though the best performing systems are not significantly affected by normal changes in indoor lighting conditions, face recognition is not yet suitable for outdoor use. It is unsuitable for large databases and large watch-lists, and even for moderately-sized lists has a mediocre performance on these tasks. Accuracy drops when the acquisition and test are separated by a longer time period, suggesting faces may need regular re-enrolment. Demographic factors have a large effect on performance and this is an important consideration for applications where everyone will be expected to participate.

### A.1.4 Challenges and limitations

*Seven pillars*

This section evaluates face recognition in each of these seven pillars (section 1.2), drawing attention to some of the challenges for face recognition. In brief, face recognition does well in the areas of universality, collectability and acceptability but struggles with distinctiveness, permanence, performance. Resistance to circumvention depends on the application.

*Universality - All human beings are endowed with these physical characteristics:* Face is one of the few biometrics that can claim to be truly universal and certainly the only physical characteristic with this property. This is important because it means that no-one is automatically excluded from being able to provide this biometric.

*Distinctiveness - For each person these characteristics are unique:* With the exception of identical twins, faces are distinct enough such that under normal conditions, humans are always able to identify the faces of people they know. Computationally however, discriminating between faces is a demanding task as faces share many similarities and all tend to be characterized by the same features: two eyes, a nose and a mouth. This is in contrast to irises or fingerprints where pattern variation is vastly greater. Identical twins pose a particular problem for face recognition and though there are systems which claim to be able to discriminate between the two, no independent study has been conducted yet to test performance on twins.

*Permanence - These characteristics remain largely unchanged throughout a person's life:* Faces change markedly with time and test data for face recognition technologies show that this problem has not yet been surmounted. FRVT 2002 results show a drop in accuracy of 5% points per year.[89] This implies that if subjects were tested against facial images captured eight years ago, the error rate would be 50% (at an FTA of 1%). Clearly face recognition will need to improve if it is to be incorporated into passports that are valid for ten years. Faces can also change due to a host of other factors including extreme weight gain or loss, injury and plastic surgery. It is likely that under such circumstances, users will need to re-enrol with the system.

*Collectability - The characteristics need to be collected in reasonably easy fashion:* Face recognition performs particularly well in this category. The hardware for most

[89] http://www.frvt.org/FRVT2002/documents.htm

types of face recognition is a high-resolution optical camera and, as described in section 2.4.1 above, the individual enrolling or being identified just has a photograph taken. The ease of taking a photograph combined with the face's universality, give face recognition low FTE (failure to enrol) and FTA (failure to acquire) rates.

*Performance - The accuracy of identification/verification:* The conclusion that arises from the figures is that accuracy, particularly under varying environmental conditions, is currently the greatest challenge for face recognition.

*Acceptability - The degree to which there is public acceptance of the technology:* It is customary to have a photograph taken for applications in the public and private sector and the process is widely accepted. From the user's point of view a face recognition system is simply a camera that takes a photograph, so the technology is viewed as non-invasive and has a high level of user acceptance. There are religious considerations to take into account with regard to showing the face. These however exist for all identity documents and procedures, and are not specific to face recognition. It is worth noting that if women are required to remove veils or headscarves, a face recognition system will have to be set up in a separate area staffed by female employees. There are also issues of acceptability with some specific applications of face recognition and these are discussed further in section 2.4.5 below.

*Resistance to circumvention – Is the technology significantly more difficult for criminals to circumvent?*
The resistance to circumvention depends on the task. For verification tasks, in order to have an acceptable FRR, FAR is usually set at 1%, a much higher level than is customary (iris and fingerprint systems usually set FAR at 0.1%). This implies 1 that out of every 100 people that try to fool the system, on average 1 could get through. Lower false-accept rates are possible, e.g. 0.1% or 0.01%, but they result in a very high FRR.

For identification and watch-list tasks, performance is worse so security is lower. Watch-list tasks in particular have the added difficulty that people who are on the watch-list may take measures to avoid identification by keeping their face obscured.

*Interoperability[90] – a further consideration for open systems*
Face recognition is a recent technology and research is being carried out in many different fields so there is by no means uniformity in terms of approach. Even within 2D face recognition, different manufacturers use fundamentally different algorithms and this makes interoperability a particular challenge. The biometric template for a face used by one manufacturer will be of no use to a system running software from a different manufacturer and so the only way to ensure interoperability is to store the raw facial image and not the template. The ICAO

[90] Interoperability is only an issue for open systems such as passports, where one stored biometric is presented at many different points. (The passport for example has to be readable at any border point worldwide).

sums it up thus, "Anything less than storage of images would be a proprietary solution selecting one (or a select few) vendors' solutions."[91]

*Face recognition and privacy*

Many privacy implications are common to all biometric modalities but there are a couple of issues specific to face recognition that need to be discussed further: the capability for covert capture and the fear of surveillance.

*Covert capture*

Face recognition differs to other biometric modalities in that the cooperation of the subject is not necessary. In the case of 2D face recognition for example, all that is required is a photographic image of the face, which can be captured quite easily with a hidden camera. This may lead to both real and imagined privacy concerns. In 2001, the Tampa Bay Police used face recognition technology to screen the spectators that attended the Super Bowl game against a watch-list of known felons. Part of the outrage that followed, derived from the fact that spectators were unaware the technology was in use[92]. The result was a negative public perception and a misunderstanding of how the technology was being used; people felt they were being identified even though they were anonymously being screened against the watch-list (Bowyer, 2003).

*Surveillance fears*

Face recognition can potentially function without any special effort on the part of the user. As the technology improves, it could become feasible to screen or identify large numbers of people. This could occur covertly or overtly. Current performance levels of face recognition limit the capabilities of a large-scale surveillance system. It is perfectly plausible though that in the future, face recognition will achieve much better accuracy under varying environmental conditions. Such an improvement coupled with advances in computer vision could potentially enable an automated system to identify everybody in a crowd using a photograph captured at a long distance. This situation is clearly hypothetical but worth considering if one is to take a prospective view.

*Face recognition and data protection*

The proposed Council Regulation on standards for security features and biometrics in travel documents states in the explanatory memorandum that, "Directive 95/46/EC on data protection applies to the processing of personal data –including biometric data- by Member States' authorities within the scope of Community law."[93] It is straightforward to see how most biometric data can be protected by this directive. A fingerprint scan will result in fingerprint pattern data which will be processed following the same rules applicable to other personal data.

[91] ICAO Technical Report http://www.icao.int/mrtd/download/technical.cfm

[92] For press coverage see http://news.bbc.co.uk/1/hi/sci/tech/1500017.stm ; "Welcome to the snooper bowl," *Time*, Feb 12, 2001; "Electronic surveillance: From 'Big Brother' Fears To Safety Tool," *New York Times*, Dec 6, 2001

[93] P.8, Council Regulation on standards for security features and biometrics in EU citizens' passports, COM (2004) 116, 2004/0039 (CNS)

The case of facial data is less clear. Nearly everyone shows their face in public every day of their life; the data are thus arguably in the public domain. In the US, the Supreme Court has ruled that a person does not have a reasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public, such as one's facial features, voice, and handwriting (Woodward, 1973). The ruling dates back to 1973, but it is frequently cited in the ongoing debate on biometrics and privacy concerns.

Though it has always been possible to identify someone by their face (it is after all how we identify our acquaintances in everyday life), face recognition presents the possibility for this process to be automated and to be implemented on a much greater scale. The question is: how can the biometric data of the face be protected? Is it plausible to expect this "data" to be kept private when we reveal it every day? These questions differentiate facial data from other biometric data.

### A.1.5 Applications

The previous section outlined certain attributes of face recognition not shared with the main other biometric technologies. They make face recognition suitable for surveillance, large-scale screening and applications where identification occurs without effort from the subject. On the other hand the relatively low level of accuracy limits such applications at present. This section describes some of the existing and planned face recognition applications.

*Machine Readable Travel Documents (MRTDs)*
The most important development for face recognition is the introduction of the face as the primary biometric on MRTDs. The ICAO's reasons for recommending the face highlight the benefits of the technology (ICAO-TAG, 2004).

- Facial photographs do not disclose information that the person does not routinely disclose to the general public
- The photograph (facial image) is already socially and culturally accepted internationally
- It is already collected and verified routinely as part of the MRTD application form process in order to produce a passport to ICAO Document 9303 standards
- The public are already aware of its capture and use for identity verification purposes
- It is non-intrusive – the user does not have to touch or interact with a physical device for a substantial timeframe to be enrolled.
- It does not require new and costly enrolment procedures to be introduced
- Capture of it can be deployed relatively immediately and the opportunity to capture face retrospectively is also available
- Many States have a legacy database of facial images captured as part of the digitised production of passport photographs which can be encoded into facial templates and verified against for identity comparison purposes
- It can be captured from an endorsed photograph, not requiring the person to be physically present

- It allows capture of children's biometrics without the children having to be present
- For watch lists, face (photograph) is generally the only biometric available for comparison
- It always acquires
- Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities

The European Parliament has now voted in favour of introducing biometrics on MRTDs and it is foreseen that this application will be implemented within the next few years.

*Existing face recognition applications*

One application that has already been mentioned is the use of face recognition to screen spectators at the 2001 Super Bowl. A borough of London was one of the first areas to introduce face recognition in 1998, in order to screen images from closed circuit television cameras (CCTV) for targeted offenders[94]. Face recognition has also been tested in airports around the world, including Keflavik Airport Reykjavik[95], Logan Airport Boston[96], Palm Beach International Airport Florida[97], and Sydney Airport[98] with mixed results.

*Law enforcement*

Face recognition offers certain facilities not available with other biometric technologies. One feature that appeals in particular to law enforcement agencies is the option of matching witness descriptions or artist-rendered images to databases of suspects, i.e. the capacity to compare biometric data with non-biometric data within the same system. Though the results are not precise enough to be admissible as evidence, they can provide the police with leads for further investigation.[99]

*Database mining*

One of the touted advantages of face recognition technology is that it is compatible with existing databases of facial images. Many countries have databases of passport photographs, driver's license photographs, mug shots, etc., and face recognition could be used to mine existing databases, checking for duplicates and multiple identities.

[94] http://www.guardian.co.uk/g2/story/0,3604,736312,00.html
[95] Keflavik Airport, Iceland, http://archives.cnn.com/2001/US/09/28/rec.airport.facial.screening/
[96] Logan Airport http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan/,
[97] Palm Beach http://www.usatoday.com/tech/news/2002/05/16/airport-face-recognition.htm
[98] Sydney http://www.ag.gov.au/agd/www/justiceministerhome.nsf/Web+Pages/106BCD218A512F16CA256CBD001160A9?OpenDocument
[99] http://www.fcw.com/geb/articles/2002/0311/web-face-03-04-02.asp

### A.1.6 Future trends

It is safe to predict that as face recognition technology matures, performance will improve. Currently face recognition systems work under constrained environmental conditions. One of the most important steps will be to achieve good performance under natural conditions, such as outdoor environments, changing poses, varying expressions, etc. It is equally important to be able to work with low-quality images, as in law enforcement frequently these are the only types of images available. Presently there are three developments that promise progress in face recognition: high resolution images, 3D face recognition, and new preprocessing techniques. FRVT 2005, the next large independent evaluation of face recognition, will look in detail at all three.[100]

As performance improves, the prospective applications discussed in the previous section, will become viable. Face recognition could be incorporated seamlessly into an automated welcoming service, for example, greeting frequent customers by name without any effort necessary on the part of the customer. It could be used in childcare facilities in order to monitor behaviour. It could further be combined with voice recognition to produce wearable systems that help users recognise others (Choudhury et al., 1999).

Further into the future, face recognition is likely to expand beyond the confines of identity and verification tasks. Choudhury (2000)[101] suggests that distinguishing facial expressions will become increasingly important for 'smart systems' which can dynamically interact with users. For example by recognising the user's expression, a system could present information faster if the user looks impatient or slower if the expression is confused. By identifying the user, the smart system can customise its performance to fit the user's preferences.

