COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

ICT-PSP-2-Theme-3 - Consensus building, experience sharing on internet evolution and security

ICT PSP call identifier:	ICT PSP 2nd call for proposals 2008
ICT PSP Theme/objective identifier:	3.2 Trusted information infrastructures and biometric technologies

Project acronym:	**BEST Network**
Project full title:	**Biometrics European Stakeholder Network**
Grant agreement no.:	**238955**

Deliverable D7.3

Overview of the ethical, social and policy implications of biometrics

Draft version prepared by Silvia Venier and Emilio Mordini (CSSC, Italy)
Dissemination level: PU
Date of submission: 23rd December 2011

Table of Contents

1. Introduction

BEST (Biometrics European Stakeholder Network) is European Thematic Network on trusted information infrastructures and biometric technologies. BEST is based on four pillars[1]:
1) technical, scientific and industrial excellence
2) legal analysis and compliance
3) ethical awareness and sensitivity
4) public and democratic scrutiny

The BEST Network Working Group 7 (WG7) specifically deals with the analysis of the ethical, legal and socio-technical aspects that shape biometric innovation. As stated in BEST DoW, the objective of WG7 is "to incorporate ethical and legal reflection and conversation directly into the industrial and policy matrix"[2]. BEST Network WG7 members include CSSC (Chair), University of Leeds (Co-chair), University of Tilburg (Rapporteur), RAND Europe, European Biometrics Forum, Independent Centre for Privacy Protection Schelswig-Holstein, University of Utrecht.
The background of WG7 is represented by a series of projects funded by the European Commission under the 6th and 7th Framework Programmes on the ethical and policy issues of biometrics and security technologies ethics, such as BITE (Biometric Identification Technology Ethics[3]), HIDE (Homeland security, identity, detection technologies ethics[4]), RISE (Rising Pan European and International Awareness on Biometrics and Security Ethics[5]), and the FIDIS Network of Excellence (Future of identity in the Information Society[6]). The work carried out by BEST WG7 resulted in the establishment of a special committee on *Ethics, Society and Privacy* within the scope of the European Association for Biometrics (EAB), as a permanent mechanism to assess the ethical, societal, legal and policy implications of current and emerging biometric technologies.

Trough the BEST Network, WG7 seeks to facilitate and structure European and international conversation in this sensitive policy area. The ambitious objectives of BEST WG7 have been accomplished in two phases:

1. ***First phase: inventories***. The first phase of BEST (2009 – 2010) was characterized by the creation of content through inventory exercises. During this first phase, WG7 produced 2 deliverables: *D7.1 Biometrics in Europe: inventory on politico-legal priorities in EU27* and *D7.2 Inventory on Privacy and Data Protection Issues in biometric applications.* WG7 members discussed on the content of these deliverables during a conference call that took place on March 2010, as well as through a regular exchange of emails and physical meetings. D7.1 and D7.2 saw the contribution of all WG7 members and were circulated among the network as a starting point for further discussion.

[1] BEST Network DoW, page 3
[2] BEST Network DoW, page 57
[3] http://www.biteproject.org
[4] http://www.hideproject.org
[5] http://www.riseproject.eu
[6] http://www.fidis.net

2. ***Second phase: networking***. The second phase of BEST (September 2011 – February 2012) has (and will) prioritize the networking and the interactions with the members of other WGs. During this second phase, WG7 has been focusing on the development of the final deliverable of WG7, *D7.3 Overview of ethical, social and policy implications of biometrics*. The deliverable is the result of the scrutiny of the existing material reported in D7.1 and D7.2 and of a mutual exchange of relevant information with BEST network members that took place during two workshops and other networking opportunities. D7.3 also presents the WG7 Strategic Research Agenda (SRA) that is meant to cover the upcoming 5 to 10 years in this field of research. Finally, D7.3 reports on the establishment of the EAB *Special Committee on Ethics, Society and Privacy (ESP)*, that directly resulted from the work carried out by BEST WG7.

1.1 Objectives and structure of D7.3

D7.3 is therefore the final outcome of the work carried out by WG7 in BEST "second phase". Its main objectives are:

1. To reassess existing data on biometrics in Europe from the ethical/legal/social perspectives and identify relevant issues that have not been included in D7.1 and D7.2;
2. To report on the networking opportunities offered by BEST to interact with the members of other WGs and external experts;
3. To prioritize policy and legal issues at a European level, identify major needs and provide benchmarks or possible indicators of action;
4. To summarise considerations on the inclusion of the ethical, social, cultural aspects in the future discussion on biometrics in Europe.

D7.3 is divided into 2 parts.

Section 2 focuses on the analysis of the politico and legal aspects of the wider deployment of biometrics in Europe and on some key conclusions and recommendations as resulted from D7.1 and D7.2. Section 2 targets objective 1 as above mentioned.

Section 3 focuses on the results of the networking and targets objectives 2, 3 and 4. Section 3 is divided into 3 sub-sections: the 1st sub-section provides more information on the interaction with the BEST network during the Darmstadt meetings, that resulted in (i) an in depth discussion on the ethical, legal and societal aspects that shape biometrics innovation in Europe and in (ii) the establishment of the *EAB Special Committee on Ethics, Society and Privacy* (**section 3.1**); the 2nd section provides some general comments from the ethical, societal and policy perspectives on the main issues at stake that were not discussed in depth in previously submitted WG7 deliverables and includes some proposals on a set of policy instruments for the future global governance of biometric technologies (**section 3.2**); the 3rd section includes WG7 *Strategic Research Agenda*, that is the final outcome of the work carried out by the working group (**section 3.3**). The Strategic Research Agenda has been circulated to the BEST members for review, and then approved by the network. The SRA will be further discussed with the BEST Network and the General Assembly of the EAB in occasion of the 1st European Biometrics Symposium (February the 16th and 17th, 2012).

2. First phase: Inventories - D7.1 and D7.2

During the first phase of the BEST Network, WG7 produced 2 deliverables. These reports were mainly the result of inventory exercises to which WG7 members contributed. D7.1 and D7.2 were circulated among the consortium and uploaded into the BEST website – WG7 devoted webpage for further dissemination.
This section briefly summarizes the main conclusions and recommendations of D7.1 and D7.2. Their results have been also discussed during the BEST network conference at BIOSIG 2010, BEST Network review meeting on the 8th December 2010 and during the two workshops held in Darmstadt in September and November 2011.

2.1 D7.1 Biometrics in Europe: Inventory on politico-legal priorities in EU27

D7.1 was edited by Juliet Lodge from the University of Leeds and focused on the broad arguments and rationales around the political-legal landscape of biometric deployment in the EU27 today.

In the first part, the paper traces a brief history of the use of biometrics in EU27. Border control procedures provided the first rationale for the introduction of biometric identification systems and biometric databases in Europe. Biometrics gained prominence as a more reliable way of identifying individuals in territorial border management. This trend started long before the treaties of Nice and Amsterdam, and was mainly the result of informal agreements between foreign affairs and justice ministers to effectively combat international organised crime and terrorism or to deal with the growing evidence of asylum shopping. The gradual adoption of reform measures led to the development of the pillar structure that opened the door to European *cooperation* (inching towards a deeper *integration*) into the most sensitive areas of national sovereignty, i.e. foreign affairs and justice. The initial enthusiasm for first and second generation e-identity cards and e-passports, however, has been soon confronted with the reality of "non-compatible legacy systems, cost cutting, cynicism, growing public distrust in the technology and more so in those handling personal data (of which biometrics are but one element) – whether in the private or public sectors" (BEST WG7 D7.1, page 6). Accordingly, biometrics have increasingly become synonymous with the erosion of privacy and of the protection of personal data.
From the other side of coin, the "convenience to citizens" claim, advanced by governments and industries in the eGovernment and eID applications, was adopted as a second rationale for their deployment in domestic daily transactions. The paper stresses the fact that, even with reference to this rationale, concern has recently grown as to "the cost relative to the savings, the difficulty facing citizens whose identity has been stolen or lost, fraud, outsourcing eID management and data storage, public-private partnership accountability, data degradation, the cost of enrolling biometrics, mission creep, data linkage, discriminatory impact, tracking, social divisiveness, exclusion, profiling and discrimination" (BEST WG7 D7.1, page 7).
The first part of D7.1 concludes that the fact that the 2 rationales for the implementation of biometrics (security and e-government) have been developed separately carries to the risk of **mission creep** resulting from the separation of policies related to ICTs used for security purposes and to ICTs used for other purposes (convenience) and to the **erosion of the credibility** of those rationales.

