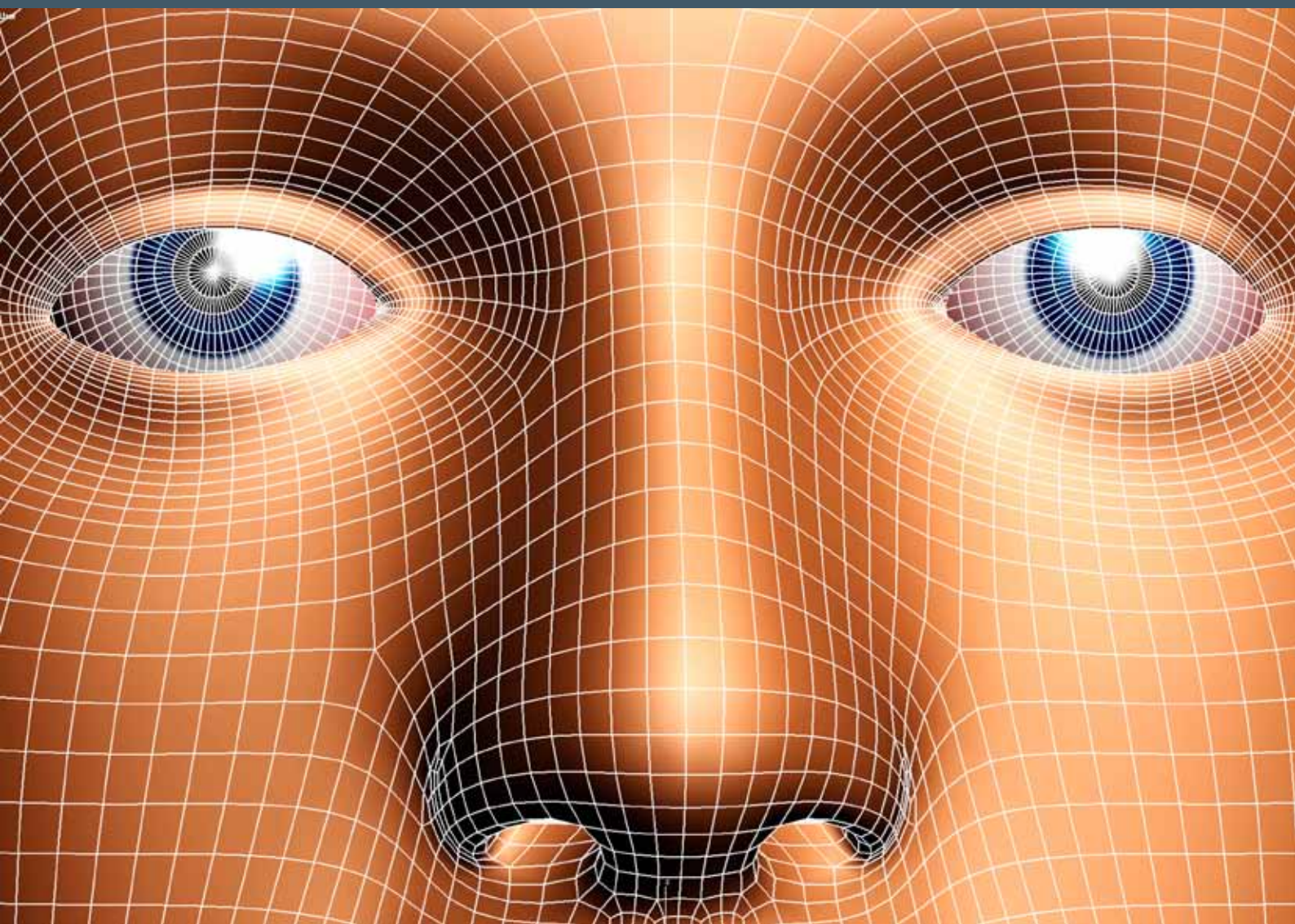


BIOMETRICS: ENHANCING SECURITY OR INVADING PRIVACY?

PROCEEDINGS OF THE IRISH COUNCIL FOR BIOETHICS' CONFERENCE
26TH NOVEMBER 2008, DUBLIN



Published by



The Irish Council for Bioethics
1 Ormond Quay Lower
Dublin 1.

Tel: +353 1 878 3051

E-mail: info@bioethics.ie

Website: www.bioethics.ie

© Irish Council for Bioethics 2009

All or part of this publication may be reproduced without further permission, provided the source is acknowledged. *Biometrics: Enhancing Security or Invading Privacy? Proceedings of the Irish Council for Bioethics' Conference, 26th November 2008, Dublin.*

Published by the Irish Council for Bioethics, Dublin.

Cover image: Pasieka/Science Photo Library

FOREWORD

Currently, biometric information is being used for numerous purposes, such as civil and criminal identification, surveillance and screening, e-Health, e-Commerce and e-Government. The use of biometric systems and applications raises a number of ethical questions with regard to human dignity and identity (individuality), as well as basic rights such as privacy, autonomy, bodily integrity, and in the case of criminal identification, due process.

In general, the issues that arise are not with the use of biometric technologies *per se* but in how they are applied and how the resulting information is dealt with. Considering the continuing developments in biometric technologies, the increasing incidences of their deployment and the diversity of their applications, the Irish Council for Bioethics (ICB) decided to hold a conference to examine some of the ethical issues surrounding the collection, use and storage of biometric information. The conference also provided the invited audience of politicians, civil servants, legislators and academics with an introduction to biometric technologies, as well as an outline of the main privacy and data protection concerns relating to biometrics. During the presentations and subsequent discussions a number of common themes were identified, in particular; how and why biometric technologies are being implemented, the link between biometrics and identity, and the importance of privacy in relation to biometric information.

Biometric technologies are considered capable of offering stronger authentication of who an individual is than traditional methods of identification. This premise is the basis of the three main factors behind the increasing use and deployment of biometric technologies namely that, this technology offers increased security, efficiency and convenience for the users and operators of such systems. The number, scope and functions of biometric applications are increasing, particularly government-based systems. However, whether it is a government, civil or commercially based biometric application, certain considerations are needed when designing and implementing such an application. For example, what is the purpose of the proposed application? What biometric modality will be used and how will this be collected? Will it be a verification-based or an identification-based system, since identification-based systems require the use of a centralised database? How will the collected information be stored and who will have access to it? The answers to these and other questions will help to clarify the potential challenges and concerns that could arise, as well as highlighting how such problems can be overcome or minimised.

One concern relating to the use of biometric information stems from the indelible link this information provides to an individual's identity. A person's identity has traditionally been interconnected with his or her physical, behavioural, biographical and cultural information. Identification using biometrics removes the more personal and biographical dimension of identity, instead distilling identity down to one or more particular features of the body. However, such body-based identification has both positive and negative implications. From a negative perspective, an individual's identity could be reduced to separate pieces of information, by which he/she could be categorised. The informatisation of the body in this way is often seen as diminishing one's human identity from the standpoint of the individual for whom many more and diverse characteristics are deemed essential to their personal identity.

On the other hand, biometrics could also help to empower and protect people precisely because it can provide a reliable means of identification. For example, in order to administer and provide services to its citizens a government requires these individuals to be identifiable. However, in certain developing countries many people, particularly children, lack adequate identity documents. Biometrics could, thus, offer a more reliable means of identifying these individuals. In addition, by enabling the separation of biographical and other personal information from the identifying information (i.e. the body), biometrics could help people to maintain some degree of anonymity and privacy in their lives and activities, particularly in today's digital and networked societies.