[100] http://www.frvt.org/FRVT2005/default.aspx
[101] Source: http://vismod.media.mit.edu/tech-reports/TR-516/node10.html

## *A.2 Fingerprint recognition*

Fingerprints have been found on potteries and cave paintings from thousands of years ago suggesting that the use of fingerprints to identify an individual dates back to ancient times. But the idea that no two individuals have the same fingerprints and that fingerprints patterns do not change significantly throughout life became accepted during the course of the 19th century. This gave rise to the law enforcement practice of using fingerprints for the identification of criminals. As a result, a criminal found it harder to deny his/her identity while innocent people were less likely to be wrongly identified as criminals. Moreover, by comparing fingerprints at a crime scene with the fingerprint record of suspected persons, proof of presence could be established.[102]

Fingerprint matching however could only be done by highly trained and skilled people. Demands for fingerprint matching from law enforcement authorities began to outpace the laborious manual and visual approach to fingerprint indexing, searching and matching. The advent of computing power led to the development of 'Automatic Fingerprint Identification Systems' (AFIS). These systems have greatly improved the operational productivity of law enforcement agencies and reduced the cost of hiring and training human fingerprint experts. The rapid growth of automatic fingerprint recognition technology for forensic use has paved the way for the application of fingerprint technology in other (civilian) domains. Fingerprint-based biometric systems have almost become synonymous with biometric systems as a whole (Maltoni et al., 2003). In 2004, fingerprint systems accounted for almost 50% of the biometrics market. [103] Other biometric technologies may gain in popularity but the use of fingerprint still remains the oldest method of computer-aided personal identification (O'Gorman, 1999).

### A.2.1 What is fingerprint recognition?

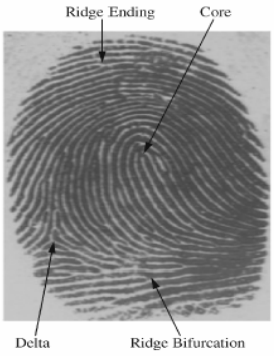
Fingerprint recognition consists of comparing a print of the characteristics of a fingertip or a template of that print with a stored template or print. Fingerprints become fully formed in the seventh month of foetus development and they do not develop further throughout the life of an individual (though injury or skin conditions may cause changes). Not only are the fingerprints of different people different, there are so many variations during the formation of fingerprints that it would be virtually impossible for two fingerprints to be exactly alike. Fingerprints from different fingers of the same individual are not entirely unrelated as they originate from the same genes. This means for instance, that the fingerprints of identical twins are said to be similar but not identical. Under good conditions and with state of the art technology, it seems that automatic fingerprint recognition is able to distinguish identical twins but with a slightly lower accuracy than for non-twins. It is important to note that the uniqueness of fingerprints is not an

[102] There is however, controversy on how "scientific" forensic identification techniques are: See for instance (Cole, 1998).
[103] International Biometric Group's (IBG's): T*he Biometrics Market and Industry Report 2004-2008.* http://www.biometricgroup.com

established physiological fact but rather an empirical observation. Fingerprint formations are well studied, but the debate on the real uniqueness of fingerprints, on the contrary, is not completely resolved (Jain et al., 2002).

### A.2.2 How does it work?

A fingerprint consists of the features and details of a fingertip. There are three major fingerprint features: the arch, loop and whorl. Each finger has at least one major feature. Loops are lines that enter and exit on the same side of the print. Arches are lines that start on one side of the print, rise into hills and then exit on the other side of the print. Whorls are circles that do not exit on either side of the print. The smaller or minor features (or minutiae) consist of the position of ridge ends (ridges are the lines that flow in various patterns across fingerprints) and of ridge bifurcations (the point where ridges split in two). There are between 50 and 200 such minor features on every finger (OECD, 2004: 21). Fingerprint matching done on the basis of the three major features is called pattern matching while the more microscopic approach is called minutiae matching. Other features may be used for matching, but patterns and minutiae are the main ones (O'Gorman, 1999: 45-46).




Minutiae of a fingerprint[104]

**a) Acquire a sample**

A fingerprint image can be captured voluntarily and/or consciously (i.e. with the person consent and/or knowledge) but also involuntarily or unconsciously. The latter typically occurs at the scene of crime where available fingerprints are investigated. People leave fingerprint trails on almost every surface they touch via the oil that coats the ridges of their print. The residue that is left behind is known as a latent fingerprint. For these to be used for identification or verification, they first need to be enhanced, for instance with special powders and brushes, and for matching they need to be photographed or lifted and placed on a fingerprint card (Sandström, 2004).

Enrolment and acquisition can furthermore be done off-line or with a live-sensor. An off-line image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on a paper (or fingerprint card). This is the oldest and best known acquisition technique that is still used by law

[104] Image Source: Dorizzi, Bernadette; Technological impacts of biometrics; Jan.05

enforcement and other government agencies worldwide. Before the age of digitalization, these finger print cards were then copied and sent to a centralized national identification office where all cards were stored and where matching takes place. Such a process is quite laborious and time-consuming. According to the US Federal Bureau of Investigation (FBI), a fingerprint check under this system would take usually three months to complete.[105]

The off-line mode has been advanced during the last decade via digitization. The fingerprint cards are now scanned digitally, allowing the image data to be stored in databases and also to be transferred via communication networks. This process is of course much faster compared to the physical fingerprint cards. In the US, responses to criminal ten-print fingerprint submissions done electronically are now possible within two hours. Civil fingerprint submissions are done within 24 hours.[106]

Live-acquisition, on the other hand, is done by sensors reading the tip of the finger directly and in real-time. A fingerprint scan contains a lot of information but scanners normally focus only on getting an image of the information that is essential for matching. The quality of the sensed fingerprint image is of key importance for the performance of the system. Given the small area of the fingertip, its detailed minutiae and its continuous use in everyday life (e.g. cuts, bruises, aging, weather conditions), poor image quality is a major concern in fingerprint applications. During the last years, fingerprint scanners have considerably improved their performance and at the same time have become smaller and cheaper. This has enabled the deployment of fingerprint authentication beyond law enforcement applications. Fingerprint scanners are now being integrated in electronic devices such as a laptop, a keyboard, a mouse and a PDA (Xia et al., 2002)[107].

There are three types of live scanners: (1) optical devices using a light source and lens to capture the fingerprint with a camera; (2) solid-state sensors or silicon sensors appearing on the market in the mid-1990s to address the shortcomings of the early optical sensors[108]; (3) and others, such as acoustic sensors that use acoustic signals to detect fingerprint details. Upcoming solid-state sensors are swiping sensors comparable to for instance swiping a credit card (Xia et al., 2002).

[105] http://www.fbi.gov/hq/cjisd/iafis.htm
[106] http://www.fbi.gov/hq/cjisd/iafis.htm
[107] Some examples: Biometric IBM Thinkpad T42 9 (Laptop launched in October 2004): http://www.pc.ibm.com/us/thinkpad/tseries/index.html; MS keybord/mouse with FP reader: http://www.microsoft.com/hardware/mouseandkeyboard/productdetails.aspx?pid=034; PDA with FP reader: http://www.hp.com; stand-alone USB based FP reader: Targus DEFCON Authenticator™: http://www.targus.com ;.
[108] Shortcomings are mainly size and cost. The chip sensors comprise an array of sensing elements (each pixel is a sensor) that image the fingerprint. Solid-state sensors have on-chip conversion (analogue to digital) so that a digital image can be generated. There are mainly two types of solid-state sensors. Capacitive sensors are most prevalent and use electric field strengths for distant measurement of fingerprint ridges and valleys. Temperature sensors measure the temperature difference of a finger between the skin ridges and the air (valleys).

Important factors to describe and compare fingerprint capture devices are cost, size and performance (e.g. image resolution, bit depth, capture area, etc.) but also their accompanying (usually proprietary) software containing the matching algorithms. There are standard requirements related to performance established by the FBI (e.g. resolution 500 dots per inch; pixel depth 8 bit). Commercial devices sometimes meet some of these requirements but usually tradeoffs have to be made, especially between size and cost. Although solid-state sensors are currently small enough to be embedded in existing electronic devices (and even current optical sensors), another important trade-off is the one between size and accuracy (both FAR and FRR): the smaller the finger print area rate, the worse the recognition rate (with the exception of "swiping sensors") (Xia et al., 2002).

**b) Extracting features**

Getting a high quality image of the fingerprint is very important for accurate fingerprint recognition but also feature extraction plays a crucial role. It consists of converting the fingerprint image into a usable and comparable format that does not require lots of storage space. The format or template is a compressed version of the fingerprint characteristics. Several approaches to automatic minutiae extraction exist, but most of these methods transform fingerprint images into binary images. This means that only the coordinates of the minutiae (30 or 40) are stored, reducing it to a few hundreds of bytes (Mainguet et al., 2000; OECD, 2004: 21). This is considerable less compared to 10 Mbytes of storage per person needed for a 500 dpi image at 8 bits (FBI requirements) for all 10 fingers. Central fingerprint databases would thus require terabits of storage (Maltoni et al., 2003: 27).

Feature extraction is also needed because even a very precise fingerprint image will have distortions and false minutiae that need to be filtered out. For example, an algorithm may search the image and eliminate one of two adjacent minutiae, as minutiae are very rarely adjacent. Anomalies can also be caused by scars, sweat, or dirt. The algorithms used for feature extraction filter the image to eliminate the distortions and would-be minutiae.[109]

**c) Comparing Templates**

The identification or verification process follows the same steps as the enrolment process with the addition of matching. It compares the template of the live image with a database of enrolled templates (identification), or with a single enrolled template (authentication).

**d) Declaring a Match**

The comparison between the sensed fingerprint image or template against records in a database or a chip usually yields a matching score quantifying the similarity between the two representations. If the score is higher than a certain threshold, a match is declared, i.e. belonging to the same finger(s). The decision of a match or non-match can be automated but it depends also on whether matching is done for identification or verification purposes.

[109] http://www.biometricgroup.com/reports/public/reports/finger-scan_extraction.html

With identification applications, automated decision-making is possible when conditions are ideal. In the case of the FBI for instance, this means that fingerprint cards can be matched automatically when both enrolment and acquisition were done by law enforcement staff. But with latent prints (e.g. collected at a crime scene) and prints with a lower quality image, the automated process is less reliable. Automated systems imitate the way human fingerprint expert work but the problem is that these systems can not have observed the many underlying information-rich features an expert is able to detect visually. Automatic systems are however, reliable, rapid, consistent and cost effective when matching conditions are good, but their level of sophistication can not rival that of a well-trained fingerprint expert. Therefore, for instance a fingerprint expert can overrule an automated match (Jain et al., 2001: 23&56)

Verification applications, especially mainstream commercial fingerprint verification may be, to a certain extent, less accurate because the issues at stake are different (e.g. identifying criminals) but also because verification consists of 1-1 matching. Verification may use less information from a fingerprint compared to forensic scientists identifying a fingerprint. The former seems to be more like a possible, "close-enough correlation" of similarities. Also, because of background interference (dirt, scratches, light, etc.) and no human supervision, the quality of fingerprint images is lower. The result is a "best" matching score which would not be feasible for law enforcement[110].

### A.2.3 Technology – state of development

Since fingerprint technology is one of the oldest automated biometric identifiers, supported by strong demand from law enforcement, it has undergone extensive research and development. According to (Maltoni et al., 2003: 2) though, there is a popular misconception that automatic fingerprint recognition technologies are without problems. They believe that fingerprint recognition is still a challenging and important machine pattern recognition problem.

