

An overview of the European approach to the cross-jurisdictional and societal aspects of biometrics



Mario Savastano

Senior Researcher

IBB / National Research Council of Italy

DIEL - Federico II University of Napoli

Convenor

ISO/IEC JTC1 SC37 WG6 on

“Cross-jurisdictional and societal” aspects
of biometrics

mario.savastano@unina.it

Biometrics has a long tradition in Italy



The Mouth of Truth (year 400 BC) is probably the first “hand sensor” of the history. According to popular belief it was said that any one putting his hand in this mouth and swearing falsely, could not withdraw it

The evolution of the “Mouth of Truth”





Main points of the presentation

1. Introduction to the non - technical aspects of biometrics
2. Some considerations on Privacy & biometrics in EU
3. The activity of the ISO/IEC JTC1 SC37 "Biometrics" WG6 on "Cross-jurisdictional and societal aspects"
4. Cross-relations between the ISO Special Working Group on accessibility (SWGGA) and SC37
5. Conclusions

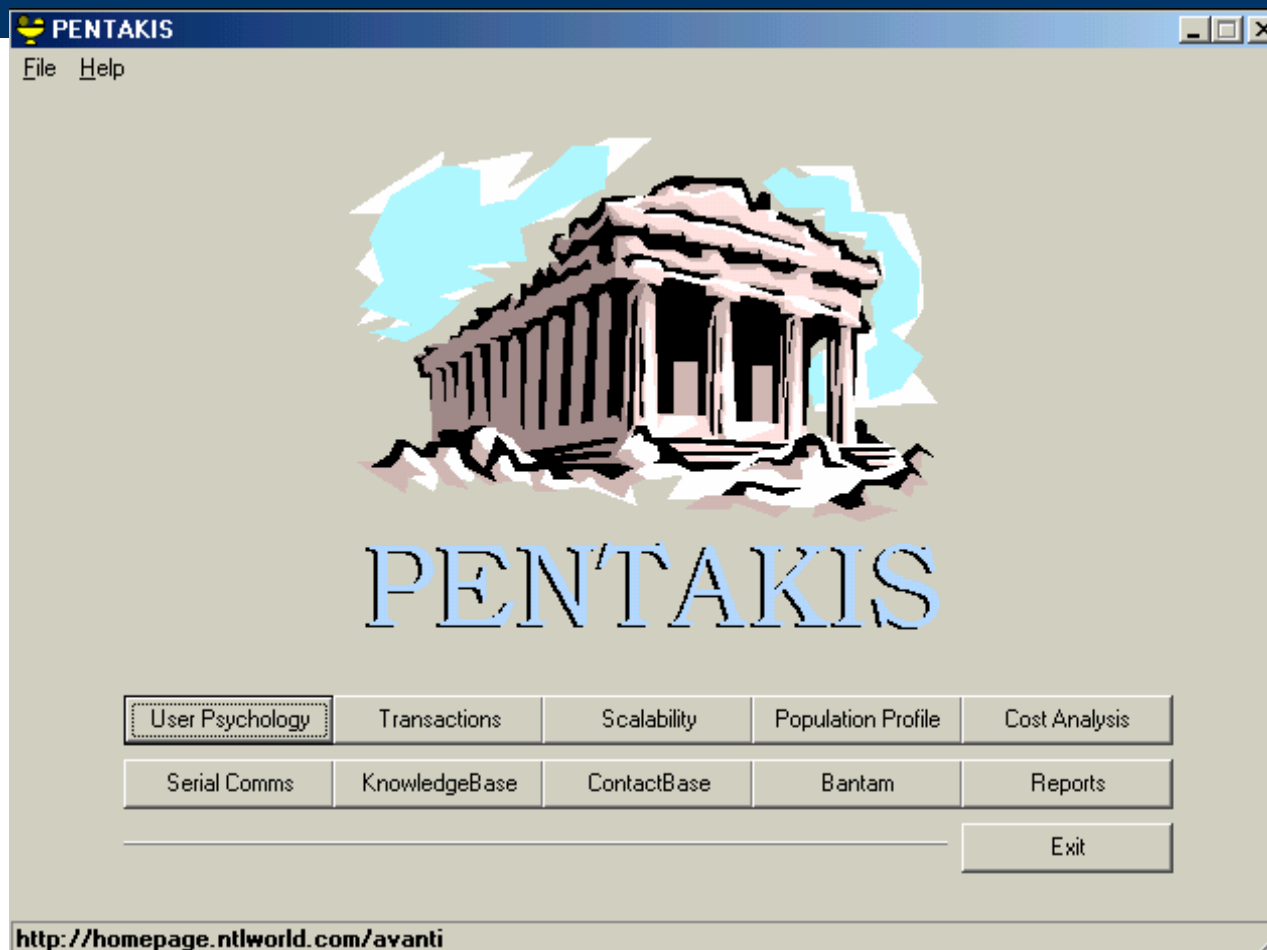


1. Non-technical aspects of biometrics

- The solution of non technical problems represents probably the real challenge that biometrics has to face
- A small increase of accuracy requires a tremendous technological effort
- A non - cooperative user may give rise to a significant decrease of accuracy in real conditions
- A negative opinion of a Data Protection Commission may even switch off an application