However, while an individual's right to privacy is well recognised in numerous pieces of legislation, both nationally and internationally, the potential negative impact biometrics could have on personal privacy was highlighted as one of the major concerns surrounding the use of this technology. Given the ease with which biometric and other personal information can now be collected, stored and processed, the appropriate use, management and protection of such information were considered to be of paramount concern. For example, biometric information should only be used to meet a specified purpose; should be obtained and processed fairly; should be stored securely; and should be kept up-to-date. Notwithstanding, identifying the promised benefits and anticipated risks involved, any assessment of the proportionality of a particular biometric application also depends on that application upholding the principles of data protection.

The ICB would like to thank each of the speakers for giving of their time and expertise to provide an insight into the evolving and emerging subject of biometrics as well as highlighting some of the ethical and social issues associated with it. Given the increasing implementation of biometrics applications, the ICB hopes that this proceedings document will help to inform both policymakers and the general public of the potential opportunities and challenges offered by this technology.



Dr. Dolores Dooley
Chairperson
Irish Council for Bioethics

TABLE OF CONTENTS

Conference Programme	2
Biographical Information on Conference Speakers	3
Biometrics and (E-) Identity	5
Implementation, Limitations and Future of Biometrics	7
The Ethical and Social Implications of Biometric Technologies	12
Biometrics: The Impact on Privacy	15
Summary Remarks and General Discussion	18

CONFERENCE PROGRAMME

9:30 – 10:00	Conference Registration Tea/Coffee
10:00 – 10:20	Biometrics and (E-) Identity Mr. Max Snijder – Director of the European Biometrics Group in the Netherlands, CEO European Biometrics Forum
10:20 – 10:30	Questions
10:30 – 10:50	Implementation, Limitations and Future of Biometrics Mr. Peter Hanel – Director European Biometrics Forum, Biometric Identity Management and Security Solutions Division, Motorola
10:50 – 11:00	Questions
11:00 – 11:20	Tea/Coffee
11:20 – 11:50	The Ethical and Social Implications of Biometric Technologies Professor Emilio Mordini – Director of the Centre for Science, Society and Citizenship, Scientific Co-ordinator, Biometrics Identification Technology Ethics (BITE) Project.
11:50 – 12:00	Questions
12:00 – 12:20	Biometrics: The Impact on Privacy Mr. Billy Hawkes – Data Protection Commissioner of Ireland
12:20 – 12:30	Questions
12:30 – 13:00	Summary Remarks and General Discussion

BIOGRAPHICAL INFORMATION ON CONFERENCE SPEAKERS

Mr. Max Snijder – Director of the European Biometrics Group in the Netherlands, CEO of the European Biometrics Forum

Mr. Max Snijder is one of the leading independent biometrics experts in Europe. His practical experience and integrated approach has led to an overall view on the biometrics business.

After a career as an entrepreneur in the not-for-profit sector Mr. Snijder became one of the pioneers of biometrics in the Netherlands. After several years of extensive experience with numerous biometric projects like Privium at Schiphol Airport, he founded the Biometric Expertise Group in 2004 with the purpose of bringing together the fragmented knowledge and experience in the field of biometrics.

Mr. Snijder is involved in several projects and consortia, ranging from passports and visas to large-scale watch list applications and physical access control. Today, Mr. Snijder is involved in the key areas of the biometrics business. On a European level he is involved in numerous workshops, committees and expert groups. As an independent consultant he is frequently hired to review, supervise and monitor projects that involve biometrics. He works for several European Union Member States' governments as well as for the European Commission.

Mr. Snijder is a member of several high level bodies, like the Consortium on Security and Technology of the EastWest Institute, The Porvoo Group, the CEN Working Group on Integrated Border Management, CEN Biometric Focus Group. He is a founding member of the International Federation for Information Processing (IFIP) Working Group on Identity Management. He is a member of the scientific committee of the World eID Conference.

As CEO of the European Biometrics Forum Mr. Snijder is chairman of the International Biometrics Advisory Council and the annual European Biometrics Research Seminar.

Mr. Peter Hanel – Director European Biometrics Forum, Biometric Identity Management and Security Solutions Division, Motorola

Mr. Peter Hanel worked for more than 4 years (until late 2005) within the European Commission's Directorate-General for Justice, Freedom and Security.

His tasks were the co-ordination, planning and implementation of large-scale Pan European IT projects such as EURODAC, the second-generation SIS (Schengen Information System) and the future VIS (Visa Information System). At the same time Mr. Hanel dealt with the biometric aspects of these projects, the general biometric co-ordination in the area of Justice, Freedom and Security and possible synergies of IT structures between European authorities. In this context, Mr. Hanel worked on further subjects such as the EU passport, the biometric visa, EU funded research and development programmes related to the protection of critical infrastructure and public safety and setting requirements for combating illegal trafficking and terrorism.

Mr. Hanel has a background with the Federal Ministry of the Interior in Austria where he worked on a variety of issues related to criminal, asylum and immigration issues for some 20 years. Additional experience as an early member of the Europol project management board, numerous Interpol and EU working groups complement his familiarity in these areas.

His current tasks are following the European requirements and trends, in particular to advise industry and its customers in meeting European policy and national needs.

Professor Emilio Mordini – Director of the Centre for Science, Society and Citizenship, Scientific Co-ordinator, Biometrics Identification Technology Ethics (BITE) Project

Professor Emilio Mordini is a medical doctor from the Sapienza University in Rome, and has a Masters Degree in Philosophy from the Pontifical University of Saint Thomas Aquinas in Rome. Since March 2002 he has been Managing Director of the Centre for Science, Society and Citizenship (CSSC) an independent, interdisciplinary research centre that addresses ethical and policy issues in healthcare and biomedical research. Professor Mordini is a certified scientific expert of the Italian Ministry of Education, University and Research.

Professor Mordini is a practising psychiatrist (sub specialised in psychodynamic psychotherapy) and he is an ordinary member of the Italian Association of Psychiatry. Since 1996 he has been a member of the Bioethical Commission of the National Research Council (CNR) where he currently serves as scientific secretary. He is also member of the Bioethical Commission of the Medical Association of Rome. He is co-ordinator of the Psychiatric Network of the International Association of Bioethics and a member of the executive council of the Association for the Advancement of Psychiatry and Philosophy (AAPP).

Professor Mordini has co-ordinated various research projects in bioethics both at Italian and European level, including “Brain Elsa: ethical, legal, and social aspects of brain research”, “EURO ELSAV: ethical, legal and social aspects of vaccine research and vaccination policies in Europe” and “Big – Bioethical Implication of Globalisation Processes”. He is past treasurer and past secretary of the European Association of Centres of Medical Ethics (EACME). He has also served as a member of the board of directors of the International Association of Bioethics (IAB).

Mr. Billy Hawkes – Data Protection Commissioner of Ireland

Mr. Billy Hawkes was appointed by the Government as Data Protection Commissioner in July 2005 for a 5-year term.

Prior to his appointment, he worked as a civil servant in various Government departments, most recently Finance, Enterprise, Trade and Employment and Foreign Affairs.

BIOMETRICS AND (E-) IDENTITY

**Mr. Max Snijder, Director of the European Biometrics Group in the Netherlands,
CEO of the European Biometrics Forum**

Verification techniques are bifurcating into "identifying" versus "anonymous" biometrics, raising new questions and challenges.

Most of us associate biometrics with on-site identification: storing fingerprints on paper and ink and then the human inspection of latent fingerprints at a physical, usually well protected, secure location. But we are now moving from a "physical" environment, where identification has been the core value of biometrics, to a new domain where biometrics are a fully digital process. This makes it possible to store reference data at any place and to do millions of matches in a matter of seconds. Typically, biometrics have entailed the following: establishing the identity of a person about whom there is little or no information and using fingerprints to trace a person's identity. This is still the widest use of biometrics across the globe.

The next step of biometric evolution now unfolding is verification. We will soon see this at border control checkpoints using electronic passports. Nonetheless, the biometrics are still stored at a protected location and controlled by the rightful owner of the passport. The claimed identity is verified by a one-to-one check of the biometrics stored in the protected chip. This is a situation characterised by the physical aspects of the process: you have to cooperate by offering your passport to a border control officer.