The second part of the paper addresses in depth the main politico-legal concerns raised by the *naive* deployment of biometric technologies. First of all, it points out the issue of the definition of biometrics. In Europe the *definition* is expanding from the "EU" definition of a biometric as a digital expression of a given feature of a person, to include the "US DHS" definition that comprises behavioural data (that are often used for "intelligence" purposes).
The second conclusion of D7.1 is that potentially risky is the lack of understanding at the political level about an unthinking adoption of a **broad definition of biometrics**. The wider definition makes the concept of biometric essentially arbitrary and contestable. If biometrics are to have legitimate uses, they have to be better specified, safeguarded and restrained. This is clear also in consideration of the fact that in Europe databases (EURODAC, SIS, VIS) have grown in size and scope.
The third part deals with the considerations surrounding the concept of **biometrics as personal data**, and briefly addresses the issues of data subject consent (it refers to the example of people may not have the option of opting out to the system, if they want to travel), purpose minimization, proportionality and out-sourced data (since, according to EU data protection law, personal data con only be transferred outside the EEA if it is protected as well there as it is within the EU).
The last part of the paper, focuses on the concept of **interoperability of systems** that has to be understood not as a mere technical concept. In the EC Communication on Interoperability of European Databases it is stated that "interoperability is a technical rather than a legal or political concept". From a mere technical perspective, the Stockholm programme's commitment to enhancing interoperability and cross border information exchange is undermined by the reality of diverse and incompatible ICT legacy systems and administrative procedures. However, the EDPS in his 2006 opinion on this subject noted that interoperability cannot be considered in a mere technical way, since it can often lead "to subsequent demands for less stringent legal requirements".
Finally, the second section of the paper deals with the analysis of a set of case studies: the Netherlands, Italy, the UK and Germany.

According to the above mentioned conclusions, the paper suggests a series of recommendations:

- a code of ethical practice regarding all aspects of handling biometric data that is digitalised and/or that is linked or linkable to other digital data
- regulation to enforce compliance with data protection and privacy laws
- regulation to combat mission creep via proportionality
- review of the robustness against intrusion and mission creep of privacy enhancing technologies and privacy by design programmes

2.2 D7.2 Biometrics in Europe: inventory of biometric data and privacy legislation

D7.2 was edited by Paul de Hert and Annemarie Sprokkereef from TILT – University of Tilburg and focused on the EU/National data protection legal frameworks vis à vis biometric technologies and applications. The report looks at International Sources of Data Protection as well as at strengths of European legal framework. It examines the EU practice of data protection with regard to large

European policy rollouts such as Eurodac, the Schengen Information System (SIS), the Visa Information Systems (VIS) and the European Biometric Passport. The report also details national developments in this area with regards to Germany, the United Kingdom and the Netherlands. In its analysis, it also looks at the shortcomings of European Data Protection and provides some key recommendations.

The starting point of D7.2 is the analysis of the international sources of data protection as background texts and the main data protection principles enlisted in those legal instruments. The **international legislation** the report refers to are those produced by the Organisation for Economic Cooperation and Development (1981 OECD Guidelines), the Council of Europe (Treaty 108), the United Nations (1990 UN Guidelines concerning computerized personal data files) and the European Union (Directive 95/46/EC). The key **principles** of international data protection legislation are collection limitation, data quality, purpose specification, use limitation, data security, individual participation and accountability. The inventory points out the strengths of the EU Data Protection Directive such as its good principles and its ability to deal with different technologies.
The Directive is applicable to the processing of biometric data both as raw biometrical images and as the derived templates. This is mainly due to that fact that the Directive, unlike other international legal instruments, uses a very broad notion of “identifiable person”. All data (raw images or digital templates) that make it possible to identify a person should be considered as personal data in the sense of the Directive. The framework has thus a very general scope and applies to all existing biometric technologies.
According to the authors of D7.2, the EU Directive is characterized by an “enabling logic”: data protection legislation is based on the assumption that the processing of personal data is allowed and legal in principle. However, this framework is lacking normative content, in terms of more specific rules for given applications.
In the second part, D7.2 describes EU practice with regards biometric databases and national developments in Germany, United Kingdom and the Netherlands. As per biometric large scale programs at the European level, EURODAC, the Schengen Information System (SIS and SIS II) and the Visa Information System are analysed in detail, as well as the case of the European Biometric Passport.
The last part of the report mentions the shortcoming of the EU data protection legal framework, that generate problems with new technological development that is considered under its framework. The report particularly addresses the case of emerging biometric technologies, the so called “second generation biometrics”, as well as the tension between the processing of those data and the individual participation principle. Behavioural biometrics may be collected covertly, without individual consent or knowledge. Additionally one has to wonder on the very applicability of the Directive to data that may not be used to identify a person, but to recognize some physiological or behavioural patterns, that may be used in surveillance or profiling practices.

D7.2 main conclusions are:

- There is an **enabling legal environment** for biometrics in Europe but it is lacking normative content: more precise rules are needed addressing specific applications and prohibiting their use where there are disproportionate power balances.
- Regulations should address the **need for transparency** in biometric systems. A general prohibition on the collection and use of biometrics without the knowledge of individuals is recommended and is needed in order to protect fundamental rights and freedoms, and to increase public confidence and trust in institutions.
- Regulations should address the **errors and technical failures**, which are inherent to any biometric recognition system. Error rates should be made availbale to the data subjects. Regulations should determine the rights of data subjects in case of failure.
- There is the need for **monitoring and certification procedures,** particularly in the case of mass applications.
- **Socio-cultural aspects** and possible reluctance towards the instrumental use of the human body should be taken into account. Basic principles such as informed consent, human dignity, equality should also be respected.

In section 3.2 we will give a brief overview of the main ethical, societal, and policy aspects that have not been included into WG7 previously submitted deliverables, and we will address also policy instruments for the future global governance of biometric technologies.

3. Second phase: Networking – D7.3

Deliverable 7.3 provides an "*Overview of ethical, social and policy implications of biometrics technologies*" as the result of the discussion among WG7 members and other components of the BEST network. D7.3 aims to deepen a common understanding of the main social, ethical and political challenges posed by biometrics and to integrate responses to these challenges into a wide range of concrete proposals.

The present section 3 of D7.3 targets the following objectives

- To report on the networking opportunities offered by BEST to interact with the members of other WGs and external experts;
- To prioritize policy and legal issues at a European level, identify major needs and provide benchmarks or possible indicators of action;
- To summarise considerations on the inclusion of the ethical, social, cultural aspects in the future discussion on biometrics in Europe.

In the second phase of BEST that started from September 2011, two networking opportunities supported the debate surrounding the development of D7.3: the 2nd BEST Workshop, on the 15th and 16th September and the 3rd BEST Workshop, on the 17th and 18th November, both held in FRAUNHOFER IGD premises in Darmstadt. The presentations given by the chair and co-chair of WG7 were followed by the discussion with other BEST members and external experts. D7.3 is mainly the result of the presentations and debate during these meetings.

The WG7 members exploited the networking opportunities offered by BEST in order to:

- discuss with BEST network on sensitive issues about biometrics that resulted from D7.1 and D7.2 and that need to be included in D7.3
- collect and share opinions on technology trends and on the emerging applications
- identify and reframe key ethical and legal issues whilst encouraging dialogue where multiple perspectives can be presented
- stimulate an open and productive debate resulting in concrete proposals
- encourage a common strategic vision on responsible biometric innovation among European stakeholders
- support the establishment of a permanent platform that takes into account the non-technical aspects of biometric innovation

Section 3 is divided into 3 parts: the first part provides more information on the interaction with the BEST network during the Darmstadt meetings, that resulted in (i) an in depth discussion on the ethical, legal and societal aspects that shape biometrics innovation in Europe and in (ii) the establishment of the *EAB Special Committee on Ethics, Society and Privacy* (**section 3.1**); the second part provides some general comments from an ethical, societal and policy perspectives on the main issues at stake that were not discussed in depth in previously submitted WG7 deliverables including some proposal on future global governance of biometric technologies (**section 3.2**); the third part includes the *Strategic Research Agenda* that is conceived as the final outcome of the work carried out by BEST WG7 and will be further discussed with the BEST Network and the EAB General Assembly during the 1st European Biometrics Symposium (**section 3.3**).

3.1 BEST 2nd and 3rd Workshop Reports on WG7 session

Under the scope of the BEST network, 2 workshop were organised on the 15th and 16th September 2011 and on the 17th and 18th November 2011. The following sections summarise the main topics of the discussion and report on the establishment of the *EAB Special Committee on Ethics, Society and Privacy (ESP)*.

3.1.1 2nd BEST Workshop (Darmstadt, 15 and 16 September 2011)

In occasion of the 1st BEST Workshop held in Darmstadt on the 15th and 16th September 2011, the discussion carried out during WG7 devoted session began with a brief overview of the WG's objectives, activities and work carried out to date. D7.1 and D7.2 results were discussed in detail with the audience and some key points were mentioned[7].