One of these challenges relates to the question of interoperability. Fingerprint recognition normally consists of a closed system that uses the same sensors for enrolment and acquisition, the same algorithms for feature extraction and matching and clear standards for the template and for instance, the enrolment procedure (e.g. FBI standard is nail-to-nail). Take the example of fingerprint sensors. There are many different vendors on the market that have all proprietary feature extraction algorithms that are strongly protected, although there are some (proprietary) sensor independent recognition algorithms on the market.[111] Different sensors using the same technology (e.g. solid state) produce different fingerprint raw image data, in the same way as sensors using different technologies (e.g. optical and solid state) deliver raw images that are significantly different. Sensor interoperability is a problem that hitherto hardly has been studied and addressed, while it will become increasingly important when fingerprint scanners are more and more embedded in

[110] http://onin.com
[111] http://www.biometricgroup.com/reports/public/reports/finger-scan_extraction.html

consumer electronics (Ross et al., 2004). In addition to image data, there is also the issue of interoperability of minutiae data that is being put forward recently.[112]

### A.2.4 Challenges and limitations

*Seven pillars*

Fingerprint recognition has a good balance related to the so-called seven pillars of biometrics. Nearly every human being possesses fingerprints (*universality*) with the exception of hand-related disabilities. Fingerprints are also *distinctive* and the fingerprint details are *permanent*, although they may temporarily change due to cuts and bruises on the skin or external conditions (e.g. wet fingers). Live-scan fingerprint sensors can capture high-quality images (*collectability*). The deployed fingerprint-based biometric systems offer good *performance* and fingerprint sensors have become quite small and affordable. Fingerprints have a stigma of criminality associated with them but that is changing with the increased demand of automatic recognition and authentication in a digitally interconnected society (*acceptability*). By combining the use of multiple fingers, cryptographic techniques and liveness detection, fingerprint systems are becoming quite difficult to *circumvent*. (Maltoni et al., 2003: 11)

When only one finger is used however, universal access and permanent availability may be problematic. Moreover, everyday life conditions can also cause deformations of the fingerprint, for instance as a result of doing manual work or playing an instrument. Certain conditions, such as arthritis, affect the ease of use of fingerprint readers. Other conditions such as eczema, may affect the fingerprint itself. It is estimated that circa five per cent of people would not be able to register and deliver a readable fingerprint. With large scale applications which entail millions of people, an estimated five per cent of people being temporarily or permanently unable to register amounts to a significant number. This will not only lead to serious delays (decrease in task performance) or annoyance (decrease in user satisfaction), but also makes fingerprinting not fully universally accessible (Sasse, 2004: 7).

*Security*

The security of the fingerprint recognition system as such is dependent on two main areas: electronic security and liveness testing. Electronic security has to do with traditional digital security issues and is tackled with for instance encryption and other techniques to make it difficult to capture fingerprint information when being transmitted. For verification applications, one of the most secure systems, it is being argued, consists of having the full system on a smart card (template, sensor, feature extraction and matching). The output would than be a simple yes or no, or an encrypted message (Mainguet et al., 2000). Such a decentralised system – it is expected to become possible in the near future – would combine the biometric advantage of strong authentication with the user being in full control and without the biometrics privacy risks (Maltoni et al., 2003: 47).

[112] In 2004, in the USA, a 'Minutiae Interoperability Exchange Test' (MINEX04) was launched to determine the feasibility of using minutiae data as the interchange medium for matching between dissimilar recognition systems. See http://fingerprint.nist.gov/minex04

Apart from the cases where physical threats and force are used to get someone's fingerprint (or a dead finger), liveness testing also deals with spoofing the system with a fake, artificial fingerprint, taken for example from fingerprint images people leave everywhere (latent fingerprints). There are cases reported that fingerprints were relatively easy to reproduce with gelatine but liveness detection procedures (e.g. 3-dimensional imaging, temperature measuring) are increasingly being integrated in fingerprint readers. It is therefore argued that fingerprint recognition is getting less vulnerable to artificial fingerprints (Mainguet et al. 2000).[113]

*Privacy*

The privacy risks related to fingerprints are mainly the ones that are similar to most biometrics: the risk that unauthorized third parties get access to the biometric data as unique identifiers; the digital traces that biometric identification leave behind and the traditional data protection issues related to storage (central or not), access (who has access ), consent, transparency, etc. There is also the issue of purpose creep or function creep whereby the data collected for one purpose are used for other purposes (OECD, 2004). In addition, specific privacy concerns with fingerprints may come from its use by law enforcement agencies.

### A.2.5 Applications

Fingerprint identification of criminals for law enforcement continues to be one of the major applications domains for this technology. Another large scale application in Europe is EURODAC for asylum requests. In New York, fingerprints are used to prevent fraudulent enrolment for benefits. Using fingerprint recognition to secure physical access is another popular application. Moreover, embedding of fingerprint readers in electronic devices opens up a whole range of digital applications that are based on online authentication. Finally, decisions have been taken for the future integration of fingerprints (with other biometrics) on travel documents and passports.

The Integrated Automated Fingerprint Identification System, more commonly known as IAFIS, is one of the largest biometric database in the world. It is a US national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI). It contains the fingerprints and corresponding criminal history information for more than 47 million subjects in the Criminal Master File. The fingerprints and corresponding criminal history information are submitted voluntarily by state, local, and federal law enforcement agencies. The IAFIS provides automated fingerprint search capabilities, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year.[114] In Europe, there is no such a database. Criminal fingerprint databases are under control of national criminal authorities. The UK for instance, has a national

[113] On artifical fingers, see for instance (Sandström, 2004) and "Gummi bears defeat fingerprint sensors",The Register, 16 May 2002;
http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/

[114] http://www.fbi.gov/hq/cjisd/iafis.htm

automated fingerprint identification system (NAFI) containing more than four million records. A recent collapse of the system was reported in the press.[115]

There is however, since January 2003, also a large central fingerprint database in the European Union, but for another purpose. It aims at preventing duplication of asylum requests in the EU Member states. EURODAC is an EU wide database (AFIS) set up to check the fingerprints of asylum seekers against the records of other EU countries. After one year of operation, an evaluation report on EURODAC highlighted satisfactory results in terms of efficiency, quality of service and cost-effectiveness. The EURODAC central unit has been operating continuously. Within one year, it processed almost 250.000 fingerprints of asylum seekers. It detected 17,287 cases of multiple-application (a same person having already made an asylum application in another country), which represents 7% of the total number of cases processed. In addition to asylum requests, also illegal immigrants are identified. Almost 17,000 fingerprints of people in an illegal situation were detected and about 8000 fingerprints related to attempts to cross borders illegally. The evaluation report also states that there were no data protection problems raised by the Member States' national data protection authorities regarding EURODAC operations.[116]

The state of New York has over 900 000 people enrolled in a system which tracks to entitlement to social services and protects against fraud known as “double dipping”, i.e. enrolling for a benefit under multiple names (OECD, 2004: 23). Fingerprint scanning is also being used to arrange secure access to schools and schools premises such as cafeterias and libraries. Finally, with the embedding of fingerprint scanners in electronic devices, online authentication (replacement of passwords, PINs, etc) becomes possible for a whole range of applications including electronic payments.

Finally, at EU level, the Council of European Ministers adopted the Regulation on mandatory facial images and fingerprints in EU passports at its meeting in Brussels on 13 December 2004. This Regulation applies to passports and travel documents issued by Member States (excluding Ireland, the UK and Denmark). After the Regulation is published in the *Official Journal* passports issued will have to contain a facial image within 18 months, and fingerprints within three years. Also a Committee will be set up by the European Commission with representatives from 22 Member States to decide on the details such as how many fingerprints are to be taken, the equipment needed and the costs.[117]

[115] Fingerprint system crash fuels doubts over ID card scheme, The Independent online, 3.12.2001, on a collapse that happened on November 24, 2004.
[116] EURODAC detects 7% of multiple asylum applications during its first year of activity; Press release by the European Commission, Reference IP/04/581, 05/05/2004, http://europa.eu.int:80/ida/en/document/2528
[117] EU Council Regulation on standards for security features and biometrics in passports, 15152/04, 10 December 2004.

### A.2.6 Future Trends

Fingerprint recognition scores well on the so-called seven pillars of biometrics. The quality of the acquired image, at enrolment, determines to a large extent the accuracy of the fingerprint matching. But also the size of the sensor, its prize and quality and the required threshold for the recognition rate are important factors to be taken into account. They relate to each other, so tradeoffs have to be made. But in general, the theoretical accuracy with fingerprint verification is said to be quite high. Also, the current embedding of fingerprint technology in consumer electronics might help to relief fingerprinting from its criminal connotation.

However, a non-negligible part of the population faces difficulties in being enrolled and verified through fingerprints. For large scale applications, this limiting factor needs to be taken into account. Also fears related to hygiene and to physical attacks to get ones' fingerprints have been reported. Some argue that all this calls for the availability of an alternative, be it a second biometric (e.g. face) or something else.

Fingerprint identification is currently being used in conjunction with large scale central databases for forensic purposes and for asylum requests. Other applications are related to checking entitlements and authorising physical access. But with the emerging trend of embedding fingerprint readers into electronic devices, fingerprint technology is losing its criminal stigma in favour a wide range of online applications that require secure authentication. Decentralised system-on-chip solutions are foreseen to address both privacy and security concerns.

## *A.3 Iris Recognition*

### A.3.1 What is Iris Recognition?

The iris is the externally-visible, coloured ring around the pupil. It is a physical feature of a human being that can be measured and thus used for biometric verification or identification through the process of iris recognition. The human iris is well protected as although it is externally visible, it is an internal part of the eye. It is not genetically determined (which means that genetically identical eyes, e.g. the right and left eye of any given individual, have unrelated iris patterns) and it is believed to be stable throughout life (barring accidents and surgical operations). Iris patterns are both highly complex and unique (the chance of two irises being identical is estimated at 1 in $10^{78}$)[118] making them very well-suited for biometric identification.

### A.3.2 How does it work

An iris 'scan' is a photograph of the iris taken under near-infrared (near-IR) illumination.[119] Though visible light can also be used to illuminate the eye, darkly pigmented irises reveal more pattern complexity under near-IR light. Iris recognition systems generally use narrow-angle cameras and ask the user to position their eyes correctly in the camera's field of view. The resulting photograph is analysed using algorithms to locate the iris and extract feature information, in order to create a biometric template or 'IrisCode'.

**a) Acquire Sample**

The image of the iris is captured from a distance of 10-20cm (non-invasively) by a high-resolution camera which first focuses appropriately given the distance of the target, discounts reflections from glasses and acquires a digital photo of the iris.

Variations in pupil size do not interfere with the randomness or uniqueness of iris patterns. Moreover, natural variations can be used as a means to confirm that the iris scanned is a real one. Other characteristics of the eye may render scanning difficult: for example the iris is often obscured by the eyelids (which may droop due to ageing or other factors), the eyelashes, lenses and eyeglasses. Furthermore, even in the absence of these obstacles, the whole process of acquiring an image of the iris for recognition purposes requires high-precision cameras since the iris is a relatively small (~1 cm), moving target, located behind a curved, wet, reflecting surface. Two more points to consider here are (a) using near infrared wavelength cameras as in this wavelength even dark brown coloured irises reveal their patterns well while with visible light cameras the result would have been dependent on the iris colour, and (b) user acceptance seems to be lower than with other biometrics as users feel a sense of discomfort during the enrolment process mainly due to the fact that it is not clear where to focus.

[118] Daugman (2004)

[119] Near-IR wavelengths lie just beyond visible red light on the electromagnetic spectrum.

**b) Extracting Features**
The first task in feature extraction is to determine the location of the iris in the picture. This is done by localising the iris, pupil and both eyelid boundaries, excluding pupil and eyelashes from the photo and thus creating an iris mapping that is invariant to size, distance, magnification and pupil dilation. The next step involves creating the IrisCode (a high number – up to 2048 – of bit probabilities) through the use of proprietary algorithms which is ultimately stored in a template (256 bytes for the IrisCode itself + 256 bytes for masking bits). This then allows local or remote storing in centralised databases or portable media (smart cards, tokens). As will be explained later the template may contain less information (surprisingly up to 80% less) without significantly deteriorating the statistical process of the decision making.

**c) Comparing Templates**
Both verification (1:1) or identification (1:N) modes, involve taking a live photograph of the iris to be matched, and comparing the resultant IrisCode against the stored template (1:1 verification) or with N IrisCodes registered in a database (1:N identification). The matching is done through bit-to-bit comparison (logical exclusive OR operator) which is a very fast method of calculating the so-called average Hamming distance between the two IrisCodes compared[120]. There are other methods of measuring the correlations between two iris images but they are still under development.