Yet the link between the biometrics and the identity of the person is less evident. The passport's biometrics are indirectly used to verify identity and not to create a direct link between biometrics and identity. In other words, the biometric reference data are made available to facilitate a single, one-off check, yet they are retained by the individual.

The next stage of development will be biometrics with no link to identity at all, used for purposes of authentication only. In the most extreme case a service provider does not even need to know which biometrics are being used or even whose biometric data are used. Why? Because biometrics are becoming a secret key.

But how secret can biometrics be? A face is public information. Using a face finder on a web-search engine can reveal a person's identity within minutes, if not seconds. The same process applies to typing in a name, which could generate multiple pictures of a face, including a lot of personal information. As for fingerprints, these can be traced and "stolen" because they are left in multiple locations.

There are now enough freely available databases where unintended links to a given identity can be established. New solutions are required for this problem. The choice of biometrics used (traceable, detectable) is one of them, as well as the way that reference data is stored and the performance level of live detection by sensors (automated or with human supervision).

Some biometrics such as the human iris obviously leave no fingerprint-like trace or are very difficult to “spoof” or fake. The newly available vein pattern recognition technologies are another good example. But the matter of storing reference data and doing the matching function still remain: usually we will always have to revert the biometric reference from whatever encrypted domain into the original image or biometric template in order to use it for matching.

New technologies will not only strengthen the protection of biometric data but also make it possible for their owner to control the storage and matching of his biometric data. From a single biometric (e.g. one finger) these technologies can generate a non-biometric derivative and multiple unique (and disposable) biometric “keys” for carrying out the matching function.

This will make biometrics revocable (in case a key is lost or stolen) and protected against being used as “pointers” to other databases. This “biometric encryption” introduces new horizons for a correct and beneficial use of biometrics in more complex operating environments such as the Internet and large federated systems.

Paradoxically, biometric encryption has the potential to make both biometric data and the matching function anonymous by never exposing a person’s original biometric information to fraud or manipulation. One of the major providers of this kind of technology is priv-ID, a spin-off venture from the laboratories of Philips Research in the Netherlands, though others are developing similar applications as well.

Indeed, we can now clearly see the two emerging faces of biometrics: identifying biometrics for establishing or verifying identity where the link to identity is key and “un-identifying” biometrics – or so-called anonymous biometrics – where a link to identity should be strictly avoided.

Given that these two “faces” will exist in parallel to one another and could get easily mixed up with each other, a new level of thinking about biometrics is needed: one that defines the policies and guidelines required so that both kinds of technology can be used, without one compromising the other.

Left to right:
Professor Emilio Mordini,
Dr. Dolores Dooley (ICB
Chair), Mr. Max Snijder
and Mr. Peter Hanel



IMPLEMENTATION, LIMITATIONS AND FUTURE OF BIOMETRICS

Mr. Peter Hanel, Director, European Biometrics Forum, Biometrics Identity Management and Security Solutions Division, Motorola

Biometrics has become a buzzword in recent years. Although this term is being used in many instances, when it comes to security and public safety, there are often certain misunderstandings regarding where and how to use biometrics. At the same time, there are high expectations and a sanguine belief that biometrics will solve all the problems relating to false identification.

Apart from the well-known drivers of biometrics such as September 11th 2001 and the London and Madrid bombings, there are a number of other reasons why names and descriptions of people are no longer viewed as an accurate enough method of identification.

THE GENERAL PROBLEM WITH TRADITIONAL FORMS OF IDENTIFICATION

People may have either very simple or very complicated names, depending on the region of the world they hail from. In early times and when smaller communities existed, people used only first names or even only nicknames. Later surnames were added to the first name. In some cultures the father's first name is adjoined, in others the mother's name is appended. Moreover, legislation allows people to use completely different names in parallel to their "real" name and marriages often result in new name combinations.

Another dilemma is the transliteration of non-Latin names. There are various standards, and depending on the use, the Latin outcome differs. The International Civil Aviation Organisation (ICAO) has recommended a standardised system of transliteration but, unfortunately, this applies only to travel documents.

Finally, whatever standard of names may be used, the mobility of people results in a mixture of name combinations, often not known to those who look at a document. Frequent names such as Mohamed, Smith, Popov and Zhang make it almost impossible to differentiate between persons as long as one does not have additional information like a photograph or other personal description. Furthermore, how do descriptions such as tall, strong-build, black hair or brown eyes help in real life? Dates of birth may be as inaccurately recorded as the places of birth. In many cases, particularly in the developing world, we only know the year of birth. Identification problems might also arise where villages or towns (again in developing countries) have altered their names due to political changes.

All this has demanded more distinctive identifiers, which would not change, which one would always carry with oneself and, which ideally would be unique to each person. Biometric technologies, which have already been used in the forensic sector to identify suspected criminals, have been further developed and now promise greater identification performance by computers than humans.

Currently the comparison of fingerprints seems to be the most developed and utilised technology, however, huge progress has been made in face recognition and iris comparison technologies. Different biometrics are also being tested in combination with each other (multimodal) in order to increase accuracy. Consequently, academic and industrial research is further working on voice recognition, gait analysis, real-time DNA comparison and various other biometric tools. Industry is permanently improving matching algorithms, manufacturing new devices for biometric capture and building highly secure databases where biometric data can be stored.

While this progress is fascinating, it also provokes a number of questions:

- **Where and how will biometric comparisons be used?** Is it just to prove someone's identity (e.g. if he/she presents a travel document) or will we retrieve data from central databases to match with someone we have in front of us? In any case, we need to capture the data and register the person in advance and ensure that the information is correct and up-to-date.
- **Will people always know when their biometrics are being captured and compared with data stored somewhere?** In the case of presenting a travel document, a person is actively involved because his/her data is stored on a radio frequency identification chip embedded in the document and the comparison takes place only locally. When a person passes an electronic gate (e.g. access control for staff), which may be supported by iris recognition, the person will have to look into a camera. In this instance, the comparison will take place with data stored in a local database.

Considering the fact that more and more video cameras are being put in public places, the question arises whether individuals are aware of such surveillance and if so, are they aware of how the data is being used after collection? In certain conditions, biometric technology is capable of extracting good quality facial images from a crowd and comparing them with data in background databases. However, there is some ambiguity regarding what kind of background databases are being used, who is responsible for their content and, more importantly, what happens if the computer system claims to have found a match. No biometric system can provide a 100% accurate matching rate. This is consequent of several quality factors, for example, shades on the face due to poor lighting conditions will not result in the same outcome as a photograph being taken in a photo booth. In relation to fingerprints, the quality of ridges on the fingers are influenced by age, the person's profession and even by the person's origin.

- **Once we concentrate on the physical appearance of a person, what importance will names have in the future?** Will we continue to use identification documents or will we have chips implanted into ourselves, like some of the patrons of nightclubs in Amsterdam or Barcelona have already done (in return for a free drink)?
- **Who is able to control the transfer of data?** In Europe we have a data protection legislative framework, which enables people to have unlawfully stored data deleted or to have inaccurate data corrected. Other data protection principles, which are upheld are that, data can only be stored for as long as they are needed, can only be collected for a limited purpose and that data storage has to be appropriate and not excessive.

Although these principles apply to Europe and many countries, they do not apply to all regions of the world. For example, it is hard to imagine how inaccurate data would be corrected in developing countries in South America.