WG7 chair first explored the meaning of **privacy** from an historical point of view, with particular attention paid to the specification of this notion in the contemporary world, mainly with respect to the more "operational", technical concept of **data protection**. The question of nudity versus nakedness exemplified such a distinction as well as all complex ethical issues surrounding these concepts. While *nudity* is the state of absence of clothing, *nakedness* is a mental state, which implies being stripped of decency, to lack an element of protection. *Nakedness* involves objectification, the process of symbolically turning a person into an object to be appraised. While *nudity* is an objective, empirical, condition, *nakedness* is a highly symbolic experience, which is culturally determined. The parallelism between nakedness / nudity and privacy / data protection lies in the fact that, while privacy is a highly culturally determined concept that refers to the protection of the inner spheres of the self (and could be thus related to the condition of nakedness, that describes a *subjective condition*), data protection refers to the operational rules of the processing of personal data (and could be thus linked to the concept of nudity, that describes a more *objective condition*).

As a second point of discussion, participants agree on the fact that trust in biometrics remains **contextually dependant**. As far as the impact of biometric technologies on citizens' trust is concerned, it is crucial to discuss this issue by differentiating between applications that are security *or* efficiency / convenience oriented. The impact of this second category of applications (efficiency/convenience oriented) has still to be properly evaluated from the *benefits/risks* and as well as *trust* perspectives.

The discussion focused then on the concept of **Privacy by Design** in the daily practice of applying biometrics. Participants agreed that Privacy by Design is a cost-efficient methodology. However, crucial questions were raised as far as the concept was concerned, such as whether it could be expanded to include also the organisational and legal "design". Additional points of discussion were (i) where does the overall designing process exactly start and (ii) who is involved in that. In order to integrate PbD in an early stage it will be needed that the senior management of an organisation is aware of the need of it. As far as biometrics are concerned, the senior management should be well informed about the typical challenges that biometrics bring regarding privacy and data protection, and how these could be addressed.

[7] For a more detailed description of the discussion, please refer to the "Report of the 2nd BEST Network Workshop", submitted on the 1st October 2011.

The need to reconcile privacy and security, that are both dynamics concepts, was also mentioned with particular reference to the concept of **biometrics "as a PET"**, that mainly refers to the idea of using biometrics as a tool to enable anonymity, as well as, from a more technical perspective, to enforce privacy enhancing aspects of biometrics (such as encryption mechanisms). Biometrics as a PETs still remains an under-explored area. A more in depth research should be carried out in this emerging field, also from the perspective of its ethical and privacy implications.
With this respect, the need to further discuss and elaborate a set of criteria for **ethical best practices** for biometrics deployment was also discussed with the audience. If today the evaluation of biometrics products is limited to the performance evaluation, also a set of ethical criteria might need to be included into the evaluation process.

The report of the 2nd BEST workshop included also WG7 inputs on "*Privacy and Data Protection aspects of European ABC systems based on e-Passport*", submitted on March 2011 (see *Annex 1* at page 30). This contribution was edited by Paul de Hert (Tilburg Institute for Law, Technology, and Society, TILT) and by Els Kindt (K.U.Leuven – Interdisciplinary Centre for Law and ICT, ICRI) and was intended as a feedback on BEST Deliverable 3.1 and Frontex Best practices Guidelines on ABC.

3.1.2 3rd BEST Workshop (Darmstadt, 17 and 18 November 2011)

During the 3rd BEST workshop held in Darmstadt on the 17th and 18th November 2011, the WG7 chair briefly outlined the structure of D7.3 and discussed with the audience on all relevant issues that should be included in the deliverable as key ethical, societal and policy aspects. The key topics to be addressed by the WG7 Strategic Research Agenda (SRA), the final outcome of the work carried out by this working group, were also debated. It was agreed that the SRA should particularly focus on emerging trends in biometric technologies and applications. The idea was to use the BEST Network to provide contents for the SRA and to discuss on suggestions on how to implement the SRA in the context of the EAB (see section 3.1.3). It was indeed mentioned that the SRA could be intended as the research agenda of the *Ethics, Privacy and Society (ESP) special committee* of the EAB. It was also proposed to the BEST Network to officially present the EAB and the *EAB ESP* during the final conference of the RISE project devoted to ethics of biometrics and organised by BEST WG7 Coordinating institution, the Centre for Science Society and Citizenship.

In the discussion that followed WG7 Chair presentation, the audience debated on the **large scale biometric ID programs** currently in use, and particular attention was paid for the Indian Unique Identification Project (UID). The purpose of the UID is to issue a unique identification number that will be linked to the resident's relevant demographical and biometric information. The UID is defined as one of most ambitious IT projects in the world. Moreover, and given the fact that biometrics has not yet been tested against such a large population, the project is capturing most of the international biometrics community attention. One of its main challenges is that it will target the most vulnerable and poorest groups of Indian society. Concerns over data security and privacy of a centralised database have been already raised and need to be taken deeply into account. In relation to the Indian UID, Max Snijder pointed out that it would be important that the *ESP* could analyse more in depth the good principles behind such an enormous project, and try to compare it with previous large scale programs developed in Europe or, to some extent, to assess

how to project these good principles into European practices. It was however mentioned that all consequences of the Indian case have still to be properly evaluated.

During the discussion on the development of WG7 SRA, Farzin Deravi suggested to add a section particularly devoted to the analysis of relevant changes in society attitudes towards the concepts of privacy and data protection, above all in the virtual environment. The analysis of "societal trends" will be of crucial importance if added to the analysis of the ethical, cultural, policy implications of emerging technological trends. During the debate on how to implement the WG7 SRA, it was also proposed that the ESP could liaise with the EAB **Training and Education Committee** (***TEC***), in order to organise seminars and additional training activities devoted to the analysis of the ethical, societal, privacy aspects.

In the conclusive session of the November workshop, a presentation was also given by the convenor of EUROSMART task force on biometrics. The presentation focused on **EUROSMART white paper** on "Smart Biometrics for Trust and Convenience", issued on December 2010. The audience agreed on the potential contribution that BEST WG on ethical, legal and societal aspects, and the derived EAB ESP Special Committee could give in that respect.
After the November workshop , further steps have been implemented in order to contribute to the white paper. A conference call has been organised on January the 12th, and BEST WG7 chair contributed to the discussion by providing some comments from the ethical and legal perspectives. The exchange of ideas will be ongoing in order to collaborate with the EUROSMART task force on a second version of the white paper.

3.1.3 The establishment of the European Association for Biometrics (EAB) Special Committee on Ethics, Society and Privacy (ESP)

As already mentioned in the introduction to this deliverable, the ultimate goal of the work carried out by BEST was the establishment of a sustainable follow up of the network after its end in March 2012. The opportunity to launch this initiative emerged during the 3rd BEST Workshop, when the *European Association for Biometrics (EAB) – Human Identity in Europe* was established.
The EAB was thus launched as a direct spin off from the BEST Network. The EAB is a non-profit organisation with the mission of advancing the proper, responsible and beneficial use of biometrics, through the following areas of interest: (i) community building, (ii) training and education, (iii) research and programmes development. As agreed during the inaugural meeting, the scope of the EAB will extend far beyond security applications and will address the wider scope of identity management in Europe.
With regard to its structure, the EAB management board members are elected directly by the general assembly. Special interest groups, working groups and special committees could be set up at any stage of its development. The first activities of the EAB will include the organisation of the European Biometrics Symposium (and final conference of the BEST Network, on February 17th, 2012), the opening of the web portal, the issue of EAB newsletter, as well as the networking activities with other relevant associations and communities that are particularly active in this field.

During its inaugural meeting the founding members, representing 14 institutions from 10 different European countries, elected the members of the Management Board. Mr. Alexander Nouak, FRAUNHOFER Institute for Computer Graphics Research IGD, was elected as EAB chairperson. In this occasion, the EAB also installed the following committees:

- Training and education (chair: Farzin Deravi)
- Testing and evaluation (chair: Michael Peirce/Raul Sanchez-Reillo)
- Ethics, Society and Privacy (chair: Emilio Mordini)
- European Biometrics Research Award Committee (chair: Patrizio Campisi)

The work programmes and the strategic research agenda of these committees are currently being elaborated and will be announced at the European Biometrics Symposium (Brussels, February 17th 2012), an event that will serve as the public inauguration of the EAB.

The establishment of a special committee on *Ethics, Society and Privacy (ESP)* was thus discussed with the BEST Network during the 3rd BEST Workshop and the EAB inaugural meeting. This committee directly resulted from the activities of BEST and this continuity was granted by the appointment of prof. Emilio Mordini, chair of BEST WG7, as ESP chairperson.
In addition, the establishment of the *EAB ESP* was officially presented during the RISE project final conference, held on the 1st and 2nd December 2011 in Brussels. In his speech, EAB chairman Mr. Alexander Nouak presented the EAB as a direct result of the BEST network and briefly described its structure and main objectives. Particular attention was devoted to the establishment of *EAB Special Committee on Ethics, Society and Privacy*. Mr. Nouak explained that this committee has been generated by the work carried out in the very last years by the BEST Network WG7, as well as by RISE and HIDE, two FP7 funded projects on ethics of biometrics and coordinated by prof. Mordini. Moreover, in this occasion RISE and HIDE partners demonstrated their interest in the activities of this committee, and started discussing on how to participate in the EAB and other future activities relevant to the European and International debate on the ethical and legal aspects of biometric innovation.
The first activity of the EAB ethics special committee will be to reach a general consensus on the Strategic Research Agenda (SRA) developed within the scope of BEST WG7. The SRA is presented in the conclusive section of this deliverable, and will be further discussed with the BEST Network, the EAB General Assembly and all interested stakeholders during the 1st European Biometric Symposium (17th February 2012).