**d) Declaring a match**
As is the case with all biometric systems, the matching process produces a score that is then forwarded to the decision process which compares the specific score to a decision threshold that may be adjusted to the application. In the case of iris recognition the threshold may be easily computed in such a way so as to allow 0 false matches almost independent of the number of entries in the database (in identification mode) and also ensuring minimal genuine false non-matches.

### A.3.3 Technology – state of development

The technology is mature enough to be used commercially although all the relevant patents belong to one company (Iridian) which may prove to be a problem for further innovation in the field. However, there is ongoing research (mainly in Asia) on alternative methods and the original patents will expire within the next 5-10 years.

The system works well in identification mode and requires less frequent re-enrolment compared to other technologies, making it ideal for large-scale identification. It may thus be attractive for government applications (electronic identity, border-control). It is also extremely efficient in verification applications (physical access control, time and attendance control) and due to convergence, it

[120] Developed by J. Daugman: US Patent 4,641,349 held by IRIDIAN Technologies, Inc

may find its way into point-of-sale and wireless and mobile applications once cost effectiveness of the wireless devices has been enhanced.

All iris recognition systems worldwide today deploy algorithms developed by Daugman. Current commercial iris scanning systems are relatively fast, flexible (in terms of operational conditions) and very efficient. They may operate at a range of about 10-20 cm although there exist research systems that operate at the extreme range of 5m. Verification time can be very fast; for example the time needed to search a database of 1 million IrisCodes on a 2.2 GHz PC would be approximately 1.7 seconds.

*Market specifics*

Anti-terrorist initiatives mean that strengthening security at borders and airports is a primary target. Iris recognition is used at several airports, either for purely security reasons, or a combination of security and convenience, e.g. Schiphol airport, NL where registered passengers are able to use the iris recognition system upon arrival at immigration control and thus bypass queues. The market growth prompted by the introduction of biometrics onto travel documents is likely to have less of an effect on iris recognition, as the face will be the primary biometric identifier and the EU has chosen the fingerprint as the second biometric. Iridian (which owns the core iris technology patents) is currently the market leader in iris recognition, followed by LG and OKI. These companies provide access control solutions that at present account for 2% of the biometric market and are forecasted to reach 12% by the year 2008[121]. Due to high costs and low user acceptance, the technology remains a niche solution for wider business.

### A.3.4 Challenges and limitations

*Seven Pillars*

Iris recognition performs very well against the so-called 7 pillars. All humans (including blind people) possess irises (*universality*) with some exceptions (e.g. aniridia, which is the absence of an iris). Iris patterns are *distinctive* and there is a scientific explanation for this. The patterns are also *permanent* from infancy to old age with the exception of the effects of some eye diseases. Existing sensors (high-resolution near-IR cameras) can capture good quality images (*collectability*) although several trials may be necessary. The iris recognition system offers excellent *performance* even in identification mode with huge databases of enrolled users; however, the necessary infrastructure is still costly. The *acceptability* of iris recognition is relatively low. Finally, while the first systems were easy to fool with a picture of an iris placed at the appropriate distance, new systems are more expensive but quite difficult to *circumvent*.

*Challenges specific to the technology*

Calculation of an IrisCode can be done in under 10 ms and enrolment in general takes 2-3 minutes. However, enrolment in an iris system can be less than

[121] forecast by IBG, 2004 report http://www.biometricgroup.com/reports/public/market_report.html

straightforward as the eye must be properly positioned and focused (it is said that this creates a sense of discomfort). The enrolment process is not invasive though as the eye does not have to touch a surface or be subject to intense illumination (as is the case for a retina scan). Iris recognition uses near-IR illumination as this gives better results for brown eyes (which is the most dominant colour on earth). There is no evidence to suggest this illumination causes any damage to eyes, however this would have to be corroborated by independent studies.

Another likely problem in the use of iris recognition is an unfocused eye image[122] that increases noise in the calculation of the IrisCode. On the other hand this enrolment inconvenience also means that this biometric technology is unlikely to be used to survey subjects without their consent. The outlier group size for enrolling to this biometric technology is small (most people have at least one eye). Blind people are able to enrol in theory, but in practice they are likely to encounter difficulties in using the system.

In order to defeat replay attacks or even as a suggestion as to what to do when someone steals our IrisCode the following action can be taken. As there are many possible permutations of IrisCode bytes, one can make a new IrisCode permutation everyday or there can be application-specific, device-specific or even session-specific IrisCode templates. Depending on the application there can be re-registration supplying the individual with a different IrisCode template that will work.

In the case of a false rejection of someone on the first attempt at identification (due to the setting of a low threshold) there is proof that with a maximum of 3 consecutive trials it is almost certain that the individual will be accepted (Mansfield et al., 2001).

Finally elderly persons' eyes sometimes show a thin white ring surrounding the iris. This optical opacity develops with age and should be accounted for.

*Accuracy*

The combinatorial complexity due to the iris pattern variability is so high that real-time decisions about personal identity are possible with high confidence even in the case of 'identification mode' very large-scale databases. This is because the algorithm that calculates the matching of any two IrisCodes is a test of statistical independence applied to the 2048 bits of the IrisCode. The test is passed every time two different IrisCodes are matched and the test fails when one eye's IrisCode is compared to itself. A variable[123] that is a measure of the dissimilarity of any two IrisCodes is set to 0 if the two IrisCodes match perfectly and set to 0.5 for two

[122] However, it would be good to note that even in the case of a defocused eye image there can be an IrisCode computed, mainly as a result of noise, which is different that any other like it making it even in this case very difficult to confuse it with another (false match).

[123] Hamming Distance (HD) is the fraction of the number of disagreement between the corresponding pair of bits in the IrisCode once those bits that represent non-iris artifacts are taken-out (e.g. eyelashes, noise) divided by the number of total number of bits that mattered in the comparison.

different uncorrelated irises. Extensive testing and matching on a set of 4258 different iris images (from cases in the UK, USA, Japan and Korea) totalling almost 9.1 million comparisons prove that the test fits excellently into a theoretical binomial curve with 249 degrees of freedom. This is a measure of the success of the algorithm since the theoretical probability of two different IrisCodes having fewer than 30% of their bits common is 1 in 1.5 billion and that of having 29% of their bits common is 1 in 13 billion showing the extreme improbability that IrisCode bits of any two different irises might disagree in fewer than a third (33%) of their bits. This suggests that in order to identify people by their iris patterns with high-confidence we need to demand that only as many as 32% of their IrisCode bits are common (theoretical odds of a false match 1 in 26 million).

When comparing two IrisCodes taken from the same iris (verification), it is possible to match the two with confidence since the distribution of same-eye images (even at different times, conditions and acquisition cameras) proves that the average percentage of disagreeing bits ranges from 1,9% to 11% and even under poor image conditions does not exceed 33%. This means that if we set a decision threshold of 33% (theoretical false match probability of 1 in 4 billion) the likelihood of a false reject is insignificant even when acquisition conditions are poor. If iris samples are low in quality (either from poor conditions or even from original iris sources that are of poor nature) this results in fewer IrisCode bits on which to compare and base the decision process; the decision criterion thus becomes more demanding. If we may extract and compare 1152 bits with 100% of the iris visible, then the acceptable fraction of bits that may disagree can be up to 35% (1 false match in 133000) while this may drop to 14% when only as many as 200 bits are available for comparison (in the case that only 17% of the iris is visible).

The technology can be used effectively in identification as well as verification mode and thus its potential for large population applications is strong. The requirements of operating in identification mode are vastly more demanding than those in verification mode but this technology is able to handle identification for large databases without any serious degradation in accuracy. In this case a renormalisation may be needed of the matching algorithms as to the number of IrisCode bits that are effectively compared due to the different database search sizes (Cambier, 2003). The standard process of splitting the reference database so as to lower the maximum number of entries and thus increase the accuracy and performance of the system need not be used with this technology. However, since such large population databases are non-existent it is unlikely that this system would be chosen as the biometric technology on which to build any system that requires historical database searching.

*Security*

It is quite clear that the accuracy of the iris recognition technology, assuming enrolment is not a problem, ensures that enhanced security may be achieved using this method. The technology used in verification mode performs in such a way that user authentication is guaranteed for physical and digital access authorisation with little risk for false reject individuals (if two or three attempts are allowed). However,

the whole process is dependent on the quality of the cameras chosen for the iris recognition. It has been shown[124] that commercially available iris recognition systems could be fooled with iris images printed on paper. It is therefore essential that cameras that can distinguish between live and fake irises (this can be done through a liveness test, for example by distinguishing the movement and light reflections of living eyes from iris images or pupil dilation). Yet another very serious problem may come from the central storage of such sensitive information which needs to be protected from abuse and misuse at all costs. Strict auditing of the centrally stored IrisCodes will be required to guarantee their safety. It is only under these circumstances that iris recognition can be used to alleviate identity theft.

*Privacy*

When considering privacy issues it should be noted that the enrolment process necessarily requires the user to opt-in since it can not be done without consent. The data collected in this way can be used for no other purpose than for identification and authentication of the individual and so we may assume that the technology cannot be used for any other purpose (such as surveillance). The technology is also ideally suited for use with smart cards due to the relatively small size of the template (512 bytes) which may be easily stored on a smart card and manipulated so as to deliver 'on-chip' biometrics. This system would also be secure against theft or loss of the smart card – even if someone could access the IrisCode inside the smart card chip, the code could be sufficiently changed when re-issued so as to prohibit unauthorized use while allowing the rightful owner continue to use the secure application. Moreover, it is impossible to re-engineer the IrisCode to produce the digital picture of the iris.

### A.3.5 Applications

Some of the major applications of iris recognition currently are: immigration control/border crossing (using verification, identification or watch-lists), aviation security, controlling access to restricted areas/buildings/homes, database/login access. There is further scope for using this technology in other government programs (entitlements authorisation), automobile entry/ignition, forensic and police applications or any other transaction in which personal identification currently relies on passwords or secrets.

The largest deployment so far is currently in all 17 border entry points (air, land and sea ports) of the United Arab Emirates (UAE). Immigration Control checks all incoming passengers against an enrolled database of about 420 000 IrisCodes of persons who were expelled from the UAE (the captured IrisCode of an arriving passenger is matched exhaustively against every IrisCode enrolled in the database). After three years of operation and with an average 6500 passengers entering every day - totalling 2.1 million passengers already checked - and some 9500 identified as

[124] Tsutomo Matsumoto, of Yokohama National University, at Biometrics 2004 conference in London

being on the list and travelling with forged identities, the system is described as very fast and effective (Daugman, 2004)

The same system is also being trialled as a 'positive' application in Schiphol airport (NL), Frankfurt airport (DE), several Canadian and 10 UK airports during 2004. Furthermore, on the Pakistan-Afghanistan border, the United Nations High Commission for Refugees (UNHCR) uses such a system for anonymous identification of returning Afghan refugees.

In terms of user acceptance it is clear that this system does not have the negative connotations that fingerprint recognition has. Moreover, the enrolment procedure is non-contact and uses video/photo technology that is familiar to the wider public. There are also currently no collections of iris data that may have been compromised. However, early users of the technology state that the enrolment process creates a sense of discomfort and that the quality of the acquiring the photo device is critical to the success of the recognition phase. Use of the technology in order to minimize fraudulent access to public services may become the most useful application although it may bring a social stigma to been recognized through your iris just as fingerprint recognition has. A fascinating use of iris scan is mentioned by the National Geographic editorial team who took a photograph of an Afghan girl and 18 years later used iris recognition to verify her identity.

### A.3.6 Future Trends

As is the case with most of the biometric technologies under discussion, reliable/objective performance data are limited. However, the accuracy of this biometric technology is undoubtedly the best compared to other modalities, assuming the system is implemented correctly. Recent field and laboratory trials have produced no false matches in 9.1 million comparison tests (Daugman, 2003). In addition, the threshold for the decision process may be set automatically (no human intervention) and thus the human role is minimized.