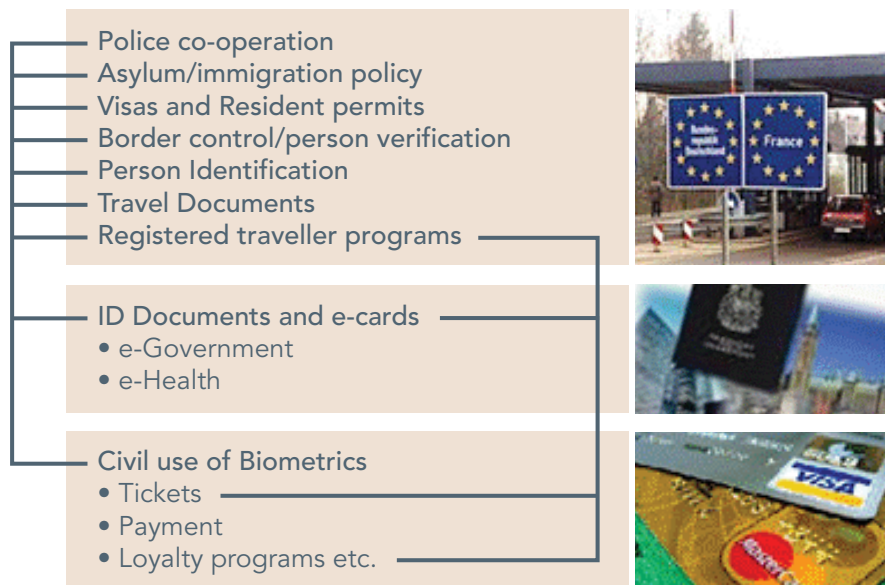
One more aspect, which must be dealt with is the community of physically impaired individuals. If someone is not in a position to provide certain biometric data, would this result in preferential treatment or would the person be deprived of services? Would criminals or fraudsters try to cheat the systems by claiming disability?

Unless these questions can be solved and the public protected from any misuse of biometric data, the impact on society will be huge. Law enforcement databases and civil applications have grown and the amount of collated information is enormous. Unfortunately, stored data are not always accurate and up-to-date. For instance, in one database the information might be five years old, whereas the same data in another database might only be three months old. Information is often used for similar purposes although the legal basis might be completely different. For example, application for a driving licence is a civil process. Typically, the document is issued by a local or central administration depending on the country. The police usually undertake the control of driving licences and this raises some questions:

- Should the driving licence office have access to police data? Maybe the person is a wanted or suspected criminal and the issuing of a driving licence would make that person even more mobile?
- Should the driving licence office transfer its most recent data to any other law enforcement authority? A person's photograph stored in an immigration database may be outdated, whereas a new photo taken for the purpose of getting a driving licence would now be available.

Banks demand the presentation of identity documents when one opens a bank account. How can a bank check if a document is genuine or if the person presenting the document is the legal owner? Would it help in combating money laundering if banks had access to civil or law enforcement document registers?

One could argue that the correction and alignment of data should be performed where necessary. Given that multiple databases exist in parallel, the situation is fairly complicated. There are logical links between several information sources although the physical link may be prohibited.



Links between biometric information sources can help to keep data more accurate and up-to-date. This would be a definitive advantage for the person concerned. The risk to favour a misuse of information and to foster unwanted side effects in terms of a "transparent individual" may increase at the same time.

Discussions on the use of biometrics are ongoing. Industry is working on new developments and decision makers are struggling with a range of different information relating to whether the introduction of biometrics would be beneficial or not. Depending on the size of biometric systems and the number of persons registered, the necessary investment ranges from low to very high. The international aspect raises difficulties for governments because there is no harmonisation of legislation and in some countries there is no legislation whatsoever. Where a legislative framework does exist its terms may be too broad and ambiguous.

The following list, although not comprehensive, may help to find balance when introducing biometric technology in an environment:

- Once you start considering the use of biometrics ensure that you use a common terminology. Terms like "identification", "verification" and "false rejection rate" are just a few examples of fundamental misinterpretation.
- Define exactly the purpose and the accuracy you really need. Be honest by saying what the current accuracy is (e.g. 80%) and define the accuracy you are confident with. In technical and budgetary terms there is quite a difference between 98% and 99.9%. One has to find the right balance between what can be done and what is reasonable.
- Be aware that biometric comparisons are never 100% precise. The combination of different biometric identifiers may boost accuracy and minimise "wrong hits". On the other hand, it requires a lot of preparation at the enrolment stage and for providing a convenient infrastructure. The roll-out and maintenance of equipment may also result in significant logistical challenges.

- Define where interoperability is needed. In a closed setting of a building it may be dispensable, whereas in a country-wide or international environment it will be essential.
- Go for pilots. There is no one-for-all solution. Each situation is different and one needs to learn where biased circumstances apply.
- Communicate with others. One of the obstacles in this area is the limited exchange of experience. Pilots are established here and there and results are promoted in different media. The circumstances, the group and number of persons involved in the pilot may be completely different (e.g. 50 factory workers, 100 desk clerks, 3,000 members of the public). In some circumstances, spectators may be confused by hearing that a certain biometric technology performs very well in one country, whereas in another country the same technology is reported to be insufficient.
- Involve independent consultancy. It is legitimate that industry wants to sell their products as it has invested a lot of money to develop suitable products. On the other hand, customers have to protect their investment as well. Locking into a certain technology may cause significant trouble at a later stage, aside from loss of money and reputation, when a particular solution has to be replaced.
- Use the European Biometric Forum (EBF) as a mediator and European-wide platform in bringing together academics, industry and users.
- Inform the persons concerned. People usually do not know what biometric technology is and how it will be used in their environment. Speculations range from "modern and convenient" to "total control and mental anxiety". Explain what kind of data are going to be stored and the exact purpose for collecting and storing it. Inform people how long their data will be kept and who will have access to this information.
- Always consider a fallback solution to guarantee business continuity. There are various reasons why a biometric system may not function properly. For example, a system fails and has no backup system to switch over to or other circumstances like electricity cuts, or fire or water damage.

Left to right:
Professor Emilio Mordini,
Mr. Peter Hanel and
Mr. Max Snijder



THE ETHICAL AND SOCIAL IMPLICATIONS OF BIOMETRIC TECHNOLOGIES

**Professor Emilio Mordini, Director, Centre for Science, Society and Citizenship;
Scientific Co-ordinator, Biometrics Identification Technology Ethics (BITE) Project**

There is an inextricable link between the construction of the private sphere and the public recognition of individuals. The definition of the private sphere is part of the overall definition of one's identity. We exist as individuals as far as we are able to represent ourselves as autonomous subjects. Most probably the need for recognition schemes started at the very beginning of human civilisation, with the first urban societies in the Middle East and China, when societies became so complex as to require frequent interactions between people who did not know each other.¹ Obviously, most people used to live within the borders of their village or town and did not need any identifier. Yet persons that travelled outside of the confines of their homes (e.g. military, sailors, traders) needed to be recognised and to recognise.

A recorded description of physical appearances (e.g. body size and shape, skin and hair colour, face shape, any physical deformity or particularity, wrinkles and scars etc.) was probably the first way to recognise someone else, and to be recognised. However, the body gets older, faces change, voices can be altered, scars fade. Consequently, a brief description of physical appearances alone probably became inadequate as human interactions became more and more frequent and complex. The first recognition schemes were probably based on artificial and more permanent body modifications (e.g. branding, tattooing, scarifications etc.) and analogical identifiers. An analogical identifier is a token, a symbol, which could be both a physical object (e.g. a pass, a seal, a ring etc.) or a mental content (e.g. a password, a memory, a poem etc.) which may be linked with only an individual or a category of individuals. The term "symbol" means "to bring together" and originally the Greek word for "symbol" meant a plank, which was broken, in order for friends to recognise each other by mail. For example, if a messenger came from a friend to ask for help, he was to bring the second part of the broken plank, and if it matched the first part, then indeed it was a meeting with a friend.