3.2 Overview of ethical, social and policy implications of biometrics

This section gives a brief overview on the main ethical, societal and policy implications surrounding the development and deployment of biometrics. It includes some issues that have not been fully addressed in BEST WG7 previous deliverables, and it particularly focuses on critical challenges that will, we believe, emerge in the upcoming 5 to 10 years in this field. Finally, it proposes a set of different instruments that could support the future global governance of this technology. Section 3.2 could be seen as the accompanying document for the Strategic Research Agenda (SRA) that is presented in section 3.3.

3.2.1 Biometric technologies are here to stay

The development of reliable methods of identification has been driven, throughout human history, by a number of different factors and has been strictly related to the different levels of complexity of a society. We are now on the verge of a new epochal transition that is characterised by the fact that the human species is becoming again nomadic[8]. In the contemporary shift towards a global information society that is characterized by increasing connectivity and both real and virtual mobility, the identification and authentication of individuals is of paramount importance. In this scenario, personal identification schemes based on the infrastructure of the national state are less and less tenable.

Biometrics are among the most sophisticated IT technologies available on the market and a result of technological advances and of these deep political and economical changes that go under the heading of "globalisation". Moreover, biometrics appear to be the most likely technological candidate for a global identification system in the digital age.
Biometrics have gained prominence in the very last decades and are replacing many conventional identification procedures based on passwords, smart cards or tokens, as an automated, more secure and convenient method to authenticate or identify individuals. Biometric systems are increasingly used both by public authorities and private companies in very diverse settings. It is a technology which is being around for quite a long time, and which, since the first commercial uses in the 1970s, has seen a lot of technological advances with rapid progress being made in research and development. The interest in this sector keeps on growing, and there are some very interesting technologies which are being planned for the future.

Experts agree that biometrics could transform many aspects of social life over the next years. In 2001, biometrics was named by the influential MIT Technology review "one of the top ten emerging technologies that will change the world"[9]. 10 years later, the recently published "IBM 5 in 5"[10] initiative includes biometrics among the key innovations that have the potential to change the way people work, live and interact. While the most visible applications on the market are

[8] See Mordini, Emilio and Rebera, Andrew P., *No identification without representation: Constraints on the use of biometrics identification systems*, to appear in "Review of Policy research – Special issue on Emerging global issues in Biometrics and Policy", vol. 29, 2012; See Mordini, Emilio, *Introduction* to appear in "Second generation Biometrics: the ethical and social context", Springer, in press.
[9] http://www.globalfuture.com/mit-trends2001.htm
[10] http://www.ibm.com/smarterplanet/us/en/ibm_predictions_for_future/ideas/index.html

"mandatory" applications for state security, such as border control and national ID programmes, biometrics may become a technology with which citizens voluntarily interact daily as an enabling, convenient technology. The application of biometrics in daily activities are expected to deeply transform our life: examples include the services offered in e-commerce, e-banking, registered travellers schemes, smart environments and ambient intelligence.

Despite of the growing interest for the technology, biometrics still have not reached a very high level of acceptance in the Western democracies. Taking the first steps in the deployment of these technologies, the governments of many western democracies have led themselves open to criticism regarding a possible erosion of civil liberties and fundamental human rights. Many concerns have been raised: first of all, biometrics are not perfect systems, since they are subject to technical failures and circumventions and are vulnerable to privacy, data protection and security concerns. In addition, biometrics evoke ethical and human rights dilemmas that transcend the realm of privacy and data protection.
For all these reasons, it is widely acknowledged that biometric technology needs democratic accountability and ethical scrutiny, that should provide a more fundamental assessment of the social implications of this technology, and the respect for values such as accountability, transparency, respect for privacy, for fundamental rights and civil liberties. An EU-wide approach on these issues is still missing, and it is however crucial in order to determine how biometrics can most appropriately be applied in the context of the European Union Charter of Fundamental Rights. Democracy, in Europe as in other democratic states, goes beyond its being the rule of the political game and fully incorporates the safeguards for the respect of fundamental human rights and freedoms.

If it is true that biometric identification has been the subject of public debate, ethical reflection and regulatory efforts for many years, emerging trends in technology development and emerging application scenarios are however giving rise to a new set of ethical, legal and socio-political issues that have not yet been discussed in depth. The contemporary era of biometrics is bringing along significant changes, that have led many to speak of a "second generation biometrics". These emerging biometrics are usually based on the analysis of body dynamics or physiological traits, captured in real time and at a distance, not necessarily requiring that the cooperation of the individual being enrolled. While most behavioural biometrics are not unique enough to provide reliable human identification, they have been shown to provide sufficiently high accuracy for identity verification or automated classification. In general, biometric recognition of this type requires more modalities to be consulted in order to augment the accuracy of the system, but also requiring more (and more sensitive) information to be collected and shared. Many elements of this "next generation biometrics" are giving rise to a new set of ethical, legal and socio-political issues that have not yet been discussed in depth and that will need particular attention in the next years.
The Strategic Research Agenda (SRA) presented in section 3.3 aims at collecting the most important issues and pointing out some key related questions, in order to contribute to the future European and international discussion on these aspects. The position we have taken in drafting

the SRA is that biometrics are, it would seem, here to stay, and it is crucial to engage with this technology from a global and multi-disciplinary perspective, to seek to ensure that it is developed and deployed in positive ways.

3.2.2 Biometrics as security technologies

Since 9/11, biometrics have been heralded by politicians as the panacea for all security problems, above all for the prevention of terrorists' threats. The feeling that the 9/11 tragedy could have been avoided was a common feeling in the United States in the days that followed the event, that was also accompanied by a certain sense of urgency in protecting the nation. The US government became eager to deploy biometric systems in order to allay concerns about national security. At the beginning of the new millennium, the widespread use of biometrics was s strictly linked to their security and military applications. In the Federal Government, the 2 bigger users of biometrics have been the Department of Defence and the Department of Homeland Security.
It has been said that in the US every major piece of post 9/11 federal security legislation included biometric provisions. Just after September 11, in the US legislation passed introducing biometrics in the name of protecting the nation, such as the USA Patriot Act and the "Enhanced Border Security and Visa Entry Reform Act". The USA Patriot Act called upon the use of a certain piece of security technologies to set the benchmark for an automated system of keeping track of the entry and exit of the foreign visitors. The US-VISIT program in those years was the largest biometric program in the world.
The EU institutional reaction to the threats coming from the international terrorism has been complex and multidimensional, and it has included, as an example, the establishment of a *Security Theme* under the Coordination program in the 7th EC framework program for research and development. Following the terroristic attacks in New York, Madrid and London, the EU has soon become also increasingly active in deploying biometrics in security applications. Major examples of biometrics in EU border control systems include EURODAC[11], VIS[12], and the SIS[13]. The EU institutions' wide investments in various border security and control initiatives has made the EU one of the single largest biometric markets of the world.

[11] EURODAC is a large database of fingerprints of asylum applicants and illegal immigrants (over the age of 14) within the EU. These fingerprints are then sent in digitally to a central unit at the European Commission, and automatically checked against other prints on the database. Currently, the European Data Protection Supervisor (EDPS) supervises the processing of personal data in the database (central unit) and their transmission to the Member States.
[12] Visa Information System (VIS). The European Union Visa Information System (VIS) is a database containing information, including biometrics, on visa applications by Third Country Nationals requiring a visa to enter the Schengen area. In VIS this biometric information (10 fingerprints and a facial image) will remain valid for five years. Information is centrally stored in a database in Strasbourg (with a back-up site in Austria) allowing checks to be made at border crossing points that the person holding the biometric visa is the person who applied for it. This database is expected to contain some 70 million biometric records at full capacity. VIS aims to prevent visa fraud and visa shopping by applicants between EU member states and to facilitate checks at external border crossing points and within territory of member states, assisting in the identification of listed persons. The bodies having access to VIS include Consulates and police authorities from member states and Europol.
[13] Schengen Information System (SIS and SIS II). SIS is a governmental database used by several European countries to maintain and distribute information on individuals and pieces of property of interest. The intended uses of this system is for national security, border control and law enforcement purposes. Information in the SIS is shared among institutions of the participating countries in the Schengen Agreement Application Convention (SAAC). SIS II is the advanced version of the Schengen information System.