Pentakis





Some non-technical parameters influencing the performances

| Variable | Positive value | Negative value |
|----------------------------------|-----------------------|-----------------------|
| <i>Knowledge of the system</i> | Knowledgeable | Non informed |
| <i>Attitude</i> | Sympathetic | Hostile |
| <i>Environment</i> | Relaxed/comfortable | Uncomfortable |
| <i>Outcome for the user</i> | Critical | Non critical |
| <i>Additional ext. pressures</i> | Presence | Non presence |



1.1 Some of the non-technical aspects of biometrics

- **Medical issues**

Direct implications (potential threat to the body) and indirect implications (potential disclosure of medical information in consequence of a biometric process)

- **Privacy compliance**

Data protection in the several phases of the biometric procedures

- **Accessibility**

Management of the physical, mental and biometric temporal or permanent disabilities in the biometric process



1.2. Medical issues

- The users of a biometric system would like be sure that:
 - The system is absolutely not harmful for the body
 - Under every circumstance it is not possible to disclose medical data in the biometric process
- These two issues are “relatively” easy to satisfy
- Sometimes, the information is not clear
- The vendor could highlight the compliance of the biometric unit with safety standards

2. Privacy





2.1 Privacy & biometrics in EU

- Actually, at the European level, there is a certain lack of clarity in the definition of the biometric applications allowed in terms of compliance with national Data Protection Commissions rules
 - e.g. time & Attendance or urban “biometric” surveillance
- On the other hand, a certain fluidity should be recognized since the Data Protection Commissions seem to be flexible, in general terms, in considering the technological evolution
 - Video - surveillance
 - Biometrics
 - RFID (coming soon.....)



2.2 Art. 29 D. P. Working Party: a point of reference for biometrics & privacy

- Members from:

- Belgium - Czech Republic - Denmark - Germany - Greece - Spain - France - Ireland - Italy - Hungary - Cyprus - Latvia - Lithuania - Luxembourg - Malta - Netherlands - Austria - Poland - Portugal - Slovenia - Slovakia - Finland - Sweden - United Kingdom



2.3 Art. 29 D. P. Working Party's primary objectives

- To promote the uniform application of the general principles of the Directives in all Member States through cooperation between data protection supervisory authorities.
- To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.
- To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.



2.4 Some Art. 29's documents concerning biometrics

- Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports (11/2004)
- Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)
- Working document on biometrics (08/2003)



2.5 12168/02/EN WP 80 Working Document on Biometrics (08/03)

- *“The purpose of the present document is to contribute to the effective and homogenous application of the national provisions on data protection adopted in compliance with Directive 95/46/EC (*) upon biometric systems.....the Working Party intends to provide uniform European guidelines, particularly for the biometric systems industry and users of such technologies”*
- *(*) protection of individuals with regard to the processing of personal data and on the free movement of such data*



2.6 Some relevant points of the working Document on Biometrics (08/03)

“the templates can be stored in one of the following ways:

- a) in the memory of a biometric device ;*
- b) in a central database ;*
- c) in plastic cards, optical cards or smart cards. This method of storage enables the users to carry their templates with them as identification devices.*

In principle, it is not necessary for the purposes of authentication/verification to store the reference data in a database; it is sufficient to store the personal data in a decentralised way.....



2.7 Some relevant points of the working Document on Biometrics (08/03)

Principle of purpose and proportionality

... personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

In addition, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (purpose principle).

The respect of this principle implies firstly a clear determination of the purpose for which the biometric data are collected and processed.

Furthermore, an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way...