The Roman Empire was the first cosmopolitan society in the west and was also the first example of a universal system for people recognition, which was mainly based on badges and written documents. In Middle Age Europe - where the majority of the population never went outside the immediate area of their home or villages - individuals were chiefly identified through passes and safe-conducts issued by religious and civil authorities. The authenticity of these documents was chiefly verified by seals and handwriting.

The birth of large-scale societies and the increased mobility associated with urbanisation imposed new recognition schemes. The first passports were issued in France by Louis XIV and by the end of the 17th century passports and ID documents had become standard. Yet only by the end of the 19th century, was a true passport system for controlling the movement of people between states universally established. Various ID documents, passes, safe-conducts, seals and other tokens remained the main instruments to ascertain peoples' identities in everyday life until the outbreak of World War I. In the 20th century,

¹ Caplan J, Torpey J, eds, 2001, *Documenting Individual Identity*, (Princeton University Press, 2001)

passports and ID cards - incorporating face photography, and in some cases also fingerprints - became the primary tool for people recognition within states, at least in those countries that made ID documents mandatory. Finally in the late 1960s Automatic Identification and Data Capture Technologies (AIDC)² emerged as the first true innovation since the birth of photographic passports. However, it took some time because people understood that biometrics had a very special status among other AIDCs.

Biometrics could overcome – or at least have the potential to overcome - all previous human recognition schemes. Biometrics do not imply any artificial modification of the body as tattoos do. Neither are biometric systems based on analogical representations (biometrics are not icons). A biometric system measures body parts, physiological and behavioural processes. Biometric systems generate digitalised representations of personal characteristics, say, digitalised tokens which link the individual observed here and now with reference data stored in a document, such as a travel document, or in a database. This is the real novelty of biometrics and what makes this technology revolutionary. For the first time in the history of the human species, human beings have really enhanced their capacity for recognising other people by amplifying - through technical devices - their natural, physiological, recognition scheme, which is based on the appreciation of a complex web of physical and behavioural appearances. Biometric technology aims to solidify this scheme, which would naturally be fluctuating, liquid, unpredictable, even arbitrary.³

Biometric technologies also promise to liberate citizens from the “tyranny” of nation-states and create a new global, decentralised, rhizomatic scheme for personal recognition. Today states keep in their hands the power to establish national identities, to fix genders, names, surnames, parental relationships and to assign rights and obligations to individual subjects according to the names written on their identity documents. In his fascinating book on the history of passports, John Torpey argues, “modern states, and the international state system of which they are a part, have expropriated from individuals and private entities the legitimate means of movement”.⁴ Beginning with the French Revolution there has been an indivisible unity of national citizenship and individual recognition. The Declaration of Human Rights has created the modern concept of citizenship. The new democratic order is based on a direct, unmediated, relationship with the citizen. Universal rights and individual identity are the two sides of the same coin. This new citizen is an unmarked individual who is uniquely and reliably distinguishable as an inhabitant of a nation-state, and not as a member of a guild, village, manor or parish. Other identity elements, which have been important in the past (e.g. religion, ethnicity, race, cast, etc.), become, at least theoretically, less and less important. One of the main tasks (and sources of power) of modern states is to register birth certificates, to secure their authenticity, and fix citizenship accordingly.

According to Torpey nation-states have generated “the worldwide development of techniques for uniquely and unambiguously identifying each and every person on the face of the globe, from birth to death; the construction of bureaucracies designed to implement this regime of identification and to scrutinise persons and documents in order to verify identities; and the creation of a body of legal norms

2 AIDC encompasses a diverse group of technologies (e.g. RFID, matrix bar code, biometrics, smart cards, OCR and magnetic strips, etc.) and systems that automate the capture and communication of data. AIDC technologies can be used both to identify items (as bar codes in a retail product) and to recognise, track, and monitor individuals.

3 J. Lacan, the French psychoanalyst, speaks of the *instant du regard* (the instant of the gaze) as the moment in which recognition and understanding merge.

4 Torpey, J, *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge University Press 2000) p4.

designed to adjudicate claims by individuals to enter into particular spaces and territories”.⁵ This state of affairs could now be radically challenged. The tourist who wants to use the same credit card in any part of the globe, the asylum seeker who wants to access social benefits in his/her host country, the banker who moves huge amounts of money from one stock market to another in real-time, they all have the same need. They must prove their identities, they must be certain of others’ identities. However, they can hardly rely on traditional means for proving identities such as birth certificates, passports or ID cards, etc. because these schemes are not dependable enough in most parts of the world and are unfit for global digital networks. Moreover, biometric systems are the only large-scale identification systems that could also be run by small private actors and independent agencies as well as large governmental structures. This makes a global system for personal recognition possible, which would be closer to the Internet than to the Leviathan. The fear that biometrics might lead to a unique identifier - a digital cage from which no one could ever escape – is probably misplaced. On the contrary biometrics permit the creation of separate digital IDs for particular purposes, by applying different algorithms to the same biometric characteristic. As well as providing the appropriate level of security for each application, this makes it much easier to revoke a biometric template and issue the user with a new one if their digital identity becomes corrupted or is stolen. Furthermore, these processes do not need cumbersome, centralised, structures but can be easily implemented by a web of local authorities, as it has been indirectly demonstrated by the astonishing penetration of biometric technology and applications in Asian and African markets.

Left to right:
Mr. Stephen McMahon
(ICB), Mr. Raymond Byrne
(Law Reform Commission)
and Professor Santiago Sia
(Milltown Institute)



⁵ *Ibid.* p7

BIOMETRICS: THE IMPACT ON PRIVACY

Mr. Billy Hawkes, Data Protection Commissioner of Ireland

Biometrics, which have a unique ability to identify people based on their physiological characteristics, are increasingly being used by governments as well as private enterprise. Their use gives rise to concerns in relation to data protection and the broader right to privacy.

The right to privacy is protected (albeit implicitly) under Article 40.3.1 of the *Constitution of Ireland*, which states that, "the State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen". It is also explicitly protected under Article 8 of the 1950 *European Convention on Human Rights and Fundamental Freedoms* (ECHR), which states that, "everyone has the right to respect for his private and family life, his home and his correspondence". Article 8 of the ECHR also places strict constraints on the extent to which the State or other bodies can limit the right to privacy. The ECHR is now, indirectly, part of Irish law by virtue of the *European Convention on Human Rights Act 2003*.

In 1981, due to the increasing use of computers for administrative purposes, the Council of Europe decided to introduce a piece of legislation to deal specifically with data protection. The *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* forms the basis of Ireland's *Data Protection Act 1988*.

The *Charter of Fundamental Rights of the European Union 2000* contains a specific article governing the protection of personal data. Article 8 states that, everyone has the right to the protection of their personal data; that data must be processed fairly and on the basis of consent or some other legitimate basis laid down by law; that people have the right to access their stored data and to have it corrected or updated where necessary; and that compliance with the rules be subject to oversight by an independent authority. Data protection will also be enshrined as one of the obligations of the *Lisbon Treaty*, if all EU Member States ratify it.

There are two EU Directives, which deal specifically with data protection. The first is *Directive 95/46/EC Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* and the second is *Directive 2000/58/EC Privacy and Electronic Communications*. These Directives are given effect in Irish law through the *Data Protection Acts 1988 and 2003* and the *EC Electronic Privacy Regulations 2003*. The *Disability Act 2005* deals with the processing of genetic data and states that such sensitive data cannot be processed without consent; that processing genetic data is prohibited in the case of insurance policies, pension and mortgages and is subject to prior approval from the Office of the Data Protection Commissioner in the case of employment.

The Irish data protection acts define personal data as, “data relating to a living individual who is or who can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller”. According to the legislation, personal data:

1. shall be obtained for one or more specified, explicit and legitimate purposes;
2. shall not be further processed in a manner incompatible with the original purposes;
3. shall be adequate, relevant and not excessive;
4. shall not be kept longer than is necessary; and
5. shall not be disclosed to any third party except in a manner compatible with the original purpose.