From one side of the coin, there is a link between security and identification. As an example, a national ID card is meant to be a security document that can prove citizens' identity in a standard way. However, from the other side, it has to be pointed out that stronger identification through biometrics does not necessarily mean more security. In the post 9/11 era, it was soon evident that biometrics were not the dramatic breakthrough in security that they were claimed to be. Despite the growing governments' spending for border security programs, and despite the heavy investments being made in biometrics and in the integration of different databases, there has been very little evidence that biometric-based security measures prevented any major crime or act of terrorism. As a result, there is a general feeling that security has not been increased and that national states are just as vulnerable as before. As it is evident, biometrics lie at the very heart of this controversy.

Biometrics, once only conceived as the only security technology that examines and extracts the unique features of our body, started to be considered as an intrusive tool that is invading our intimacy. Citizens were risking to lose control over their personal, sensitive biometric data. Moreover, biometrics have been increasingly used for *other* purposes, such as border control, electronic identification, eCommerce, eBanking and eHealth. This has led civil liberties and privacy advocated to argue that biometric are integral to the surveillance apparatus with which governments aim to control their citizens. Two concerns were particularly raised, i.e. (i) the idea that biometrics were inherently humiliating (that, in other words, were threatening the principle of human dignity); and (ii) that there was the potential for the technology to be mis-used (and that this was raising important privacy and data protection concerns).

3.2.3 The principle of human dignity: biometrics as inherently humiliating technologies?

One of the main philosophical concerns raised by biometric technology relates to the fact that they are strictly linked to the human body, whose integrity (physical and psychological) constitutes a key element of human dignity. Even if it is very complicate to reach a satisfactory and comprehensive definition of what constitute the concept of dignity, this principle is protected in the main international legal instruments as a fundamental human right. Moreover, it represents the basis for the protection of other human rights.

Practices involving the human body are "unavoidably invested with cultural values and in their turn produce new values"[14]. Biometrics oblige us to be confronted with changes that have to do with the anthropological essence of individuals. According to a popular aphorism, biometrics are turning the human body into a password, or a token. In line with this view, in a well-known case, the Italian philosopher Giorgio Agamben refused to enter the USA in protest of the US-VISIT programme's requirement for visitors to be fingerprinted and photographed, claiming that this

[14] Mordini Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE&RISE policy report, February 2010 (updated March 2011), available at www.riseproject.eu

practice was a form of bio-political tattooing, akin to the tattooing of Jewish during the Holocaust. In this occasion, Agamben has evoked Foucault, and was alluding to "a new bio-political era"[15].
The key issue is that, even if from one side of the coin the human body is "measured" for different purposes, such as for medical monitoring in order to identify pathological conditions, from the other the *legitimacy* for using biometrics as a tool for *identifying* individuals has been under discussion[16]. The French Ethical National Council raised severe doubts about the legitimacy of using biological features – instead of biographical – to identify individuals[17]. In its 2008 opinion, the French Authority warned against the potential for the widespread use of biometrics to *instrumentalise* the human body, and to reducing the human person to an accumulation of digital (and simplified) data. The opinion also mentioned the growing use of "behavioural features" not only to *describe* an individual, but also to *define* who he is and what he does/consumes. The range of body features that can be used for biometric recognition has greatly expanded since the technology was first developed, and it has also been said that in the future any personal feature would appear to be biometric measurable[18], even if with varying degrees of reliability.
In line with this view, scholars more properly speak of the "*informatization* of the body" with reference to the digitalization of physical and behavioural attributes of a person and their distribution across the global information network[19]. At the core of this concept there is a concern for the simplification of human attributes through digitalisation that could affect the representations of ourselves, and may produce processes of *disembodiment* or body dehumanisation, or offend human dignity[20]. Some scholars refer to the development of soft, behavioural, electrophysiological biometrics (the so called "*next generation biometrics*"), as well as to the potential for distant and covert data capture, as a further step in the informatisation of the body. This is mainly based on the idea that these systems represent "a significant increase in the extent to which bodies are assumed to become available"[21]. The informatisation of the body is a relatively new phenomenon, it is however evident that critical attention should be paid to today's exponential growth in the *amount* and *quality* of bodily data available with improved biometric technologies.

Additional risks linked to the concept of human dignity are related to the risks of discrimination, social exclusion and stigmatisation. Biometrics may collect very sensitive information revealing medical status, racial origin, or other genetic information, and this poses serious concerns over

[15] Foucalt had articulated bio power as a "set of mechanisms through which the basic biological features of the human species became the object of a political strategy, of a general strategy of power". See Foucalt, M., *Security, Territory, Population: Lectures at the College de France 1977-1978*, Translated by Graham Burchell, 2009.
[16] Mordini, Emilio, Sonia Massari, "Body, Biometrics and Identity", *Bioethics*, Vol. 22, No. 9, 2008, pp. 488–498. http://www.hideproject.org/downloads/Mordini_Massari-Body_Biometrics_Identity.pdf
[17] National Consultative Ethics Committee for Health and Life Sciences, *Biometrics, Identifying Data and Human Rights*, Opinion No. 98, 20 June 2008.
[18] Commission de l'Ethique, de la Science et de la Technology in Québec, *In search of balance: an ethical look at new surveillance and monitoring technologies for security purposes*, Position Statement, 2008.
[19] van der Ploeg, Irma, *The Machine Readable Body. Essays on biometrics and the Informatization of the body*, Shaker, Germany, 2005.
[20] Mordini Emilio, "Ethics and Policy of biometrics", in Tistarelli M., *Handbook of remote biometrics for surveillance and security*, Springer, 2009
[21] Van der Ploeg Irma, "Security in the danger zone: normative issues of next generation biometrics", *Second-generation biometrics*, op. cit. Springer, in press.

the potential for discrimination of individuals in terms, for instance, of job opportunities, insurance coverage, public recognition. Discriminatory practices might be also perpetuated on a non-voluntary basis. For instance, certain biometric identifiers might not be suitable for certain parts of the population due to physical inabilities or ethnic background. As a more and more use of biometrics is made, there can be an increasingly presumption that everyone should be able to enrol into a biometric system. However, the enrolment of injured and disabled groups[22] could lead to more false rejection rates than average. Ageing is a particular issue for most biometric modalities, but also children may have particular problems in being enrolled, mainly because they are still in the development phase. Discrimination of this type happens involuntarily, but may deeply affect vulnerable individuals and impact on the principle of equity. Additionally, the issue of informed consent could be very critical for incapacitated and disabled persons.
Finally, if not *inherently* humiliating, traditional biometric technologies are for sure conventionally associated with negative connotations, being largely bound up in the popular imagination with criminality and crime detection.

3.2.4 Biometrics as a tool for surveillance?

The concerns regarding surveillance are perhaps more tangible than those discussed above. A sharp debate has emerged around whether biometric technology constitutes a potential weapon in the hands of authoritarian governments: In combination with CCTV, through embedded sensors that can perform the covert data capture, identification can increasingly take place at a distance, without the individual consent of even knowledge. Biometric technologies open the door to an enormous potential for surveillance.
Profiling is also a key area of concern for biometrics. The strong authentication ability of biometric would potentially allow tracing a person through stations at which he has to authenticate himself (both physical or virtual) and thus facilitating the establishment of behavioural profiles. The major risks of biometric profiling include discrimination (information used to exclude persons from certain areas), stigmatisation (risk of longer term profiles with negative interpretation) and "unwanted confrontation" (with, as an example, information on the health status, in the case that body signals indicate certain diseases for which the medical treatment is unlikely or even impossible)[23]. It should be pointed out that this can become a realistic scenario only when it will become technologically possible to mine and link vast amounts of sensors and data.

Generally speaking, we can say that surveillance practices are supported by a "function creep", i.e. the expansion of a process or systems, where data collected to a specific purpose is subsequently used for another, unintended purpose. Function creep usually involves three elements: 1) a policy vacuum; 2) an unsatisfied demand for a given function; 3) a slippery slope

[22] Wickins has recently explored the vulnerability of a typical user population falling into six groups, mainly including people with physical or learning disabilities (e.g. spelling problems, walking impairments), people of certain races and religions, those that are elderly or homeless. See Wickins, Jeremy "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification", *Sci Eng Ethics*, vol. 13: 45-54, 2004.
[23] See the FIDIS report on behavioural profiling.

effect, or a covert application[24]. From a political perspective, it is a serious breach of public trust and threaten to destroy confidence in technology such as biometrics.
Mainly national large scale centralised biometric database are posing the risk of function creep. Once the database is established, there is always a potential for it to be used for future applications that may differ from its original purpose. It is also difficult for a government to provide assurances in relation to this issue, unless a technological solution is put in place to specifically avoid function creep. The purpose specification principle, that lays among the main principles of the international data protection legislation, plays a key role in this respect, as it prescribes that biometric data should be collected only for *specified*, *explicit*, and *legitimate* purposes.
As a conclusive remark for this section, even if fears of the growing of a surveillance society are not completely unjustified, we believe however that biometrics could be hardly considered as a building block of the surveillance apparatus of the state, provided that this apparatus exists. Other issues, related to the concepts of privacy and data protection, need probably a more in depth discussion at this point.