(introduction the concept of the NECESSITY)



2.8 Some relevant points of the working Document on Biometrics (08/03)

*“For access control purposes (authentication/verification), the Working Party is of the opinion that biometric systems related to physical characteristics which do not leave traces (e.g. **shape of the hand but not fingerprints**) or biometrics systems related to physical characteristics which leave traces but do not rely on the memorisation of the data in the possession of someone other than the individual concerned (in other words, the data is not memorised in the control access device or in a central data base) create less risks for the protection for fundamental rights and freedoms of individuals.*

*Several Data Protection Authorities have endorsed this view stating that biometrics **should preferably not be stored in a database** but rather only in an object exclusively available to the user, like a microchip card, a mobile phone, a bank card. In other words, authentication/verification applications which can be carried out without a central storage of biometric data should not implement excessive identification techniques...”*



2.9 The consequences

- *France*
 - *The French CNIL has refused the use of fingerprints in the case of access by children to a school restaurant;*
- *Portugal*
 - *The Portuguese data protection authority has recently issued an unfavourable decision concerning the use of a biometric system (fingerprint) by a university to control the assiduity and punctuality of the non-teaching staff....*
-
- *Italy*
 - *Regulations for the use of biometrics in banks (2001)*
 - *Limitation of the use of biometrics - different cases (2004)*
 - *Opinion for the use of biometrics for time & attendance applications (2005)*
- *Greece*
 - *Block (operated by the Greece's national Data Protection Authority) of a biometric project intended to acquire biometric identifiers of passengers on international flights (2003)*



2.10 Summary - Main point of biometrics and privacy in Europe

- Purpose
- Proportionality
- Necessity
- Try to avoid (where possible) a centralized database
- Protect the flow of the data (cryptography)



2.11 Essentials of biometrics and privacy in Europe

- In Europe there must be a robust motivation for the use of biometrics in the private sector
- The application should be characterized by a consistent degree of sensitivity
- Some “necessity” motivations should support the installation of a biometric control
 - Confirmed case of irregular access due:
 - Inappropriate use in consequence of a theft
 - Inappropriate use in consequence of a voluntary exchange of badge

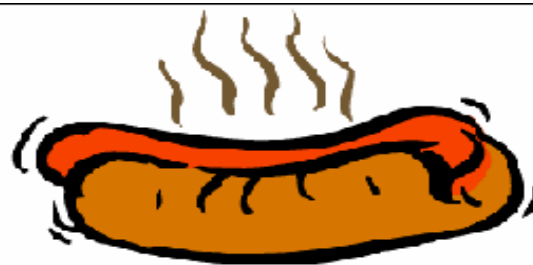


2.12 Privacy & biometrics in EU and US

- In some cases the US legislation about privacy & biometrics seems less restrictive than the European. This is not always true
- In Italy the new ID card will have on board biometrics
- In Italy is allowed the acquisition of fingerprint for accessing the banks

2.13 A special test

- In the early applications of the biometrics in banks, the fingerprint sensors did not make a quality control on the images acquired
- Some clients were using the palm (instead of fingerprints)
- Other ones were using “Hot Dogs”





2.12 Privacy & biometrics: the necessity of a global approach

- New international large scale programs will require a strict collaboration among Data Protection Commissions and experts in biometrics at an international level
 - e.g. travel documents equipped with biometric identifiers
 - Passports
 - Seafarer's cards
 -
- It should be wise to create a joint international working group for the global harmonization of the rules in terms of privacy & biometrics



3. ISO/IEC JTC1 SC37 “Biometrics”

Scopes

- Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include:
 - Common file frameworks
 - Biometric application programming interfaces
 - Biometric data interchange formats
 - Related biometric profiles
 - Application of evaluation criteria to biometric technologies
 - Methodologies for performance testing and reporting
 - Cross jurisdictional and societal aspects



3.2 WG 6's Terms of Reference

- Standardization in the field of cross-jurisdictional and societal aspects in the application of ISO/IEC biometrics standards. Within this context, the terms of reference includes the support of design and implementation of biometric technologies with respect to:
 - accessibility
 - health and safety
 - support of legal requirements and acknowledgement of cross-jurisdictional and societal considerations pertaining to personal information
- Specification and assessment of government policy are excluded from the scope of WG6



4. The ISO SWGA and SC37

- The Resolution 24 of the nineteenth Meeting of ISO/IEC JTC1 (25-29 October 2004 in Berlin, Germany) has established a Special Working Group on Accessibility (SWG-A) - ISO/IEC JTC 1 N7688
- “Accessibility” is one of the terms of reference of ISO / IEC JTC1 SC37 WG6
- The resolution 4 of the adopted by WG6 during the ISO/IEC JTC1 SC 37 working Groups meeting of Paris (November 2004) has instructed the Convenor to express to SWG-A the interest of WG6 in its activities