Despite the very good accuracy rates achieved, which are necessary for high-security applications, and the lack of negative connotations (not associated with criminals and law enforcement as fingerprints are), the high costs of the technology deployment combined with the fear of lock-in to the technological platform and the user perception of discomfort are putting a brake on the diffusion of iris recognition.

## *A.4 DNA as a Biometric Identifier*

### A.4.1 How is DNA used as a biometric identifier?

*DNA structure*
DNA (deoxyribonucleic acid) is the complex substance that contains the genetic information of an individual. DNA has a double helix structure[125] (discovered by James Watson and Francis Crick in 1953 at Cambridge University). Each helix is a linear arrangement of four types of nucleotides or bases: A adenine, C cytosine, G guanine and T thymine. Between the four bases, only two pairings are chemically possible; A always pairs with T and G with C. As the helixes are complementary, when the first helix contains the sequence AGTCCTAATGT for instance, the second one contains the complementary sequence, so TCAGGATTACA. The sequence of the bases determines all the genetic attributes of a person.

For this study and with the current knowledge on the DNA, it is very important to observe the following points[126]:

- only 2-3% of the DNA sequence represents the known genetic material;
- almost 70% of the sequence is composed of non-coding regions, i.e. we do not know the function of these regions;
- almost 30% of the sequence is composed of non-coding repetitive DNA, and only 1/3 is tandemly repetitive, the rest (2/3) is randomly repetitive.

Thus DNA identification is based on techniques using the non-coding tandemly repetitive DNA regions, so only the 10% of the total DNA that in as far as we now understand bears non-sensitive information.

In general DNA identification is not considered by many a biometric recognition technology, mainly because it is not *yet* an automated process (it takes some hours to create a DNA fingerprint). However, because of the accuracy level of the process and because we consider it as a possible future biometric trait we decided to further analyse it together with the standard biometric technologies.

*DNA sample*
DNA can be isolated from a sample, such as: Blood, Semen, Saliva, Urine, Hair, Teeth, Bone, Tissue, etc. So, DNA counts several sources of biological evidence, which are especially easy to collect or to find (so consequently to steal) in every place that an individual has been.

*DNA template*
In the case of DNA use as a biometric, it is necessary to transform the sample into a template; an irreversible process. DNA fingerprint or DNA profile does not enable analysis related to genetic or medical aspects because the technique used for establishing a DNA template focuses on the non-coding[127] regions of DNA[128], and

[125] http://faculty.ncwc.edu/toconnor/425/425lect15.htm
[126] http://www.college.ucla.edu/webproject/micro7/lecturenotes/finished/Fingerprinting.html
[127] Non-coding is the term used for labeling these regions because the current knowledge on the DNA does not allow knowing the function of these regions.
[128] www.dsmz.de/mutz/mutzdnaf.htm

more precisely only on a specific part of the non-coding regions characterized by a high polymorphic degree.

*a) DNA template: DNA fingerprinting*

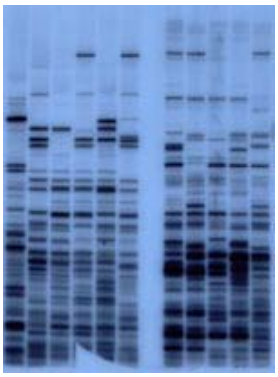
DNA fingerprinting (discovered by Alec Jeffreys in 1984 at the University of Leicester) allows identifying DNA patterns at various loci (specific places within the DNA sequence) that are unique to each individual - except identical twins. Each pattern is a repeated DNA fragments section, known as variable number of tandem repeats (VNTR), and its size depends on the number of repetitions. At a given locus, the number of repeated DNA fragments varies between individuals. The technique used to examine DNA patterns, is based on the restriction fragment length polymorphism (RFLP) analyse. Due to the low quality and quantity of the DNA sample in crime scene, the technique based on the polymerase chain reaction (PCR) is privileged in Forensic.

**Make a DNA Fingerprint: detailed procedure** (Betsch, 1994)

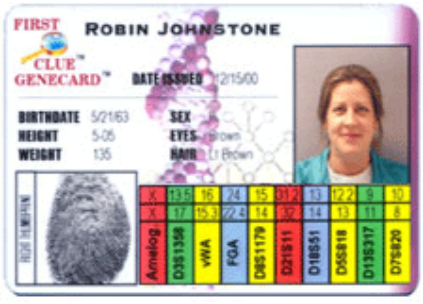
The procedure to make DNA fingerprint is composed of the following steps:

- Isolation of DNA; DNA must be recovered from a source of biological evidence. It is essential to avoid any type of contamination.
- Cutting, sizing and sorting; special enzymes called restriction enzymes are used to cut the DNA at specific places. Thus, the repeated DNA fragments sections are recognized. Then, they are separated and sorted by size through a gel electrophoresis.
- Transfer; the resulting distribution is transferred to a nylon or nitrocellulose sheet placed on the gel by blotting.
- Probing; this step consists in adding radioactive or coloured probes to the sheet in order to producing the DNA fingerprint.
- Final DNA fingerprint is built by using several probes simultaneously (5-10 or more). The result resembles bar codes.

The procedure to make DNA fingerprint is composed of the following steps, i.e. isolation of DNA; denaturalization of DNA (cutting, sizing and sorting); transfer and probing. DNA fingerprint is built by using several probes (5-10 or more) simultaneously. The result resembles bar codes (see pictures below.



**DNA fingerprint image**




**DNA profile representation**

**DNA templates**

*b) DNA template: DNA profiling*
From DNA sample, it is possible to establish DNA profiles (Butler, 2004) in order to represent the specific DNA patterns by numerical data. The numerical result is a string of values, e.g. "13.5,17 – 16,15.3 -.. - 11,9 - 10,8"; each pair of values is associated with a specific locus (e.g., D3S1358, VWA, FGA, etc.). Below the photography, the card[129] shows the DNA profile (in fact just and extract) of this person, Robin Johnstone.

Nowadays, DNA identification is mainly used in forensics. More precisely in forensics investigation, DNA fingerprint appears as a powerful tool in order to exclude an individual from a given DNA sample. Indeed, in criminal identification, it is necessary to contrast the DNA of suspects with the DNA evidence found in the crime scene, and when a suspect has a different DNA pattern than the evidence, he is excluded. So the DNA fingerprint is used to prove the suspect innocence. It is easier to exclude an individual than it is to include an individual with the same certainty[130].This assessment is also made for the paternity proof enactment. In this field, there are only three legitimate conclusions from DNA identity testing: 1) *exclusion*; the individual cannot be the source of the evidentiary sample; 2) *non-exclusion*; the individual cannot be excluded from being the source; and 3) *no results*; the analysis cannot be performed (Strom, 1999).

### A.4.2 How does it work?

Unlike other biometrics identifiers, DNA enrolment is always possible; everyone has DNA at every time. In addition, DNA allows an enrolment at birth. So, the main advantage of DNA for this step is DNA enrolment presents no failure case (i.e. no probability that a user will not be able to be enrolled), so the DNA rate FTE (Failure to Enrol) is 0%. However, DNA enrolment is neither direct (needs a physical extraction and biochemical process, we cannot take a picture of DNA as for fingerprint or iris) nor automatic (needs human intervention). Consequently, DNA is frequently considered as a specific case of biometrics because of the non-automatic enrolment.

**a) Acquire Sample**
DNA collection consists in performing an extraction of cells from one of all mentioned biological evidences in order to obtain a DNA sample. DNA collection is easy and takes some seconds. Several methods exist, e.g. finger prick for blood, a bucal swab for saliva or a patch for skin.

[129] http://www.testsymptomsathome.com/GTI85_productfeatures.asp
[130] http://www.adoptiondna.com/what-is-dna.php

Nonetheless, DNA is subject to degradation and contamination. The preservation of DNA sample is a particular concern in order not to interfere with the analysis and the final result. There are various types or sources of degradation (temperature, humidity, light) and contamination (chemical, biological and human source). Therefore, it is necessary to dry the sample and freeze it; otherwise the integrity and the quality of the sample could not be guaranteed.

In 2002, Interpol launched an **inquiry on DNA database** in order to obtain a global overview of DNA usage in Forensics. The final objective is to gather DNA profiling information in order to facilitate the possible future exchange of DNA related to intelligence between the Interpol Member States (Interpol, 2003).

**Results for the European Region**

- The European Region consists of 46 countries and 1 Sub-Bureau
- 93% of the European Region replied to the DNA database inquiry year 2002
- 36 countries perform DNA analysis in criminal investigations
- 26 countries have an implemented DNA database including 9 CODIS software
- 9 countries have an implemented DNA database including 4 CODIS software
- 21 countries have officially accredited laboratories and 7 countries pending
- the most prevalent category in the database is Stains with the most quantitative being the convicted category
- 24 out of the 35 countries with an implemented or planned DNA database allow the international exchange of profiles.

**b) Extracting Features**

*Transforming the sample into template*

As was shown, DNA sample is used to provide DNA Fingerprint whose representation is an image. A DNA fingerprint is a representation of the specific DNA patterns (black bands in the image) at various loci. However and always from DNA sample, it is possible to represent them by numerical data by establishing DNA profile, as described before. In both cases, the transformation is a time consuming process (several hours) and requires specific skills.

*Digitalisation and storage*

For the digitalization of DNA fingerprint, it should be necessary to capture images by using a digital camera for instance. Hence, the database should be a bank of images. Some aspects, such as the number of probes and the quality of the image (resolution, format) should be normalized, especially if in the future we would apply software in order to store and compare DNA fingerprint.

In the case of DNA profiles, the database stores numerical data, and more precisely strings of values, the direct representation of the DNA profile. The length of the string depends on the number of loci used to provide the DNA profile. It seems that this number is not fixed among the DNA profile databases. Moreover, the used precision of the value seems to be variable; it is possible to find a precision with one or two decimals. If this type of digitalisation is used, these two points should be subject to standardisation in order to enable future comparisons.

In USA and for forensic perspectives, a CODIS (Combined DNA Index System) database has been launched in 1997/1998. DNA samples have been collected in all states in order to link serial crimes and unsolved cases with report offenders. This database stores DNA templates, i.e. DNA profiles with the numerical representation and uses 13 loci. *The CODIS database allows law enforcement to cross-reference their DNA templates with that of other agencies across the country* (Yen, 2004). Four loci have been established by Interpol as the European standard (Interpol Standard Set Of Loci or ISSOL) (Interpol, 2001), and the European Network of Forensic Science Institutes (ENFSI) recommends the use of European Standard Set (ESS) - three additional loci than the Interpol list - in laboratories throughout Europe (OJ, 2001).

**Some DNA markers systems in Forensics:** (Interpol, 2003)

- CODIS software
- ESS
- SGM+
- Profiler+
- Power Plex 16

**DNA markers**

STRs (Short Tandem Repeats) are the most widely DNA markers used in forensics. The CODIS database uses 13 STRs as the core loci (Ashcroft et al., 2004). STR is a small base sequence (e.g. TCTA for the STR marker at the locus DYS391) repeats itself several times, e.g. 8 times, so the DNA pattern is $(TCTA)_8$.

An STR marker is a simple sequence (preceding example TCTA); let's show a contrasting example, a polymorphic DNA marker in order to understand the wide range of DNA markers:

$(TCCTGTCAAAC(TAACC)_2)_8$

Besides the standardization issue that has just been raised by the considerations about digitalization and storage of DNA templates, storing DNA templates in data bases generates further security and privacy concerns in the public opinion. These will be detailed later in the report.

**c) Comparing Templates**

DNA matching is not a trivial process and is expensive due to the complex transformation from the sample into template. The time required for the verification process is long; it is around 4-5 hours (Yen, 2004) with forensics marker and some parts of this process are still manual.

So, the comparison does not take place in real-time. In addition, this process must be performed by scientists and depends on the kind of marker system used; so it requires a lot of knowledge and skills (Butler, 2004). The risk concerning the matching is DNA-based system would create potential false matching because of the impossibility to differentiate identical twins.