3.2.5 Privacy and Data Protection as intertwined but distinct concepts: implications for biometrics

Privacy and data protection concerns are among the most debated aspects of the deployment of biometrics. They have been discussed as different but intertwined concepts from diverse perspectives, such as by philosophers and legal theorists. The protection of both principles is guaranteed by the major international human rights legal instruments as the right to respect for private life and the right to the protection of personal data. The aim of this section is to clarify the relation between the two concepts and to address the particular challenges raised by biometrics.

First of all, what is **privacy**? One would say that privacy is a founding principle of our democracies, even if scholars have been experienced a great difficulty in reaching a satisfying definition of the term. The contemporary notion of privacy is associated with the concept of autonomy, as the capacity to put distance between us and others, to develop our beliefs and desires, to maintain a certain level of control over the inner spheres of the self, to exercise a certain degree of individual power to make choices, to limit access to oneself and to be separate from the community. The concept of privacy involves claims about the moral status of the individual self, about its dignity and relation to others. The individual power to be autonomous is the result of the delicate balance between our desire to be independent and our need of the community, and is thus culturally dependant. Moreover, the notion of privacy has transformed and is continuously transforming in the light of scientific advances and technological developments.
In the 1950s Hannah Arendt was one of the first scholars to observe the importance of privacy, while warning against dangers arising from the evaporation of the private sphere during the 20th centuries totalitarian regimes, that sought to rob people of their private life in order to better control them.

[24] Mordini E., S. Massari, *op. cit*, 2008.

With reference to the concept of **personal data**, this originated in the 1980s as a result of the increasing capacity of new electronic devises to turn continuous properties into discrete, measurable quantities. This has been a key historical event, since it represented a shift from personal knowledge understood as self knowledge (attained by introspection) to personal knowledge understood as knowledge about the self (attained by technical instruments), that became detachable from the person and marketable. During those years, privacy started to give increasingly way to personal data protection, which was however focusing only on the "ownership of the knowledge about the self", disregarding any other, more intimate, aspect. Framing everything in terms of data protection ends up framing all issues in terms of risk management, while this cannot be the case for some privacy-related implications. In this model, privacy and security meet as counterweights of the same balance.
In these days we are experiencing some different trends that are changing this situation. In parallel with the *privacy vs. security tradeoffs model* (zero-sum approach), a positive-sum approach is being developed. According to this view, privacy, security and liberty are mutually incremental, being the different sides of the same prisms. This basic perspective is, for instance, contained in the idea that EU security policies shall safeguards Europe's values, freedoms and fundamental human rights.
In addition, data protection is likely to be an increasingly complicate process for at least two kinds of reasons, i.e. the fact that digital data is now everywhere (and it is almost impossible to truly limit the amount of data shared and processed) and that such type of data is by default public (no data can be truly protected in the online environment).

From the personal data perspective, biometric data are personal data[25] and as such they have to be processed, in Europe, under the scope of the EU personal data legislation[26]. As already described in detail in WG7 D7.2, the European legal framework for personal data protection[27] is based on principles such as purpose specification, proportionality, confidentiality and individual consent and participation.
With reference to the *individual participation principle*, identification procedures pose a much greater risk from a data protection perspective when personal data are stored in centralised databases and cannot be under the strict and full control of the individual. Moreover, as briefly mentioned in the previous section, some biometrics are collected without the user's knowledge or consent: embedded technologies and remote and covert biometrics raise serious concerns on the free consent, transparency and on individual control over her personal data.
Biometrics have also the potential to collect extra information, that may detect people's emotional states, or information about their medical history. These practices may deeply impact on the *proportionality* principle.

[25] On the controversial definition of biometric as personal data see chapter 6 on "Extent to which the existing legal frame work addresses the privacy and data protection impacts".
[26] De Hert, Scheurs P, Brouwer E, "Machine readable identity documents with biometrics data in the EU – part III – Overview of the legal framework", *Keesing Journal of Documents and Identity* vol. 22, 23-26, 2007
[27] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

Moreover, some biometric data could be considered as sensitive in the meaning of Art. 8. The degree of *sensitivity* of biometric data varies according to the kind of biometric features (physical or behavioural), the modality (unimodal vs. multimodal) and the storage format (row image vs. template). Some biometric characteristics have the potential for direct disclosure of personal medical information, even if this may vary depending on the technologies used[28]. Relevant examples include the pictures of retina/iris that can reveal health status (diabetes), as well as lifestyle habits (drug use), or gait recognition that may reveal some muscle-skeletal disorders but also emotional states such as depression[29], voice recordings can reveal laryngitis or throat cancer, Human-Computing Interface biometrics can reveal psychiatric and neurological conditions, as well as some sensors could detect surgical modification of the body.

To conclude, while privacy is a fundamental human right that protects the integrity and intimacy of the person, data protection refers to the operational rules of the processing of personal data. It is crucial to understand the difference between the 2 concepts, in order to analyse the implications of biometrics from these different, but intertwined, perspectives. As an example, biometrics can be conceived as a privacy enhancing technology when it is used as a tool to support anonimity, by avoiding using family names to authenticate a person[30], while biometric data protection issues still remain. Such a dramatic divarication between privacy enhancing biometrics and their data protection implications is likely to be a crucial issue to be faced in the next future.

3.2.6 Biometrics beyond security technologies

Biometrics can make easier and more reliable all human activities in which is important to recognize, identify or authenticate an individual. These activities may include trade and financial transactions, in the real and virtual environments, the management of welfare services, but also the exercise of civil, social and political rights. Moreover, biometrics (above all "of next generation") are likely to be essential to smart environments and to support the trend towards ambient intelligence. According to this view, biometrics could help to address a set of different problems that are crucial to the globalised world, both in its developed and under development regions.
As per the latter case, the biometric industry is experiencing a growing penetration in Africa, South America, and Asia. In countries under development, biometrics can also provide practical support for the identification of people who are not able to identify themselves in other ways. This is particularly the case for countries under development, where the inability to prove your own identity is one of the biggest barriers preventing the most vulnerable groups of people in the

[28] Mordini, Emilio and Holly Ashton, "The Potential for Disclosure of Personal Medical Information", to appear in Mordini E, Tzovaras D., op. cit, in press.
[29] See M R Lemke, T Wendorff, B Mieth, K Buhl, M Linnemann, "Spatiotemporal gait patterns during over ground locomotion in major depression compared with healthy controls", *Journal of Psychiatric Research,* Vol. 34, No 4-5, 2000, pp. 277-283.
[30] This has been the case for many health care programmes, such as those implemented in the US (at the Mayo Clinic in Minneapolis, for undocumented patients), Australia (where a biometric methadone dispenser is used to assist drug addicts) and the Nederlands.

poorest countries from accessing benefits and subsidies. Throughout Africa and Asia, governments are moving towards national identity programs that will allow their population access to services such as education and healthcare. Large scale ID programmes based on biometrics are being implemented, but their impact on people's lives have still to be evaluated in detail. What is evident, however, is that biometric technologies are at the heart of this revolution that is focusing on empowering the individual with fundamental human rights.

3.2.7 A global governance is needed

Biometrics are evolving fast and have made impressive progress during the last years. The need for a reliable and convenient way of identifying individuals makes the further development of this technology inevitable. The current technological developments that brought some experts to speak of a "next generation" of biometrics require an even more structured debate on what should be the policy instruments to be put in place for the future governance of this technology.
There is the need that the ethical, legal and policy aspects of biometrics are debated and regulated upon a global scale. The term "global" in this respect refers to the fact that the discussion should be multidisciplinary, reaching a world-wide audience and involving all relevant stakeholders. The European biometrics community could play a leadership role in this area.

This section proposes an overview of those policy instruments that may support European and international governance of biometrics. The starting point of discussion is that the balance model between privacy and security is a problematic model, and that win-win solutions exists and have to be privileged. Ethics and privacy by design are dominating the current debate on how to conjugate the respect of fundamental rights and values with technological innovation.

Legal governance
Since December 2009, the EU is operating on the basis of a legally binding bills of rights, the EU Charter of Fundamental Human Rights, while the current EU data protection framework was established before the Lisbon Treaty entered into force. Emerging technologies are raising new concerns over fundamental human rights that are leading to calls of modernisation of the EU data protection legal framework. This is in line with the dynamic nature of the democratic constitutional state, which "evolves as a result of permanent balancing of individual, social and state interests"[31].
Since the Data Protection Directive came into force in 1995, the ways in which the personal data is accessed, collected, processed, stored and used, as well as the possibilities it is abused or misused, have seen critical changes from different points of view. The current EU legal framework based on the 95/46/EC Directive is only partly adequate to face up these challenges to the effective protection of personal data. The Directive has been currently under review and a proposal from the European Commission will be presented in the early 2012.

[31] Gurtwirth, Serge, "Biometrics between opacity and transparency", *Annali dell'Istituto superiore di sanità*, Istituto superiore di sanità, Vol.43, No. 1, 2007, pp. 61 – 65.

