Identity in the Information Society: Exploring Legal Approaches to the Use of Biometric Data

Annemarie Sprokkereef
ICS - University of Leeds
TILT- University of Tilburg

What is Biometrics?

- Biometric technology identifies individuals by means of biological characteristics through a pattern recognition system (face scan, fingerprints, iris scan and the list is growing)
- Relevant for EU: combined with ICT it makes unprecedented automation and checking against large data bases possible
- The use of biometrics is a key element of EU policies with stated objectives such as increasing safety, achieving interoperability of systems, availability of data, and more efficient immigration and border control

Current Situation

- Biometric identifiers have been introduced in passports, residence permits, visa, SIS II and the Eurodac system. A second biometric identifier will be added to some of these.
- Purpose specification for using the data collected left relatively open
- It has been left to member states whether or not to set up national databases containing the biometric data thus collected
- European wide biometric registers and data banks are policy objectives for the medium term.

Why use Biometrics?

Purpose of using a biometric can take three basic forms:

- Authorization (checking the right of a person)
- Authentication (checking the genuineness of a document)
- Verification (checking whether a person is the person claimed to be: data base)

Biometric applications (in the private and the public domain) often combine some of these basic purposes

Biometrics and Privacy

- Personal particular biometrics: can with reasonable effort be traced back to the person who has provided the biometrics
- Anonymous biometrics: cannot be traced back with reasonable effort
- Semi-anonymous: only the issuer of a biometric identifier knows the identity of the person whose biometric feature is registered

Opportunities

- “Anchor” for identity (Report on the Surveillance Society: 2006, p9) to which other data and information can be fixed
- Option to authenticate someone without identifying him or her (and other related privacy enhancing technology PET)
- Higher level of automatisation
- More efficient law enforcement

Complications

- Biometrics cannot be replaced
- Reliability of biometrics questioned (error rates and fall back procedures)
- Presence of biometric features in the public domain
- Some technological options tend to remain unexplored in the policy making process
- Absence of European standards
- big economic interests

Legal approach

- through data protection legislation
- Data protection core values are the principles of purpose specification, and proportionality (minimal collection, no use beyond original purpose, and maximum anonymisation of data)
- Legal sources: Data Protection Directive 95/46/EC and OECD Guidelines for Fair Information Practices
- Technical government (self) regulation by adhering to ICAO standards

EU Directive 95/46 and Biometrics

The directive applies to the processing of personal data and the term “biometrics” does not feature in the directive

- ‘Personal data’: any information relating to identified or identifiable natural person. Identifiable person one who can be identified directly or indirectly “by reference to an identification nr or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.
- Notion of identifiable is extensive and includes semi-anonymous data

EU Directive 95/46 and Biometrics (cntd)

- Interesting Article 29 working party working documents on biometric data
- Introduction of biometrics justified for security reasons, relatively lenient interpretation of proportionality and purpose binding principle in relation to the handling of biometric data by European authorities. Whether or not to set up a database left to national authorities and function creep not specifically excluded
- Large scale evaluation and impact assessment have only marginally taken place and few reports have been published.

Conclusions

- In the EU large scale (private and) public collection of information is already a fact of life and of that of biometric information a matter of time
- The question whether biometrics is the suitable primary key to make government more efficient and the EU safer remains unanswered yet, what about implanted RFIDs?
- Data protection law does not address new issues related to scale and new technological possibilities on time to meet the challenges that are arising
- Paradigm shift required from considering the effects on individuals (the basic test for data protection so far) to considering the impact on society.
- Technological possibilities to achieve more privacy by biometric system design are not used to the full, should setting of European technical standards be explored?

Thank you for your attention.

Comments and suggestions are most welcome!

A.C.J.Sprokkereef@uvt.nl