**d) Declaring a match**

In the case of DNA fingerprint and in forensic framework, the matching is performed with some DNA templates, the evidence template from the scene and some templates from suspects. The declaring matching process is a human process supported by computer. First of all, the examiner or analyst must verify that the laboratory comparison conditions are fulfilled, for example he proceeds to some

computerized measurements[131] in order to ensure that the templates are comparable. Then, the examiner must establish whether two templates match in accordance with a match criterion[132] and finally, he must determine the probity of the match, i.e. the probability that this match is not a random match, so-called probability random match (RMP) [133] (Thompson, 2003). In addition, some European countries carry out another examination from a second sample in order to verify an inclusion declaration.

In the case of CODIS[134], computer software is used to automatically search its two indexes, Convicted Offender index (felony sex offences and other violent crimes) and Forensic index (from crime scene evidence) for matching DNA profiles.

### A.4.3 Technology – state of development

DNA testing is a technique with a very high degree of accuracy. The statistical sampling shows a 1-in-6-billion chance of two people having the same profile (Burgess, 2004). Nevertheless, using the DNA technique it is impossible to distinguish identical twins (the probability of identical twins in the US is 1 in 250 or 0.4%)[135]. And according to (Bromba, 2004), the accuracy of DNA is considered as lower than the one of the iris or retina recognition. Moreover, the possibility of sample contamination and degradation also impacts the accuracy of the method.

Concerning DNA fingerprints, there are systems in various stages of research and development which will enable rapid interpretation for the matching, such as AnaGel (Silva et al., 2001). We can therefore expect more automation for the DNA verification process in the future.

### A.4.4 Challenges and limitations

*Seven pillars*

DNA is present in all human beings (universality) and with the exception of monozygotic twins it is the most distinct biometric identifier available for human beings. DNA does not change throughout a person's life, therefore the permanence of DNA is incontestable. It performs well for the applications where it currently used (forensics, paternity tests, etc.) though it would not be suitable for every application. DNA tests are difficult to circumvent under certain conditions (supervised sample collection with no possibility of data contamination.) If sample collection is not supervised however, an impostor could submit anybody's DNA.

[131] These computerized measurements must to confirm that the difference immigration distances is less than some standard deviation of a set of independent measurements of fragments taken from one sample. Source: http://www.ajc.state.ak.us/Reports/dnaframe.htm

[132] "A match criterion is an objective and quantitative rule for deciding whether two samples match. For example, a match criterion for VNTR systems might declare a match between two samples if the restriction-fragment sizes lie within 3% of one another." (DTFC, 1992)

[133] The theoretical risk is 1 on 1 billion when the laboratories are able to match two templates over ten or more STR loci and the templates stemming from single source sample, this risk is 1 on 1 million when fewer loci are examined and is 1 on 1000 when the comparison involves templates stemming from mixed samples. In fact, under the real conditions the rate of laboratory error may be much higher.

[134] http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml

[135] http://www.keepkidshealthy.com/twins/twin_statistics.html (in the US)

We all leave DNA traces wherever we go (a single hair can provide a sample) and so it is impossible to keep DNA samples private.

DNA faces several other challenges. Several hours are required in order to obtain a DNA fingerprint. In addition the collection methods (involving an extraction of a physical sample) generally raise privacy concerns and DNA data encompass not only identification data but also genetic data. The public is fairly hostile to DNA usage and storage. In conclusion, DNA performs well on the aspects of universality, distinctiveness, permanence, performance and resistance to circumvention, while it is weak on collectability and acceptability.

*Privacy and Security concerns*

DNA collection is regarded as invasive sampling (e.g. finger prick for blood). However, currently DNA sampling methods have evolved and allow less invasive sampling (collection with a bucal swab of saliva sample or of epidermal cells with a sticky patch on the forearm). Thus, the new sampling methods are considered as not violating the social expectations for privacy (Quarmby, 2003).

The main problem with DNA is that it includes sensitive information related to genetic and medical aspects of individuals. So any misuse of DNA information can disclose information about: (a) Hereditary factors or (b) Medical disorders

However, DNA profile representation is just a list of numbers, so it is non-informative and is regarded as neutral. In addition, in forensics the selection of DNA markers is performed with the aim to be neutral and endeavours to locate DNA markers away from or between genes rather than being part of gene products. Hence, DNA markers are not established in order to be associated with any genetic disease.

Race and ethnicity are actually cultural, not biological nor scientific, concepts. Nevertheless, DNA can tell a person what parts of the world some of their ancestors came from[136].

Finally, the concern is really linked with the DNA sample because it enables to establish sensitive information related to genetic aspects. So, that point directly leads to the security of the DNA samples database or to the certainty of the DNA sample destruction after the DNA template elaboration.

Indeed, the two main security concerns are about the security of DNA system (access rights, use of information only for the overriding purpose), the implementation of security mechanisms in order to ensure for instance a high level of confidentiality and the security of DNA database (access rights, length of information retention). It seems essential to define the conditions under which the samples can be banked (anonymous/coded/identified storage) and to guarantee data protection. So, a quality assurance plan and safety regulations of banking

[136] http://www.adoptiondna.com/what-is-dna.php

(certification of authorized personal, responsibilities listing, safety measures, etc.) are primordial requirements (Godard et al., 2002).

### A.4.5 Applications

Each person has a unique DNA fingerprint and it is the same for every single cell of a person. A DNA fingerprint, unlike a conventional fingerprint cannot be altered by surgery or any other known treatment. Apart from its use in medical applications (e.g. diagnosis of disorders), DNA is widely used for paternity tests, criminal identification and forensics. It is also used in certain cases for personal identification as the following two examples illustrate. In the US, a pack, known as DNA PAK[137] (Personal Archival Kit) is sold with the aim of conserving a sample so that an individual can be identified in the case of kidnapping, accidents or natural disaster. Another US company, 'Test Symptoms@Home' sells several products and services based on DNA. One such product is a personal identification card[138] which exhibits general data, such as name, weight, sex, etc, a fingerprint picture and an extract of DNA profile based on the same loci used by CODIS database. Despite these examples, commercial applications for DNA are very limited; privacy fears and low user acceptance will undoubtedly be a bottleneck for the use of DNA in large-scale applications.

### A.4.6 Future Trends

Progress in DNA testing will come in two areas: current techniques will improve, offering more automation, precision and faster processing times, and new techniques will be developed (e.g. by exploiting the electronic proprieties of DNA[139]). Nowadays it is impossible to distinguish identical twins. In future however it may be possible to do so either through technical improvements in current DNA testing or through a different approach. One such alternative is to study the DNA of the micro-organisms each person carries, such as viruses, bacteria, or other parasites (Crow, 2001).

A joint partnership between a US and a Taiwanese company[140] currently exploits DNA technology for security solutions and provides several products based on plant DNA technology for anti-counterfeit or tracking purposes, such as the DNA ink[141] with a real-time authentication (DNA test pen) or DNA marker integrated into textile materials. For this study, an interesting application of the DNA ink would be to use it for the authentication of passports or visas. Though this is not a direct use of DNA to identify a human, it is a potentially interesting application.

It is important to understand that DNA from bacteria, plants, animals and humans is the same at chemical and structural levels; the differences lie in the length of the DNA (number of letters, 4 million for a simple bacteria DNA and at least 3 billion

[137] http://www.yellodyno.com/html/dnahome.html
[138] http://www.testsymptomsathome.com/GTI85_productfeatures.asp
[139] http://physicsweb.org/articles/news/8/3/8/1, http://physicsweb.org/articles/world/14/8/8/1
[140] http://www.adnas.com/products.htm, http://www.biowell.com.tw
[141] a scientific view of DNA-based ink is provided in Hashiyada (2004)

for human DNA[142]) and the sequence. So studying DNA from bacteria is easier than studying DNA from plants, and by transitivity, easier than the one from animals and ultimately humans. From this assessment, we can infer two future tendencies: the first one is the use of another type of DNA to supplant the human DNA for individual identification (e.g. the case of the study of the parasites constellation that each of us carries or the application of DNA ink) and the second one is that current applications based on plant DNA or on animal DNA may in future exist for human DNA.

The Canadian Royal Botanical Garden has presented its future view on the botany in the field[143]. The botanist of tomorrow is likely to use a DNA scanner, a small hand-held device enabling some complete analysis from the collected sample. In addition, new methods will emerge,[144] e.g. DNA may be scanned in a contact-less way based on Bluetooth technology. Thus, we can easily imagine this idea of hand-held device for the analysis of sample found in a crime scene or disaster scene.

Today, the time required for DNA testing (from the extraction through the matching) is around 4-5 hours (Yen, 2004) due to the time needed for the amplification process (2-3 hours). Recent tests however suggest that the time required will be reduced in the near future. Real time PCR (Schaad et al., 2002) provide good results on plant DNA. And recently, the time needed to extract and amplify animal DNA was reduced to less than 15 minutes [145] using Extract-N-Amp™ technique based on PCR (Origins, 2003). All tests have been performed with a tissue sample from a mouse. This technique provides as a result a DNA ready to the sequencing. In addition, this technique has been tested using saliva, hair and human tissue sample and seems to operate well.

[142] www.nal.usda.gov/bic/Education_res/ iastate.info/bio1.html
[143] http://www.rbg.ca/greenlegacy/pages/botanists_future.html
[144] www.cs.odu.edu/~dtran/cs410/Super DNA Scanner.ppt
[145] (Newby, 2003) declares "The best systems out there still take at least 15 minutes per sample".

# ANNEX B: MAIN QUESTIONS ASKED

In spring 2004, the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE) of the European Parliament asked DG – JRC - IPTS to carry out a prospective study on the implications of biometrics on the future everyday life of citizens through an analysis of the socio-economic, technological, legal and ethical aspects of the introduction of biometrics.

The Committee were fairly specific in terms of the questions they wished to be explored, driven by a tight timetable for voting on the Commission's proposals for implementing biometrics for border control applications. During the study kick-off meeting which took place in Brussels the following July, the decision was taken to tackle the tasks in two stages:

(a) Stage 1 consisted of a presentation by experts to the newly elected EP LIBE Committee members on the most important issues (related to the pressing political agenda of biometrics for border control applications), which was organised on October 6th 2004; and

(b) Stage 2 consists of the current report on other issues (including the more prospective ones).

By all accounts the result of stage 1, which was intended to provide as much information as possible to help MEPs make an informed decision on the vote, was well received. As a result the study team was able to explore further the implications of deploying biometrics, through a wider and more prospective approach.

The study has by and large addressed all initial specific questions, although the structure of the Report does not follow the line of those questions. A listing of the original questions asked and a description of how the report addresses each one can be found below.

## *B.1 THE QUESTIONS ASKED BY THE EP LIBE COMMITTEE*

1. The first issue regards the technology; technological development and applications in the field of biometrics are flourishing. Nevertheless we are entering "unknown dimensions", in the words of the Commission. An up-to-date comprehensive overview is needed on the impact of the technologies to be used for the specific application envisaged by the Commission's proposals (two fingerprints and the photograph, with or without facial recognition technology depending on each Member State's decision). A presentation of the tests that have been conducted so far with these technologies is also necessary. In addition, a technology impact assessment of the Commission's envisaged border protection scenario could be undertaken.
2. A second question is whether, given the technological possibilities, the existing and developing legal framework, in particular as regards ICAO, and other constraints like patents, different scenarios using other biometric identifiers would be realistic.

3. Thirdly, another important element is the cost of introducing biometrics, which is largely not taken into account at the European level even if it is sometimes considered at the national level (see "Biometrie und Ausweisdokumente, Leistungsfaehigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung, 2. Sachstandsbericht" Report by the office for technology assessment of the German Bundestag).
4. Fourthly, although the evaluation of whether the increased security made possible through the use of biometrics outweighs the costs is and will be essentially a political one, all factual elements which could help make this cost-benefit assessment (costs and benefits would need to be understood in the widest possible sense) and the associated proportionality analysis would need to be collected.
5. Finally, the wider impact of the use of biometric technologies by governments, businesses and end-users on the everyday life of the citizen will also have to be addressed. Such an analysis would complement the cost-benefit and proportionality analysis indicated above by addressing social and ethical considerations.