In the meantime, the current legal framework in Europe regarding the use of biometric data remains "vague", as affirmed by the Council of Europe – Committee of Legal Affairs and Human Rights Report in February this year[32], while asking member states to take further measures to improve it. The CoE Committee Report highlighted how the rapid development of biometrics, despite the fact that they offer a solution for security concerns, "put at stake several human rights, such as the right to respect for private life, the right to a fair trial and the presumption of innocence, the freedom of movement and the prohibition of discrimination". According to the report, specific legislation is needed in this area that should elaborate a standardised definition of "biometric data" (par. 4.1),[33] keep the legislation under review in order to meet the challenges stemming from the further development of biometric technologies including the so called "second-generation" biometrics (par. 4.2), promote proportionality in dealing with biometric data (par. 4.3) put in place supervisory bodies (par. 4.4) and promote multi-disciplinary research on new biometric technologies.

Self-regulatory governance

Considering that biometric innovation marches on rapidly, however, there will be always some inevitable lags between technology innovation and the development of new effective regulations. In this respect, a number of other bottom up and participatory instruments are needed that can support the innovative and global governance for biometrics, and these may include self regulations as well as technology alternatives.

The adoption of soft law instruments, that are able to support the introduction of best practices, ad hoc agreements and ethical codes of conduct, should be encouraged among those actors who are directly responsible for the information management and the processing of personal data. Bottom-up participatory instruments are particularly relevant, and have been introduced also to biometrics. Some examples include privacy impact assessment tools[34], codes of conduct[35] and self-regulatory bodies[36].

---

[32] Council of Europe, Committee on Legal Affairs and Human Rights, *The need for a global consideration of the human rights implications of biometrics*, 16 February 2011.

[33] The legislators are experiencing a higher difficulty in defining what is a "biometric data". This is mainly due to the fact that the definition is broadening in order to include also behavioural and physiological characteristics. A wider definition would make the concept of biometrics more arbitrary and contestable. If biometrics are to have legitimate uses, however, they have to be better specified, safeguarded and restrained.

[34] See US Department of Homeland Security, "Privacy Impact Assessment for the Biometric Storage system", March 2008 (http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf) and "Privacy Impact Assessment for the US Costal Guard - Biometrics at sea, March 14, 2008 (http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_biometrics.pdf

[35] See International Biometric Industry Association, "IBIA Statement of Principles and Code of Conduct", http://www.biteproject.org/documents/ibia_code_ethics.pdf

[36] An example is the Data Security Council of India (www.dsci.in), a Self Regulatory Organization created by Nasscom, the premier trade body and chamber of commerce of the IT-BPO (Business Process Outsourcing) industries in India. DSCI main mission is to facilitate the culture of security and privacy in the Indian IT industry and promote the message that India is a secure destination for outsourcing: DSCI is the only organization of its kind in the IT-BPO Industry globally. It is guided by and independent Steering Committee with balanced representation from industry and experts from the various domain of security (academia, government, law enforcement bodies and IT/ITES orgs). DSCI is partner of the RISE project on ethics of biometrics and security technologies.

Technology alternatives

In order to build up a sustainable and trustworthy ICT environment, the development of PETs (Privacy Enhancing Technologies) should also be supported. The principles behind the concept of PETs are transparency, data minimization, built-in privacy protection, user empowerment, while an harmonized definition of the concept is still missing. The European Commission in its Communication on Promoting Data Protection by Privacy Enhancing Technologies, describes PETs as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system"[37].

With reference to biometrics, technical solutions may include the development of privacy *aware* (such as biometric encryption, but also the implementation of the "privacy by design" principles) and privacy *enhancing* technologies (that are based on enhancing privacy sympathetic qualities of biometrics). These technical solutions are, however, relatively new to biometrics in general and in particular for biometrics of next generation. Among these technical solutions, template protection is a crucial aspects, and has become a compulsory aspect of consideration for any biometric modality. The protection of templates for next-generation biometrics could, however, be even more complex, depending on the number of aspects of relevance that are recorded in the template.

[37] COM (2007) 228 final

3.3 BEST WG7 - Strategic Research Agenda (SRA)

This section outlines **BEST WG7 Strategic Research Agenda**. The SRA addresses a set of key thematic areas/challenges that will particularly need to be discussed in the upcoming 5 to 10 years in the field of research of BEST/WG7. The WG7 SRA includes 9 key thematic areas, focusing on technological trends and main current and future applications, and addresses the related ethical, societal, legal and privacy aspects. The main issues at stake concern large scale applications, biometric databases, remote and covert biometrics, risks of misuse and function creep, biometric profiling, identification of vulnerable and disable groups, biometrics applied to children and child identification, biometric information sharing, biometric system interoperability, convergence with other identification and detection technologies, behavioural and soft biometrics.
Following the discussion with the network during BEST 2nd and 3rd Workshop, in December 2011 a first draft of the SRA was prepared and circulated to each member of the BEST network for their review.

The BEST WG7 SRA will hopefully be, at the same time, a starting point of discussion on the ethical, societal, cultural, legal aspects surrounding biometrics, under the scope of new initiatives in Europe. With this respect, BEST WG7 fully supports the implementation of the SRA by the recently established European Association for Biometrics (EAB), as far as the ethical and legal issues are concerned. The EAB ESP aims to support the conversation on ethical and social implications of biometrics in Europe, and will rely on the SRA as a starting point of discussion.
The WG7 SRA will be discussed in depth with the members of the BEST Network and the EAB General Assembly during the upcoming 1st European Biometrics Symposium (Brussels, February 17th 2012). The prioritization of the ethical, social, legal issues should be considered as one of the main short-term measures to be decided with the EAB Assembly.

Strategic Research Agenda (SRA)

	THEMATIC AREAS	MAJOR ETHICAL AND LEGAL ASPECTS
1	**EMERGING TRENDS IN TECHNOLOGY DEVELOPMENT** Soft Biometrics, behavioural and physiological biometrics; Multimodal systems; Sensors for data capture on the move / at a distance; Intention Detection technologies; Anti-spoofing techniques, Liveness detection methodologies; Privacy preserving biometrics modalities: Biometric Encryption, PETs and PbD in biometrics.	• What new ethical, societal and cultural implications are raised by the collection of particular sensitive data (e.g. health data; data related to peoples' emotional states; data on racial origins)? • Is the introduction of the so called "next generation biometrics" (i.e. behavioural, physiological and soft biometrics) facilitating social sorting or discriminatory practices? • How is the potential for covert data capture challenging the individual participation principle? • How are multi-modal systems impacting on the proportionality and data minimization principles? • Which non-negotiable values are at stake? • What are the priority issues to be regulated (e.g. technical failures, user control over personal data..)? • How can the adoption of PETs become a default setting of biometric technologies? • How can ethics be embedded in technology at the design stage? How can the senior management of an organization be trained to implement privacy by design principles?
2	**LARGE SCALE GOVERNMENT PROGRAMS** Border control programs National ID management programs	• How are biometrics in large scale governmental programs impacting on the relationship between the democratic state and the individual? • How should the potential consequences of biometric data leaked outside the established context be addressed? • How should the potential for function creep be evaluated? • How can large scale ID programs as developed in India/China be evaluated? • How can the most vulnerable groups of people be protected against the risk of discrimination? How can the most vulnerable be assured access to ICT based services that rely on certain types of biometrics? What ethical principles, if any, underlie the allocation of financial and personnel resources needed? • Is the use of biometrics impacting on the principle of freedom of movement?

		• Is it possible to make public/private partnerships and what are the challenges? Under which conditions can (biometric) data be exchanged under this partnership?
3	**BIOMETRICS in LAW ENFORCEMENT and CRIMINAL INVESTIGATION**	• What are the implications of the widespread use of biometrics deployed in mobile devices and of the potential incorrect association of a user with these devices? Should specific guarantees be put in place? • Fast DNA and genetic data: what are the main ethical and legal emerging challenges? • What are the ethical and legal aspects of international data sharing for law enforcement purposes? • From the law enforcement agency perspective: What happens if law enforcement turns to biometrics, and, as an example, regular cops are replaced by computer scientists?
4	**BIOMETRICS in eBANKING and eCOMMERCE**	• What are the main privacy and data protection implications in these applications? • How can the principle of proportionality be respected? • The whole issue of e-ID thefts is crucial in this context: what are banks doing in this respect? • What is the balance of trust between banks and governments after the banking collapse in 2008/9? Do citizens still think that banks are more likely to maintain personal data privacy and high standards of data protection? What are the consequences for society of the response? • How to deal with customers' biometric identifiers in cases of mergers and acquisitions of companies , esp. if non-EU companies are involved?
5	**BIOMETRICS in SMART ENVIRONMENTS**	• How can biometrics be used to support the most vulnerable groups of people (i.e. elderly, disabled people)? • Are the principles of individual autonomy and dignity at stake in daily use of behavioral and physiological biometrics in these applications?
6	**BIOMETRICS in REGISTERED TRAVELERS SCHEMES / AUTOMATED BORDER CONTROL PROCEDURES**	• Is there any risk of discrimination among different classes of travelers that is supported by biometrics? • How can the principle of proportionality be respected in this applications? • Is the use of biometrics impacting on the principle of freedom of movement? • Is it possible to make public/private partnerships and what are the challenges? Under which conditions can (biometric) data be exchanged?
7	**ONLINE and ON THE CLOUD BIOMETRICS**	• How are online available biometric database impacting on the private sphere of the individuals? • What are the ethical consequences of third party