The acts also require that data controllers implement appropriate security measures against unauthorised access, alteration, disclosure or destruction of data. Irish data protection legislation also provides special protection for sensitive data, i.e. data, which can give indications of characteristics such as physical or mental health and racial origin.

There is consensus at a European level that biometrics constitute personal data and, in some cases, may constitute sensitive personal data because of the possibility that sensitive personal information can be deduced from particular biometrics. Therefore, proportionality is a key concern for data protection practitioners as it is important that any interference with privacy rights should be proportional to the objectives being pursued (i.e. that the benefits of implementing a biometrics system will outweigh any risks to privacy rights).

Where the use of biometrics is found to be justified on proportionality grounds, it is recommended that data be stored on a chip or token, which is under the control of the user (e.g. a smartcard as opposed to being stored on a central database). Encryption (i.e. a non-reversible algorithm) as opposed to storing a complete biometric profile, is also recommended. These measures would help to ensure that privacy is maintained.

There are a number of risks associated with using biometric technologies in order to identify individuals. Personal information might be shared with third parties, with or without a person’s knowledge, in a practice known as “function creep”. For instance, the European EURODAC system was set up to assist Member States in dealing with claims for asylum. EURODAC allows a Member State to check whether an asylum seeker has previously sought asylum from another European country. This central database of fingerprints will now also be accessible for broader immigration and law enforcement purposes. There are also risks related to the incidence of “false certainties”. Biometric technologies are not always completely accurate and a person may also be incorrectly identified as someone else. Proving one’s correct identity could be very difficult, which would be particularly problematic if one was falsely identified as a criminal. Finally there is a risk that, if the use of biometrics became the norm, especially among children, it could lead to a society based on distrust.

The State use of biometrics raises a number of other data privacy concerns. The US visitor and immigration programme (US-VISIT) and the proposed EU immigration programme require visitors entering their borders to have fingerprints and photographs taken. The information is then compared

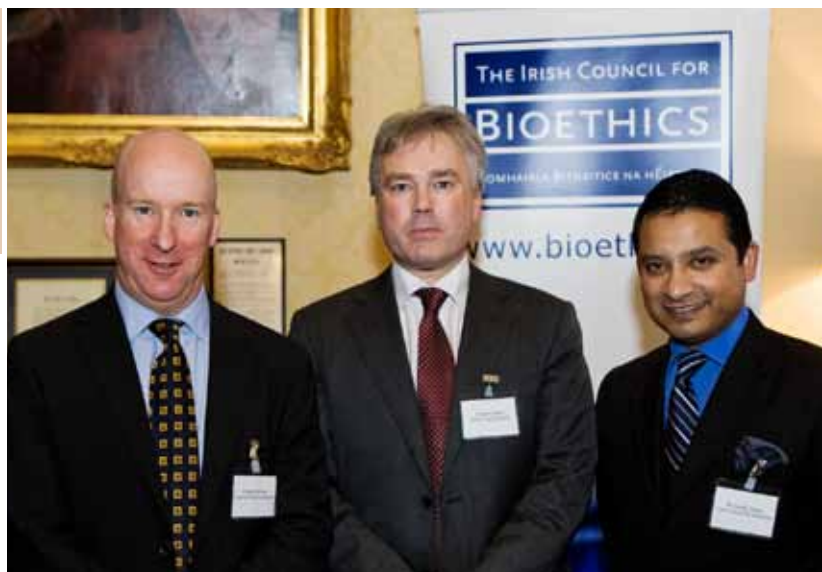
with profiles stored on a database of known criminals and suspected terrorists. Typically the State use of biometrics involves long (possibly indefinite) periods of retention of data and its up-take is becoming increasingly obligatory for citizens. For example, one cannot enter the US unless one abides by the US-VISIT requirement of providing fingerprints and a photograph. Consequently, there are concerns that we are heading towards creating a “Big Brother” society, where the State holds a substantial amount of information about individuals and is unwilling to grant services where biometrics are refused.

Many people view DNA as the “ultimate” form of biometric identifier. However, by virtue of its ability to reveal certain characteristics, such as health or predisposition to genetic diseases, DNA data is extremely sensitive. As aforementioned, the *Disability Act 2005* restricts the non-State use of DNA. However, a Bill currently under discussion at Government level, the *Criminal Justice (Forensic Sampling and Evidence) Bill 2007* would intensify the use of DNA by An Garda Síochána (Irish police). The Bill provides for the establishment of a forensic DNA database and states that DNA data taken from individuals, who are subsequently found to be innocent, can be retained indefinitely.

The Office of the Data Protection Commissioner has issued two sets of guidelines in relation to the use of biometric technologies: *Biometrics in the Workplace* and *Biometrics in Schools, Colleges and other Educational Institutions*. In terms of biometric use in the workplace, the guidelines recommend that a Privacy Impact Assessment be carried out to establish if the introduction of a biometric system would be proportionate. In relation to educational institutions, a more stringent approach is recommended, including the seeking of explicit written consent from students and, in the case of minors, from their parents.

Privacy, once lost – especially through the operation of law – is very hard to regain. Biometrics is a “frontier” issue for privacy in our society. It is essential that there be recognition of the risks involved in their use and enforcement of stringent safeguards surrounding such use.

Left to right:
Professor Alan Donnelly
(ICB), Professor Bert Gordijn
(DCU) and Mr. Asim A. Sheikh
BL (ICB Vice-Chair)



SUMMARY REMARKS AND GENERAL DISCUSSION

MR ASIM A. SHEIKH BL:

I'm going to open up the time now to the floor for questions, and then after that I'm going to ask our Chair Dolores Dooley to close today's session. So if anybody has any questions Paul has the mic and if I could ask you to speak into the mic please. Thank you.

QUESTION:

Hi I'm at DCU, but as you might hear from my accent I am originally from South Africa. So what I'd like to do is just preface my question with a statement of some scepticism, towards both Professor Mordini and I'm sorry I've forgotten the other speaker's name. Mr. Hanel, sorry about that, that biometrics will actually be beneficial for refugees, or people in the Third World, people in developing countries. I think Professor Mordini you pointed to the fact that 55% of sub Saharan South African children are not registered at the moment. Well one of the reasons for that is that we don't have offices, we don't have computers, people live many hundreds of kilometres away from very basic infrastructure. How on earth is biometric technology supposed to infiltrate such poverty stricken, resource deprived areas? The reason I say this, is because, I think one of the very interesting privacy issues and first of order issues here, we've got to be aware that this impacts on the developing world. The decisions that are taken here are going to place restrictions on, and unjust restrictions on, the people of the developing world.

ANSWER:

PROFESSOR EMILIO MORDINI:

South Africa is one of the countries more biometricised in the world. And if you analyse markets, apart from US market the most important markets, currently growing markets are Asia and Africa. And why it is very difficult to find, have, strong industry, in Africa of course, but even in small villages people have this one (Professor Mordini holds up a mobile phone) What does it mean? That we should try to change our perspective on technology? New technologies are light soft technology and they are affordable, more affordable than the hard industrial type technology of the past, of course I know that people are poor that they don't have computers but to set up a birth registration system, effective birth registration system, is more, more, more, expensive than to set up a biometrical network, registration network. Imagine what does it mean in terms of democratic organisation of people, training people, paying people, making them reliable because when you are an officer you issue birth certificate, you can sell birth certificate. It happens in a lot of places. So I don't think that, generally speaking, I agree with you, that technology is not the solution for the political problem. Political problems need political solutions but technology can change a landscape.