## *B.2 ANSWERS THROUGHOUT THE REPORT*

The first question is addressed as follows:

a. There is an overview of the selected technologies in chapter 2 (with further detail in annex A) where important points related to border control as well as other likely applications are presented. There is also a section in chapter 2 where these and other prominent technologies are compared against the seven pillars and relevant conclusions are drawn.

b. The report describes as much as possible any information on trials in chapter 2 (either completed or on-going) but the problem is that very little data on trials are publicly available. Moreover, if data are available, they are usually not comparable with the results of other trials. As a result, one of the recommendations of this report is precisely that existing trials should exchange information and best/worse practices and that more trials, especially related to the use of multimodal biometric systems is required.

c. During the October 6 meeting at the EP, the specific use of fingerprint and face technologies for border control applications was presented. In addition one of the scenarios presented deals with a border control situation and its analysis in chapter 4 reveals some of the more interesting points on this issue.

The second question is addressed as follows:

a. It was mostly addressed during the October 6 meeting, but some information on how to match technologies and applications based on the seven pillars is provided in section 2.8 and 3.4.

b. The border control scenario shows how biometric identifiers are used in other parts of the world.

c. The equivalence principle is explained in section 3.1.3 and it also emerges as one of the report's conclusions. However, no reliable data were identified to produce an in-depth analysis of this concept.

The third question is addressed as follows:

a. Costs of deployment are mentioned throughout the report and especially in sections 1.4.4 and 2.9. However due to the lack of identified sources, no conclusions could be drawn on this point. Suggestions as to what to consider when dealing with implementation costs in a specific context are provided. The lack of field trials that could provide information on true rather than theoretical costs is reported.

b. Moreover, chapter 3.2 is on the economic implications of biometrics. It tries to give an account of the broader economic issues that have to be taken into account when implementing biometrics.

The fourth question is addressed as follows:

a. A cost/benefit assessment can only be performed in a specific context and no publicly available reliable data were identified for this purpose. A cost/benefit analysis done by specific manufacturers tends to maximise the benefit and minimise the cost. These are also application-specific and thus difficult to generalise. Moreover, no independent analysis was identified that uses data from real life experiments with heterogeneous sample populations. This is clearly reported as a policy recommendation.

b. The security efficiency vs. costs dilemma is taken up within many sections of the report. It relies on understanding the limitations of biometric technologies and the necessary trade-offs as a result of any specific application deployment. It is also worth noting (section 3.2.1) that targeting the strongest identification process (more security) is not always optimal from an economic point of view.

c. The need for a proportionality analysis is stressed (see section 3.3.2) but no such analysis is undertaken due to the lack of available data.

The fifth question is addressed as follows:

a. This specific approach is central throughout the report, i.e. discussing the wider impact of the use of biometrics by governments, businesses and end-users on the everyday life of the citizen. Typical for this approach is that biometrics are not only discussed from a technological point of view, but social, economic, legal and other issues are also raised, such as medical implications, interoperability, as well as privacy and security.

b. The so-called 'diffusion effect' is presented as a central argument and conclusions are drawn as to its possible positive and negative implications. Strong social and ethical challenges and ways to counter their effects are also cited; the clarity of purpose recommendation is the most significant.

# References

**(Ashbourn, 1999)** J. Ashbourn, *A biometric white paper*.

http://www.avanti.1to1.org/whitepaper.html

**(Ashcroft et al., 2004)** John Ashcroft, Deborah J. Daniels, Sarah V. Hart. *DNA forensics Research and Development*, U.S. Department of Justice, Office of Justice Programs, Nov. 2004

**(Bailly-Bailliére et al., 2003)** E. Bailly-Bailliére, S. Bengio, F. Bimbot, M. Hamouz, Jo. Kittler, J. Mariéthoz, J. Matas, K. Messer, V. Popovici, F. Porée, B. Ruíz, and J.-P. Thiran. *The BANCA Database and Evaluation Protocol*. Audio- and Video-Based Biometric Person Authentication (AVBPA), Guilford, 2003.

**(Beslay & Punie, 2002)** Beslay L. & Punie Y. 'The virtual residence: Identity, privacy and security', The IPTS Report, Special Issue on Identity and Privacy, No. 67, September 2002, 17-23.

**(Betsch, 2004)** David F. Betsch, *DNA Fingerprinting in Human Health and Society* Biotechnology Training Programs, Inc. Edited by Glenda D. Webber, Iowa State University Office of Biotechnology, 2004

**(Bowyer, 2003)** K. W. Bowyer, *Face Recognition and the Security versus Privacy Tradeoff*. http://www.cse.nd.edu/~kwb/nsf-ufe/SecurityPrivacy.pdf, August 2003.

**(Bromba, 2004)** Dr. Manfred Bromba, *Biometrics FAQ*, last change November 2004

http://www.bromba.com/faq/biofaqe.htm

**(Brown et al., 2002)** C. C. Brown, X. Zhang, R.M. Mersereau & M. Clements *Automatic Speech Reading with Application to Speaker Verification*. ICASSP International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2002

**(Burgess, 2004)** Richard Burgess. *Defence challenges accuracy of DNA*. Oct. 6, 2004.

http://www.acadiananow.com/searchforakiller/html/5922BC48-F441-4EA3-929A-5685BD070A51.shtml

**(Butler, 2004)** Dr. John M. Butler. *Technology Developments in Forensic DNA Typing and Prospects for Non-Forensic. Use of DNA Identification*. NIST Biotechnology Division May 12, 2004

**(Cambier, 2003)** J. Cambier, *technical Report TR-02-004*, IRIDIAN technologies, USA, 2003

**(Choudhury et al., 1999)** T. Choudhury et al., *Multimodal person recognition using unconstrained audio and video* in Proceedings of the Second Conference on Audio- and Video-based Biometric Person Authentication, Washington, D.C., March 1999

**(Clarke, 1994)** R. Clarke, Human identification in information systems: Management challenges and public policy issues, Information Technology and People, Vol. 7., No. 4, 1994, pp.6-37.

**(Cole, 1998)** S. Cole, *Witnessing identification: Latent fingerprinting evidence and expert knowledge,* Social Studies of Science, 28/5-6, 1998, pp.687-712.

**(Crow, 2001)** James F. Crow *DNA FORENSICS: PAST, PRESENT, AND FUTURE* Genetics Department, University of Wisconsin, Madison, WI 53706, 2001

**(Daugman, 1993)** John Daugman, *High confidence visual recognition of persons by a test of statistical independence*, IEEE Trans, Pattern Analysis and Machine Intelligence, Vol. 1, No. 11, 1993, pp 1148-1161.

**(Daugman, 1994)** John Daugman, Univ. Cambridge, protected by U.S. Patent No. 5291560 issued March, 1, 1994

**(Daugman, 2003)** John Daugman, *How Iris Recognition works,* Univ. Cambridge, 2003. http://www.cl.cam.ac.uk/users/jgd1000/

**(Daugman, 2004)** John Daugman, Univ. Cambridge, BIOSEC conference. Barcelona, June 2004.

**(Daugman et al., 2004)** John Daugman, Univ. Cambridge, I. Malhas, IrisGuard Inc. *International Airport Review*, issue 2, 2004,

**(DTFC, 1992)** *DNA Technology in Forensic Science*, Committee on DNA Technology in Forensic Science, Board on Biology, Commission on Life Sciences, National Research Council, NATIONAL ACADEMY PRESS, Washington, D.C., 1992

**(Ducatel et al., 2000)** Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. & Burgelman, J-C. (eds.) (2000) *Scenarios for Ambient Intelligence in 2010*, IPTS-ISTAG, EC: Luxembourg. http://www.cordis.lu/ist/istag

**(EUR 20823 EN, 2003)** Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie Y. & Rodriguez, C. *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC, July 2003.

**(Garcia-Salicetti et al., 2003)** S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J. Leroux-Les Jardins, J. Lunter, Y. Ni, D. Petrovska-Delacretaz, *BIOMET: a Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand and Signature Modalities*, Proc. of 4th International Conference on Audio and Video-Based Biometric Person Authentication, pp. 845-853, Guildford, UK, July 2003.

**(Gavigan et al., 2001)** Gavigan, J.P., Scapolo, F., et.al. (Eds.) *A practical guide to Regional Foresight*, IPTS, Sevilla, EUR 20128, EN December 2001.

**(Godard et al., 2002)** Beatrice Godard et al., *Data storage and DNA banking for biomedical research: Informed consent, confidentiality, quality issues, ownership return of benefits.* A professional perspective, EUROGAPPP Project. November 2002.

**(Godet, 2000)** Godet, M. *The art of scenario and strategic planning*: *tools and pitfalls*, Technological Forecasting and Social Change 65, 3-22, Elsevier Science Inc, New York. 2000

**(Hashiyada, 2004)** Hashiyada Masaki, Development of Biometric DNA Ink for Authentication Security Division of Forensic Medecine, Tohoku J. Exp. Med., 2004, 204, pp109-117

**(Hazen et al., 2003)** T. Hazen, E. Weinstein, R. Kabir, A. Park, B. Heisele, *Multimodal Face & Speaker Identification on a Handheld device*, Workshop on Multimodal User 'Authentification' (MMUA), pp. 113-120, Santa Barbara, California, USA, Dec. 2003.

**(Hopkins, 1999)** Richard Hopkins. *An Introduction to Biometrics and Large Scale Civilian Identification.* International review of law, computers and technology; vol. 13 (1999), No. 3, (337-363), 338

**(ICAO-TAG, 2004)** *Biometrics deployment of machine readable travel documents.* ICAO TAG MRTD/NTWG, Technical Report, Version 2.0, May 2004.

http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf

**(Interpol, 2001)** *Interpol Handbook on BNA data Exchange and Practice*. Recommendations from the Interpol DNA Monitoring Expert Group. Lyon, June 2001.

**(Interpol, 2003)** *Global DNA database inquiry; results and analysis*, 2002. Interpol DNA unit. 2003 I.C.P.O.

**(ISTAG, 2001)** *'Scenarios for Ambient Intelligence in 2010'*, K. Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. and J-C. Burgelman (eds), IPTS-ISTAG, EC: Luxembourg http://www.cordis.lu/ist/istag

**(Jain et al., 1999)** Anil K. Jain, Ruud Bolle and Sharath Pankanti: "*Personal Identification in Networked society*", Kluwer Academic Publisher, ISBN 0-7923-8345-1, 1999.

**(Jain et al., 2001)** Jain, A. & Pankati, S. *Automated Fingerprint Identification and Imaging Systems*, in Lee, H. & Gaensslen, R. (eds.), Advances in Fingerprint Technology, 2nd Edition, Elsevier Science, 2001. http://www.research.ibm.com/ecvg/pubs/sharat-forensic.html

**(Jain et al., 2002)** Jain, A., Prabhakar, S. & Pankanti, S. *On the similarity of identical twin fingerprints*, Pattern Recognition, 35, 2002, pp-2653-2663.

**(Jain et al., 2004)** Anil K. Jain, Arun Ross and Salil Prabhakar, *An Introduction to Biometric Recognition* IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

**(Jain et al., 2004a)** A. K. Jain and A. Ross, Multibiometric Systems, Communications of the ACM, January 2004/Vol. 47, N°1

**(Kittler et al., 1998)** J. Kittler, M. Hatef, R. Duin and J. Matas, *On combining classifiers*, IEE Trans. On Pattern Analysis and Machine Intelligence 20, 3 (Mar. 1998), IEE, NY, 226-239.

**(Ly Van et al., 2003)** B. Ly Van, R. Blouet, S. Renouard, S. Garcia-Salicetti, B. Dorizzi, G. Chollet, "Signature with text-dependent and text-independent speech for robust identity verification", pp. 13-18, Workshop on Multimodal User Authentication, Santa Barbara, USA, 2003.

**(Mainguet et al., 2000)** Mainguet, J-F. & Pégulu, M. & Harris, J-B. *Fingerprint recognition based on silicon chips*, Future Generation Computer Systems, 16, 2000, pp 403-415.