		mobile devices providers building tracking into them without the explicit consent or knowledge of the consumer/owner? • Can online services be secured in a way to avoid spreading biometric identifiers in a case of attack on central or individual systems (e.g., by biometric encryption)? • Is it advisable to implement biometric authentication to protect children in the online environment? • What are the main risks related to the incorporation of the Software as a Service (SaaS) trend in biometrics? • How can biometrics be implemented in order to secure online/on the clouds environments? • What are/will be the implications for censorship?
8	**BIOMETRICS and GLOBAL IDENTITY ASSURANCE**	• Is an ID assurance based on biometrics needed at a global level in order to have access to all services which the global economy can provide? What will be the ethical and legal implications?
9	**SOCIETAL ACCEPTANCE AND PUBLIC AWARENESS ON BIOMETRICS**	• How is society evolving in its relation to emerging ICTs for security and convenience? • How can the lay public be involved in the debate on the responsible deployment of biometrics? • Does acceptance of biometrics depend on the relative access of ICT in different states? • Does acceptance of biometrics depend on age? How to involve young generations into the debate?

Annex 1 - WG7 comments on D3.1 and Frontex ABC Best Practice Guidelines

Input on Privacy and Data Protection aspects of European ABC Systems based on E-Passports

in particular for WG6: Testing and Certification of the BEST Network. Paragraph 6: Perspectives/Recommendations/Issues on Privacy and Data Protection

by Paul de Hert and Els Kindt – 30.3.2011

1. General

First of all, it is necessary to point out that there has been very little consideration of any privacy and data protection issues in the BEST Network Deliverable D3.1 and the Frontex Best Practice Guidelines on ABC systems as starting point documents. In one document, reasons have been given ('lack of expertise and time' – Frontex), the other devotes half a page (of 17) to some limited data protection considerations (mainly about transparency) and remains very general and incomplete. The lack of focus on privacy and data protection aspects which are of major importance as these systems involve the processing of (sometimes sensitive) personal data of citizens raises serious concern. Data protection considerations have thus possibly not been as incorporated as other considerations. ABCs and e-passports present, of themselves, a range of data protection concerns both as to their own security and as to their potential social impact. These issues are part of a wider series of debates regarding the security imperative, automation of security networks, government surveillance, legitimacy of collection of biometric data etc. These discussions and concerns must be considered as a background in the development or analysis of any certification or testing. The FRONTEX document states 'the primary goal of ABC systems MUST be facilitation without disregarding security. Facilitation is thus the main objective to maximize, and security a boundary condition that has to be met'. Data protection and privacy considerations are the rights predominantly harmed by encroaching security and as such should be accorded due consideration.
Since it is impossible to cure this default in a short contribution as requested, we hereunder make general remarks and evocate some issues which need further follow up and elaboration in due course.

2. Need for clear and detailed description of data collection and use

First of all, it would be necessary for the envisaged ABC and the RT systems to describe in detail and to clarify what data collection and processing activities are taking place in combination with an explanation which external processing acts are made and by whom as required in practise. This is essential for a privacy and data protection analysis aims, but is lacking.
Similar, for the testing and certification, it is necessary to elaborate in clear terms what is to be certified and tested. Only with a greater degree of clarity and certainty on the processes of the personal data involved is it possible to clarify the data protection and privacy issues involved.
In general, all testing and certification requiring the processing of personal data (with the exception of data already anonymised or not identifying an individual as defined in data protection legislation) shall follow the principles of Directive 95/46 (laid out in article 6) and

national applicable supporting legislation. The privacy rights of the individual must also be borne in mind as laid out in article 7 of the Charter of Fundamental Rights of the European Union and article 8 of the European Convention on Human Rights. Pure privacy concerns may not be so relevant here, but should be taken into account with the development of any more invasive systems (e.g., extensive profiling or data mining activities, …).
Another aspect is the aim of the testing and certification. Is it aimed at (only) testing and confirming particular functionalities/data flows/assertions made (e.g., that particular data are compared locally and after comparison deleted from particular components), or aimed at a broader goal of attesting overall or particular data protection compliance of (particular components of) the system ? Certification of the latter may be very ambitious, but an ever increasing demand as it is believed that this may enhance compliance, transparency and accountability for systems.38

3. Specific comments

a .Legal obligations for each of the specific data processing operations. Each data processing operation potentially engages the legal framework in a different and potentially unique way. The following factors may influence the specifics of engagement and the legal obligations: specific ABC design, the location of the ABC operations and the data (collection) and the national legislative issues its operation touches on, the purpose of the operation, to whom the data is distributed and who the data controller is, what data is being collected and distributed and accessed, which external/other systems are involved in processes and how they interact with these processes, etc…. The principles of the framework must thus be applied to each processing operation with the specifics of the above issues in mind.

b. Different national data protection legislations will apply and international personal data transfer issues The data protection framework is transposed differently in various countries and under certain circumstances this can lead to different engagement in different states. The potential for this must be considered as well as the difference across states in the interplay of the data protection framework and relevant local non-harmonised legislation. The data protection framework may also overlap or interact with other relevant European or international legislation. Legal boundaries and interaction should be clarified

c. Determining the controllers, the processors and the receivers. When data must be shared out or dispersed among systems or operators, designations such as controller and processor and the consequent responsibilities should be considered and determined beforehand, otherwise this risks of getting lost amongst the dispersion.

d. Need to define specific purposes, re-use of data and need for a legal basis. Data may be collected toward different aims, for instance toward improving the operational effectiveness of the system, toward statistics collection or toward developing the business model. Following this, data may be transferred to different types of bodies. The legality and the legitimacy and justification of each entity's collection and processing of data and every re-use of data (in particular of additional data collections) must be carefully considered. Data collection,

[38] Various Data Protection Authorities and the European Data Protection Supervisor ('EDPS') have stressed the opportunities that certification may offer See also European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union*, 4.11.2010, COM(2010) 609 final, pp. 12-13, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf and the reply of the EDPS in his opinion of 14 January 2011.

distribution and storage processes must be tailored with the status of likely recipients and future use in mind.
e. Data minimisation. The collection of data necessary for each operation should be kept to the minimum necessary for that operation and data should be stored only for as long as necessary. If possible, data should be anonymised (for example in statistics collection) and the possibility of 'anonymising' biometric data must be considered. Additional privacy enhancing technologies should be considered as well, as in order to make 'biometric identities' revocable, irreversible and unlinkable (with other applications to the extent feasible/desired).39 The difference between different types of biometric data must also be considered. Different types of biometric data may contain different information about the individual and alone or in combination with other categories of data this may demand their consideration under the more strenuous considerations required by article 8 (processing of special categories of data).

f. Information, transparency and rights to the data subjects. Where possible and required, it must from a legal point of view be made clear to the data subject how and why the data is being processed although, due to clear legal and practical reasons there are limits to this. This has been recommended in the FRONTEX best practises and should be defined more precisely in according with applicable data protection requirements as information and transparency are general legal rights of the data subjects.

g. Use and interaction with other data collections. In testing and certification, the interaction of ABC mechanisms with other external databases must be carefully reviewed and safeguarded. There must be particular attention when considering interoperable systems in which data may be dispersed across networks. Where data is captured and re-used, it must be considered, (beside the legal issues of e.g., re-use, profiling, transfer of data, consent, timely deletion,…) where this data will be stored, authorizations for accessing the data, and whether it will be stored with or will be easily accessible alongside other data or data sets which together may constitute a breach of the principles of the framework. It must be borne in mind that the ABC system will work in tandem with systems which themselves raise considerable data protection issues and this must be borne in mind when considering testing and certification.

h. Use of 'best available technologies' and privacy by design. ABCs and RT systems (which should properly be distinguished) operate differently depending on design and incorporate novel technologies. Thought should be given to the use of 'best available technologies', for example to restrict access or to minimize data collection (see also below) and to Privacy by Design of the systems. The specific qualities of the systems must be considered when considering the privacy and data protection in testing and certification. The practicality of their setup and background layout may also be important although are probably not key concerns.

Paul de Hert (paul.de.hert@uvt.nl) & Els Kindt (els.kindt@law.kuleuven.be)

[39] About the importance of these aspects of biometric identities, see EDPS, *Opinion 1.02.2011 on a research project funded by the European Union under the 7th Framework Programme (FP 7) for Research and Technology Development (Turbine (TrUsted Revocable Biometric IdeNtitiEs),* also available at http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation/OpinionsC/OC2011