MR. MAX SNIJDER:

Maybe to add to that, I think it was South Africa where I was involved in a project, an early stage phase of a project of the World Bank. The World Bank wanted to dispense a certain amount of money to each citizen. I think it was Africa. Poor people living inside the country...I don't know exactly the details anymore but they decided not to dispense the money to the Government because then you know where the money goes. So they thought about a different way, and the way they had designed a system was, an ATM system, where people were enrolled with their iris or I don't know what they decided in the end, with the purpose of dispensing the money directly to those people but those people are not registered, so

that's exactly the problem and the biometrics just enabled it. That's just a very simple example. And I also know that some banks in Asia are using biometrics to give financial services to people who don't have a bank account with them. So there you have some very practical and pragmatic things, which biometrics can do. I'm not speaking about long-term consequences because you have to think about it, but it's just a very practical thing of solving these problems.

QUESTION:

Thank you very much for a very enjoyable morning. One of the issues, I think maybe one which hasn't been addressed, is not so much the use of the technology itself but actually where the information goes in terms of biometric data that's used. Now there maybe different rules for private industry as opposed to public industry but I haven't heard very much about what happens with the data that's derived from biometrics and how much there is consent for dealing with that. In that there is a model from the private side where you subscribe to a particular agency and you do or don't sign up as to whether your information is passed onto third parties or not. To my understanding, this doesn't necessarily apply in State circumstances that such information is necessarily going to be sent, yes or no to pass on, and I don't know how easy it is to find out information about where this data goes, how widely it is used, how widely it is shared, and whether there are limits on it in terms of the consents that people might give for the use of the information? I'd be interested in the thoughts of the panel on that one.

ANSWER:**MR. MAX SNIJDER:**

Just a short remark. This is not a biometric problem. It is a problem of any kind of information, which is being asked from you, if you would like to participate in any kind of scheme. So it is a case-by-case issue and it would be nice to have some general guidelines for specific applications how you should deal with the biometric data, but I would like to put the biometric data, also in the same line with other personal data, because it is not really, only, a specific biometrics issue what you just mentioned.

COMMENT FROM THE FLOOR:

I think it fairly much infringes on your privacy there is no point in having the data unless its used.

MR. MAX SNIJDER:

It totally depends on the application.

MR. PETER HANEL:

Let me give you an example. In Europe it's supposed that visa data that will be kept for five years, whereas in the United States it's for 75 years. So now what answer do you expect? I mean it depends actually not so much on the kind of data but on the legislation. Data, biometrics data, is just an add-on to other data so actually why should biometrics be kept longer or shorter? I mean it depends on the purpose. It's one of the principles, that you keep data only as long as you need them. So I think the EU way is not too bad, saying better shorter than longer. Because one risk is, and I tried to explain it in my speech, the more information you have the less reliable in the end it is because you do not know how old it is. It is not updated properly and with these centralised systems you don't know which one is the right information. So actually it's better to have only few, but highly reliable. It's better for all. For those who need information and for people concerned.

QUESTION:

Thank you. Thank you very much. I'm from the Forensic Science Laboratory, and thanks for a fantastically thought provoking presentation from all the speakers. I just want to clarify something that Billy mentioned and I'm sure Billy and I will have many discussions about this before it's out, but it was in relation to the DNA slide. The way the slide is put up quite rightly says that lots of information is available from DNA. But then the next part of the slide talks about the databases that are held by police and I'd just like to clarify that any of the databases, that I'm aware of held by police with DNA, are not suitable to gain the type of information you've listed there, with the exception of sex. So that the data that's stored as police DNA databases, don't allow, are not capable of giving information such as health, or cultural identity or anything else.

MR. MAX SNIJDER:

Also not if they store samples?

ANSWER FROM THE FLOOR:

The samples are obviously open to further interrogation should that happen, but the data that's held in the way of a database at the moment and it goes back to whether or not it's considered the material is personal data or not, because there is a difference between a sample and the databases that are stored as digital information.

MR. PETER HANEL:

Won't comment to DNA.

QUESTION:

Just to say that I think that the event and each of the contributions was very valuable. I work with the Justice Spokesperson in the Oireachtas and we have had, like as outlined earlier, a number of developments. Whether it was in the criminal justice acts, in the taking and storage of samples, through to the Passport Bill. I felt at the time that the legislators were going through that that they weren't preceded by this wider debate that's actually necessary that has to be had outside of legislators but that should also include them. The thing in terms of the ongoing considerations of privacy is obviously a huge one. Another one for me would be the opportunity cost of all of this spending, on the technologies and systems, and as often times the objective that is put forward for a lot of these biometric systems and that is security. I think people aren't looking at them and we're missing out on in terms of, not investing in a wider approach being put forward in terms of the human security approach. That, you know, you actually address all of the causes that result in threats. So I wonder if maybe if you could give a sense of the scale of spending of public money in Europe. Whether it's on research and development currently, or the, the EU visa system mentioned earlier and the shift over to biometric passports from traditional passports. Just to give a sense of what the scale of that would be?

ANSWER:

MR. MAX SNIJDER:

I will look up a slide for you and then I can tell you something, probably, about the scale of how the expenditure is on homeland security and homeland defence. But it is very difficult to cut out the

biometric piece of it because I can say, the Dutch passport project is a €250 million project and somewhere you have a piece of biometrics in it. The same counts for the visa. If a country decides to procure a biometric system, a system at the consulate is not only biometrics, it's a lot of connectivity you have to read passports etc. it's a bit difficult to say but maybe I can find a version for you if you like.

MR. PETER HANEL:

In the meantime, I would like to come back to the DNA discussion. DNA what police is using today is a so called uncoded information within the DNA and it's true that these parts of DNA being analysed do not let conclude to behaviour or colour of eyes or hair or whatever. The risk I see in DNA is that the samples have to be kept somewhere and they are being kept, they are frozen and they are kept. So, you have the physical security that you have to ensure other than the data security because actually the content of the data is not sensitive at all, actually it's the samples which have to be protected because out of these samples, you can analyse other parts of the DNA and this could then lead to fear with this problem, but usually it depends on who is, who keeps the samples and to date it's actually criminals or suspects who have to give samples. As regards and just as an introduction, before Max answers to the EU passport, the EU passport actually is not only something where you say how much does it cost? We shouldn't forget that the EU passport is linked to the incidents of September 2001, which we all know did not happen in Europe, but it was in the United States and it was the United States coming out with introducing biometrics into their borders and it was them asking ICAO to investigate which kind of biometric should be used. ICAO finally came up with face obligatory, as I said before, whereas fingerprint and iris is optional. Only in Europe it is face and fingerprint because face does not distinguish enough we know this that face alone was not accurate enough only for a certain period of time. Whereas, the European passports often are valid for 10 years. So actually it was a hand-in-hand process and also please don't forget that it started actually already in 2003 with introducing EURODAC asylum seekers system, based on fingerprints, then it was the first proposal of the resident permits so this means non EU residents, and as a third step it was supposed to introduce EU passport to protect EU citizens for misuse of their existing documents. Unfortunately the sequence was already turned around but this is actually the situation so you will be able to use this biometric passport anyway when you travel to the United States otherwise you would have to apply for a visa. But to keep your visa waiver status you need this passport. Similar activities ongoing in Australia, in the Far East so it is not a pro-European decision it was, honestly speaking, influenced by other factors.