**(Maltoni et al., 2003)** Maltoni, D., Maio, D., Jain, A. & Prabhakar, S. *Handbook of Fingerprint Recognition*, New York: Springer Verlag. 2003

**(Mansfield et al., 2001)** Tony Mansfield, Gavin Kelly, David Chandler and Jan Kane Biometric Product Testing, Final Report, CESG/BWG Biometric Test Programme, Issue 1.0, 19 March 2001

**(Mansfield et al., 2002)** A. J. Mansfield and J. L. Wayman, Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01, August 2002. By National Physical Laboratory and San Jose State University. http://www.biometricscatalog.org/2003GBW/downloads/Best_Practice.pdf

**(Mason et al.)** J.S.D Mason, F. Deravi, C. Chibelushi & S. Gandon BT DAVID - Final Report, Speech and Image Processing Research Group, Dept. of Electrical and Electronic Engineering, University of Wales Swansea, UK.

**(Massini et al., 2000)** Massini E.H. & Vasquez J.M., *Scenarios as seen from a human and social perspective*, Technological Forecasting and Social Change 65, 49-66, Elsevier Science Inc, New York, 2000, pp. 51-52.

**(Matsumoto et al., 2002)** Matsumoto T., Matsumoto H., Yamada K., Hoshino S.; *Impact of artificial "gummy" Fingers on Fingerprint Systems*; Proc. of SPIE, vol. 4677, pp. 275-289, Feb. 2002

**(Messer et al., 1999)** K Messer J Matas J Kittler, J Luettin and G Maître. XM2VTSDB: *The Extended M2VTS Database*. Second International Conference on Audio and Video-based Biometric Person Authentication, 1999.

**(Newby, 2003)** Deborah Newby, Even the very best of today's detection technologies require at least a 15-minute wait for each batch of samples. U.S. Department of Energy's Idaho National Engineering and Environmental Laboratory. http://www.sciencedaily.com/releases/2003/05/030522083139.htm

**(OECD, 2004)** *Biometric-based technologies*. Working Party on Information Security and Privacy, 30 June 2004, DSTI/ICCP/REG(2003)2/FINAL. http://www.oecd.org/sti/security-privacy

**(OJ, 2001)** Official Journal of the European Communities, COUNCIL RESOLUTION

of 25 June 2001 on the exchange of DNA analysis results. (2001/C 187/01)

**(O'Gorman, 1999)** O'Gorman, L *Fingerprint verification*, in: A. Jain, Personal identification in a networked society, Dordrecht: Kluwer Academic Publishers. R. Bolle & S. Pankanti (eds.), 1999. pp. 43-64

**(Origins, 2003)** Origins, issue ten, July 2003, SIGMA, pp 4-7

**(Pigeon et al., 1997)** S. Pigeon & L. Vandendorpe, *The M2VTS Multimodal Face Database*. In Proceedings of AVBPA 97, Springer LNCS, Bigün et al. Eds, 1997.

**(Punie et al., 2002)** Punie, Y., Burgelman, J-C. & Bogdanowicz, M., '*The future of online media industries. Scenarios for 2005 and beyond'*, The IPTS Report, 64, May 2002, 35-42.

**(Quarmby, 2003)** Ben Quarmby, The case for national DNA identification cards Duke Law and Technology Review, 2003 http://www.law.duke.edu/journals/dltr/articles/2003dltr0002.html

**(Ross et al., 2004)** Ross, A. & Jain, A. *Biometric Sensor Interoperability: A Case Study in Fingerprints*, Appeared in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), Prague, Czech Republic, Springer Publishers. LNCS Vol. 3087, 2004, pp. 134-145

**(Sanderson et al., 2003)** C. Sanderson, S. Bengio, H. Bourlard, J. Mariéthoz, R. Collobert, M.F. BenZeghiba, F. Cardinaux, S. Marcel, *Speech&Face Based Biometric Authentication at IDIAP*, IDIAP Research Report 03-13, February 2003

**(Sandström, 2004)** Sandström, M. *Liveness detection in fingerprint recognition systems*, Linköpig University Electronic Press, Thesis, June 2004, http://www.ep.liu.se.

**(Sasse, 2004)** Sasse, A. *Usability and trust in information systems*. Report for the Cyber Trust & Crime Prevention Project, UK Office of Science and Technology Foresight Program. 2004. http://www.foresight.gov.uk/

**(Shaad et al., 2002)** Norman W. Schaad and Reid D. *Real-time PCR and its application for rapid plant disease diagnostics* Frederick Pages 250-258 http://pubs.nrc-cnrc.gc.ca/tcjpp/k02-043.html

**(Silva et al., 2001)** Silva LM, Montes de Oca H, Diniz CR, Fortes-Dias CL.

Fingerprinting of cell lines by directed amplification of minisatellite-region DNA (DAMD). Brazilian Journal of Medical and Biological Research. 2001 Nov; 34 (11):1405-10

**(Strom, 1999)** Charles M. Strom. *Genetic Justice: A Lawyer's Guide to the Science of DNA Testing*, 1999. http://www.illinoisbar.org/Member/jan99lj/p18.htm

**(Thompson, 2003)** William C. Thompson, 1 J.D., Ph.D.; Franco Taroni,2,3 Ph.D.; and Colin G. G. Aitken,4 Ph.D. *How the Probability of a False Positive Affects the Value of DNA evidence.* J Forensic Sci, Jan. 2003, Vol. 48, No. 1 Paper ID JFS2001171_481

**(Wilkinson, 1998)** *'How to build scenarios'*, http://www.hotwired.com/wired/scenarios/build.html

**(Woodward, 1973)** D. Woodward Jr. *Super Bowl Surveillance: Facing up to biometrics*. United States v. Dionisio, 410 U.S. 1, 14 (1973)

**(Xia et al., 2003)** Xia, X. & O'Gorman, L. *Innovations in fingerprint capture devices,* Pattern Recognition*,* 36, 2003, pp.361-369.

**(Yen, 2004)** Robert C. Yen. *Forensic DNA Typing and Prospects for Biometrics*. Department of defense Biometrics Management Office. Summary Report, Biometric Identification Seminar, 16 JUNE 2004

# Glossary

**A**

***Attempt:*** The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

***Authentication***: Alternative term for 'Verification'

***Automated Fingerprint Identification System (AFIS):*** A specialized biometric system that automatically compares fingerprint images with a database of finger images. In law enforcement, AFIS is used to collect fingerprints from criminal suspects and crime scenes. In civilian life, fingerprint scanners are used to identify employees, protect sensitive data, etc

**B**

***Biometric:*** A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrolee.

***Biometric Data:*** The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

***Biometric Sample:*** Raw data captured as a discrete unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrolee as captured by a biometric system (e.g. biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).

***Biometric System:*** An automated system capable of capturing a biometric sample from an end user; extracting biometric data from that sample; comparing the biometric data with that contained in one or more reference templates; deciding how well they match; and indicating whether or not an identification or verification of identity has been achieved.

**C**

***Capture:*** The method of taking a biometric sample from the end user.

**D**

***DNA sequence:*** order of bases (A, C, G, and T) in a DNA molecule.

**E**

***End User:*** A person who interacts with a biometric system to enrol or have his/her identity checked.

***Enrolee:*** A person who has a biometric reference template on file.

***Enrolment***: The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

***Equal Error Rate:*** The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.

***Exclusion:*** when the DNA from a crimes scene fails to match that of a suspect. Inclusions are probability statements, exclusions are absolute.

***Extraction:*** The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

**F**

***Failure to Acquire:*** Failure of a biometric system to capture and extract biometric data (comparison data).

***Failure to Acquire Rate:*** The frequency of a failure to acquire.

***Failure to Enrol:*** Failure of the biometric system to form a proper enrolment template. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality).

***Failure to Enrol Rate:*** The proportion of the population of end-users failing to complete enrolment

***False Acceptance:*** When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

***False Acceptance Rate/FAR***: The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as:

$$FAR = NFA / NIIA$$

or

$$FAR = NFA / NIVA$$

where

FAR is the false acceptance rate

NFA is the number of false acceptances

NIIA is the number of impostor identification attempts

NIVA is the number of impostor verification attempts

***False Match Rate:*** Alternative to 'False Acceptance Rate', used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrolee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Non-Match Rate'.
***False Non-Match Rate:*** Alternative to 'False Rejection Rate', used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrolee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Match Rate'.
***False Rejection:*** When a biometric system fails to identify an enrolee or fails to verify the legitimate claimed identity of an enrolee.
***False Rejection Rate/FRR:*** The probability that a biometric system will fail to identify an enrolee, or verify the legitimate claimed identity of an enrolee. The False Rejection Rate may be estimated as follows:

FRR = NFR / NEIA

Or FRR = NFR / NEVA

where
- FRR is the false rejection rate
- NFR is the number of false rejections
- NEIA is the number of enrolee identification attempts
- NEVA is the number of enrolee verification attempts

This estimate assumes that the enrolee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes 'Failure to Acquire' errors.
***Forensic:*** Of or relating to courts or legal matters. Molecular markers are increasingly common in the context of forensics, both in wildlife and human cases involving identity or relatedness.

**I**

***Identification:*** The one-to-many (1:N) process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrolee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.

**L**

***Locus (pl. loci):*** from the Latin for "place".

**M**

***Match/Matching***: The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold
***Minutiae***: Small details found in finger images such as ridge endings or bifurcations.

**S**

***Screening:*** A few-to-a-few (N:N) process or N time a one-to-a-few process, which is regarded as a hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a "watch list" of persons who warrant detailed identity investigation or are known criminals, terrorists etc.
***Smart Card:*** A card-shaped portable data carrier that contains one or more integrated circuits for data storage and processing. A typical smart card chip includes a microprocessor or CPU, ROM (for storing operating instructions), RAM (for storing data during processing) and EPROM (or EEPROM) memory for non volatile storage of information.

**T**

***Template/Reference Template***: Data, which represents the biometric measurement of an enrolee, used by a biometric system for comparison against subsequently submitted biometric samples.

**V**

***Verification:*** The one-to-one (1:1) process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. Contrast with 'Identification'.

# Abbreviations

2D Two Dimensions
3D Three Dimensions

**A**
AFIS Automated Fingerprint Identification Systems

**C**
CCTV Closed Circuit Television cameras
CODIS Combined DNA Index System

**D**
DNA Deoxyribonucleic Acid
DMI Direct Medical Implications
DRM Digital Rights Management

**E**
EER Equal Error Rate
ESS European Standard Set
ENFSI European Network of Forensic Science Institutes
EU European Union

**F**
FAR False Acceptance Rate
FERET FacE REcognition Technology
FBI Federal Bureau of Investigation
FMR False Match Rate
FNMR False Non-Match Rate
FRGC Face Recognition Grand Challenge
FRR False Rejection Rate
FRVT Face Recognition Vendor Test
FTE Failure to Enrol rate
FTA Failure to Acquire rate

**I**
IAFIS Integrated Automated Fingerprint Identification System
ICAO International Civil Aviation Organisation
ICT Information and Communication Technologies
IMI Indirect Medical Implication
IPR Intellectual Property Rights
IR Infra-Red
ISSOL Interpol Standard Set Of Loci
IST Information Society Technologies
IT Information Technologies

**L**
LED Light Emitting Diode

**M**
MRTD Machine Readable Travel Document

**N**
NAFI National Automated Fingerprint Identification system

**P**

| | |
|---|---|
| PC | Personal Computer |
| PCR | Polymerase Chain Reaction |
| PDA | Personal Digital Assistant |
| PIN | Personal Identification Number |

**R**

| | |
|---|---|
| RFID | Radio Frequency Identification |
| RFLP | Restriction Fragment Length Polymorphism |
| RMP | Probability Random Match |
| ROC | Receiver Operating Characteristic |
| RTD | Research and Technology Development |

**S**

| | |
|---|---|
| SELT | Social, Economic, Legal and Technological |
| STR | Short Tandem Repeats |

**U**

| | |
|---|---|
| UK | United Kingdom |
| UAE | United Arab Emirates |
| US | United States |
| UV | Ultra-Violet |

**V**

| | |
|---|---|
| VNTR | Variable Number of Tandem Repeats |
| VWP | Visa Waiver Programme |