4.1 Accessibility & biometrics

- Accessibility in biometrics has two aspects:
 - Problems concerning disabled people
 - Problems concerning infants and elderly users
 - Both may encounter difficulties to correctly enroll and verify
- Large international projects (such as new electronic travel documents) have to keep these accessibility issues into the right perspective

4.2 Accessibility & biometrics

- Also in biometrics a sort “golden window” may be identified in the age of the users in which it is possible to obtain the best performances





4.3 Some classical accessibility problems in biometrics

- Absent, non usable or unstable physical body parts or behavioral features required for the correct operation of a biometric technique
- Inability to access, or difficulty in accessing the biometric sensor or user terminal
- Inability to understand the instructions, or recall the correct procedures



4.4 Some accessibility points addressed in WG6

- A biometric system should be easily accessible to all subjects and should not disadvantage any subject
- The operator/designer should take into account disabilities, inabilities and problems of subjects operating a system



5. Conclusions

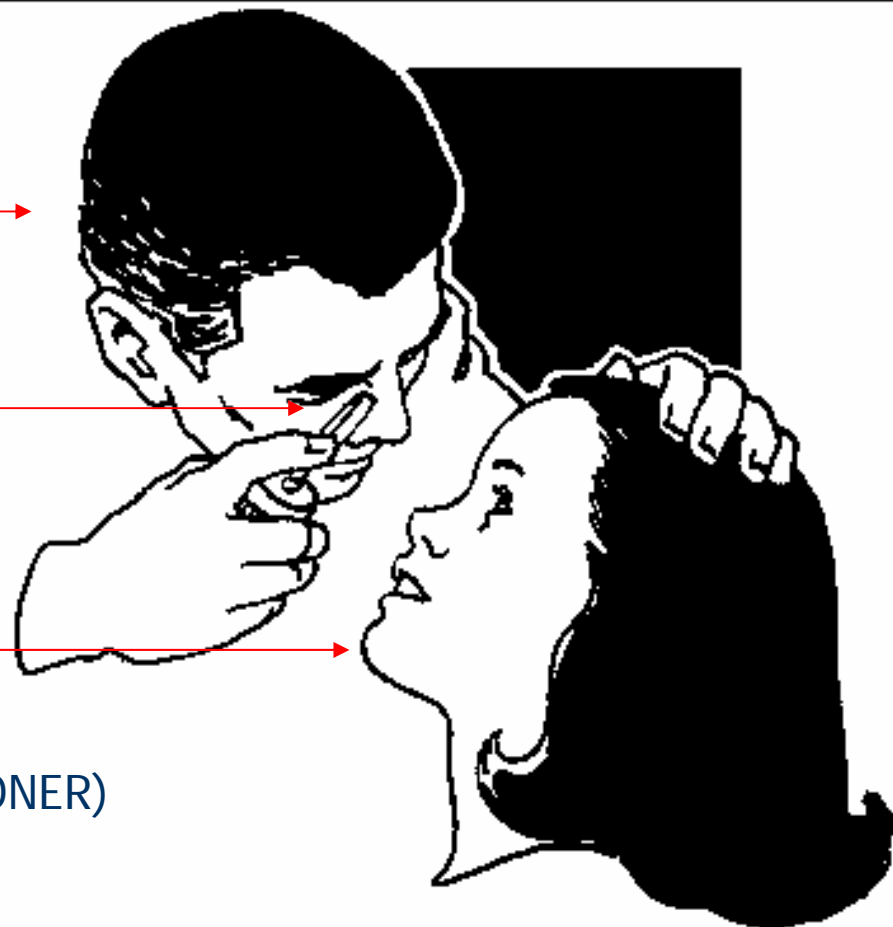
- An international coordination is needed to approach the problem of non-technical issues in biometrics, with particular reference to privacy issues
- The collaboration between US to EU in terms of trying to harmonize privacy issues in biometrics, should be enhanced
- ISO/IEC JTC1 WG6 may represent the “incubator” to attempt global harmonization into a wider international framework
 - Australia, Canada, France, Germany, Italy, Japan, Korea, Norway, RSA, Russia, UK, US

A strange examination

FALSE DOCTOR

NEW IRIS CAMERA

FALSE PATIENT
(DATA PROTECTION COMMISSIONER)



An overview of the European approach to the cross-jurisdictional and societal aspects of biometrics



Mario Savastano
Senior Researcher
IBB / National Research Council of Italy
DIEL - Federico II University of Napoli
Convenor
ISO/IEC JTC1 SC37 WG6 on
"Cross-jurisdictional and societal" aspects
of biometrics
mario.savastano@unina.it

Thanks for the attention !