PROFESSOR EMILIO MORDINI:

A brief remark on the issue. About passport you should consider that the last figures we have say that there are some 500 million air passenger, per year, transit through international airports and eight million each given day people travelling in the sky. So starting this morning at eight until tomorrow at eight, eight million persons travelling are in the sky. You can't think to handle, with this huge flow of people just using paper documents, two-thirds of them are issued by states, which are not reliable. So in any case we have to find an answer and the answer cannot be to close borders. I love globalisation, I love people mobility, I love freedom, I want people more free to move and we have to find a solution to this. Maybe biometrics is not the solution but we have to find a solution unless we run the risk that the only answer is to close the border. First point. Second point, DNA biometrics and I agree, actually my position and Mr. Hawkes' position are closer, than it seems because I am posing exactly, I appreciate that his point of view and I am posing the same question actually. Biometric data are more sensitive than DNA exactly for the

very reason that I told you, that we are biography, we are phenotype we are not genotype. DNA details concern genotypes, which are only part of human beings. On the contrary biometrics data conserved within themselves, in themselves a trace of our history, of our biography even fingerprint is something that tells about our life if our fingerprint is not readable very well it means that we have done work which utilised with blood and our fingerprint is an information about our lifestyle about our age and so on. This is the reason why we should differentiate between raw biometrics data and digital biometric data, but raw biometric data are full of details of our lives.

MR. ASIM A. SHEIKH BL:

Any final questions before I give my comments? Yes.

QUESTION:

Thank you very much. It's been a real eye opener very much as a lay person here but I'm also on the board of IAPO, a global patients organisation in all continents and we were actually over in Uganda there last week, and looking at people out in the city where they have no electricity I think that biometrics and all the rest of it is a long way, in all seriousness, from their normal day-to-day living. But one thing I would like to pick up on that the Data Commissioner mentioned there, which I think is very important, is the whole issue of consent and the whole issue of informed consent. It's fine saying tick this box but it's another thing to know that that box is going to be distributed all over. I think from the point of view of international relations, I think that in individual countries there could be distrust of the governments and security services. That your personal information within say a European domain, what can actually happen to that information when it goes further afield? I'm not talking about America I'm talking about other countries around the world and so on and I think that when we lose the right to informed consent we lose part of our personhood a bit and I think that, it's not consent that if you don't do this you don't get something and there's something fundamentally flawed in that premise. But I did find this extremely interesting and exciting.

ANSWER:

MR. MAX SNIJDER:

I have here some figures, of course these are some figures, it's the growth of the homeland security and the homeland defence market starting 2008 estimated €392 billion growing average with a 6.7% average growth rate to 2018 to €748 billion and then the RFID biometrics and people screening it's not the biggest part of that market but will be the fastest growing to up to 10% in the next 15 years. If you would like to speak to someone who has personal experience in access to the stored data then you should go to Brussels on December 2nd. I will be on a panel with Sophia in't Veld. Sophia in't Veld is a member of the European Parliament and she has tried to track down the data which the US government has stored about her, because I also know from my discussions with HIDE in the US, that you get access to your stored data if you ask for it, she tried, but she could not get access so she is now going to, she went to the European Court of Justice to sue the American State because she cannot get access to her stored data. So she speaks on December 2nd at a conference called "Integrated Border Management".

CLOSING REMARKS

MR. ASIM A. SHEIKH BL:

Alright, thank you very much. Could I just once again, before I pass the floor on to Dolores to close today's meeting could I thank Professor Mordini, Mr. Hanel, Mr. Hawkes and Mr. Snijder for their expertise, their contributions and their time. We are very grateful to all of you and I think this discussion could go on for the rest of the afternoon but in the interest of time we'll have to call it a day. Personally, I think it's been a huge learning experience for me as well and I certainly hope that in this climate of economic difficulty, that following on from what Stephen imparted about informed consent, is the ability to give information to people about the advantages and disadvantages of biometrics and it will be interesting to see how the State deals with that outreach programme. We obviously at the Irish Council for Bioethics are tasked with that issue but it will be interesting to see how we manage to maintain some semblance of sanity in these difficult times in relation to educating the population at large, which is all of us here and the wider audience as well. Without saying anything else I'll pass the floor onto Dolores to close today's meeting.

DR. DOLORES DOOLEY:

Thank you Asim and I do wish to say thank you to Asim for chairing, to Emily, Emma and Paul and the secretariat of the Council for all the organisational work that went into this: it is a large task in itself. And our speakers, it is very difficult to overstate the value of the contributions that have been made by our four speakers and as I sat there Asim and Andrew in the back and Stephen, well no I guess Stephen, Asim and Alan over there were the three rapporteurs for the document which will be coming out in the new year from the Council and Andrew in the back is our geneticist and he has his keen eye open on possible implications from DNA procurement on identification. When I, I won't go into any detail because we do have a time question, Billy Hawkes raised in his talk at the end this question of proportionality and that concept in itself with regard to this topic it seems to me opens up a huge Pandora's box because once you get into proportionality judgements you are into profound value judgements, which raise questions. I couldn't help but think when somebody mentioned 2001 and the terrorists, well the situation that occurred in the States, situation that's very neutral, but I couldn't help but think that the invasion of Iraq was based on a proportionality judgement. But that judgement of course lacked evidential foundation and I don't want to get political here except to say that it struck me very much that a proportionality judgement raises questions for all of us as ordinary citizens about who is making the judgement, and what is their value framework. And so I thank Billy for raising that, because it seems it was in the background of all the talks. So to each of the speakers I just want to say a warm thank you for being here, for giving of your time and we may well be getting back to you with regard to the video, which will be made available to anybody accessing the Bioethics Council's website and of course we will be sending you the document in the new year as well and will look forward to your feedback and likewise to all the participants and the audience today. Thank you very much for coming.

THE IRISH COUNCIL FOR BIOETHICS

Dr. Dolores Dooley, Chairperson

Philosopher and Lecturer in Bioethics

Professor Alan Donnelly

Senior Lecturer, Department of Physical Education and Sport Sciences, University of Limerick

Professor Andrew Green

Director, National Centre for Medical Genetics, Our Lady's Hospital for Sick Children, Crumlin; School of Medicine and Medical Science, University College Dublin

Professor Linda Hogan (Until December 2008)

Head, Irish School of Ecumenics, Trinity College Dublin

Dr. Mary Henry

Retired Medical Practitioner and Former Independent Member of Seanad Éireann

Dr. Richard Hull

Lecturer, Department of Philosophy, National University of Ireland, Galway; Director of the Centre of Bioethical Research and Analysis (COBRA)

Dr. Peter McKenna, Vice Chair

Consultant Obstetrician and Gynaecologist, Rotunda Hospital, Dublin

Professor John Vincent McLoughlin

Department of Physiology, Trinity College Dublin

Mr. Stephen McMahon

Chairman, Irish Patients' Association

Mr. Turlough O'Donnell SC

Practising Barrister and Former Chair of the Bar Council of Ireland

Professor Cliona O'Farrelly

Professor of Comparative Immunology, School of Biochemistry and Immunology, Trinity College Dublin

Dr. Darina O'Flanagan (Until December 2008)

Director, Health Protection Surveillance Centre

Professor Richard O'Kennedy

Professor of Biological Sciences, School of Biotechnology and National Centre for Sensor Research, Dublin City University

Mr. Asim A. Sheikh BL, Vice Chair

Practising Barrister and Lecturer, Division of Legal Medicine, University College Dublin

Professor David Smith

Senior Lecturer, Department of General Practice, School of Medicine,
Royal College of Surgeons in Ireland

Dr. Sheila M. Willis

Director, Forensic Science Laboratory

SECRETARIAT

Dr. Siobhán O’Sullivan

Managing Scientific Director

Ms. Emily de Grae

Communications and Outreach Manager

Mr. Paul Ivory

Programme Manager

Ms. Emma Clancy

Executive Assistant

TERMS OF REFERENCE

1. To identify and interpret the ethical questions raised by biomedicine in order to respond to, and anticipate questions of substantive concern.
2. To investigate and report on such questions in the interests of promoting public understanding, informed discussion and education.
3. In the light of the outcome of its work, to stimulate discussion through conferences, workshops, lectures, published reports and where appropriate suggest guidelines.



The Irish Council for Bioethics
1 Ormond Quay Lower
Dublin 1
Tel: +353 1 878 3051
E-mail: info@bioethics.ie
Web: www.bioethics.ie