

At face value

6 Conclusions and practical directions

The determination of human characteristics, biometrics, is increasingly being used for identification and authentication of persons. Widespread introduction of biometrical identification techniques is about to happen.

Privacy issues concerning the use of the biometrics are generally seen as important topics to deal with before the general public is willing to accept this new technology. Biometrical data, apart from being unique identifiers of a person, can additionally contain data from which other personal information can be derived, such as race, mental and physical condition of a person.

The European Directive 95/46/EC gives the legal framework for the processing of personal data. In summary the main consequences of this Directive are:

- 1 In the context of biometrical identification, biometrical data generally classify as personal data in the sense of the Directive, at least in some stage of their processing. This implies that the processing of biometrics is processing of personal data and therefore should follow the Directive. We note that a (possible) exception is the case where the data are strictly for personal use only. In a few cases it can be argued that the biometrical data is processed in a purely personal activity, article 3(2) of the Directive, which implies that the rest of the Directive is not applicable. In all other cases the processing of biometrical data comes within the scope of the Directive.
- 2 The Directive reads that personal data must be (a) processed fairly and lawfully and (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The data collected for a certain purpose, e.g. identification, may only under certain conditions be used for other purposes. Also the data should be adequate and not excessive in relation to the purpose.
- 3 An important consequence is that persons should, in all cases, be informed that the collection of personal data takes place. The Directive also states that the purposes of the processing should be made clear to the person whose biometrical data are being collected.
- 4 Some personal data are classified as 'special categories of data'. The Directive states that Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Only in certain specified cases can this prohibition be lifted. In the report it is argued that some biometrics can be classified as such sensitive data. These data therefore should adhere to a stricter regime, dependent on the implementation in the different member states. In some cases explicit consent of the person involved is needed, in some other cases, e.g. the central storage of templates containing sensitive

data, it may be necessary to create a specific legal basis with all appropriate safeguards.

Besides these issues related to personal data, other privacy issues are relevant when biometrical identification or authentication is applied. These are:

- 5 Each human characteristic is unique, and therefore its digital representation or template can be used as a key to search databases that contain other personal data;
- 6 Certain human characteristics can be used for identification, and for other purposes such as the exposure of emotions, without the knowledge and the consent of the persons involved;
- 7 The quality of personal data can be at risk, because of the technical restrictions of the technology.

6.1 Recommendations

To minimise or eliminate the impact of privacy risks associated with biometrics, the following measures should be taken:

- 1 Analysis of the need for biometrical identification or authentication. Is the application of biometrics proportional with the goal to be achieved?
- 2 Decentralisation of the template storage and verification process; As a rule both the storage of templates and the verification process should be decentralised. In some specific cases and environments, the processing of personal data can be seen as a pure personal activity.
- 3 Encryption of databases: the protection of personal data can be realised by using different encryption keys and algorithms to encrypt the personal data (including biometrical data) in different databases. The original biometrics should preferably be destroyed after the derivation of the digital template;

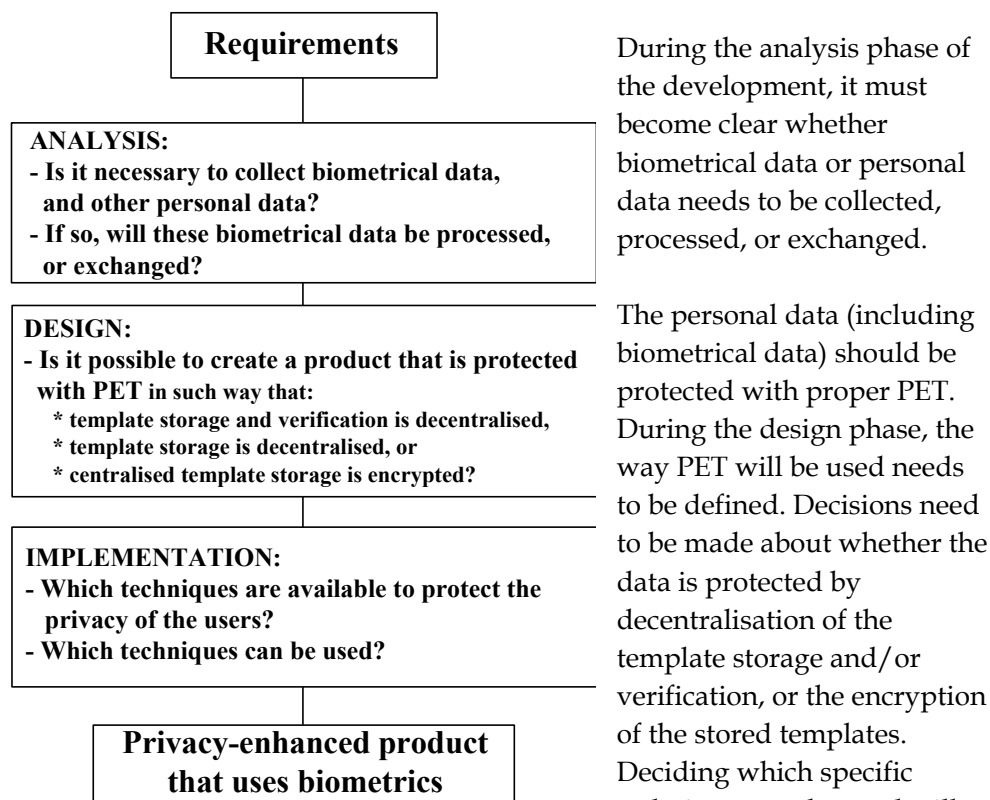
The individual whose human characteristics are measured may consider the following:

- 4 Use of different characteristics: the previous countermeasures should be integrated into the system. If a system does not contain any countermeasures, individuals can use different pseudo identities and different human characteristics to identify and/or authenticate themselves;
- 5 Use of scramblers: just like the use of different characteristics, individuals could use scramblers to randomly distort the results of the recording of the characteristic. This countermeasure can only be used for certain characteristics, like the voice.

Certification of the privacy-compliance of products will guarantee an adequate handling of the personal data of future users.

Designers, developers, suppliers, and users of products using biometrics for identification, authentication, or exposure of emotions need to consider ways to protect the privacy of the users. Figure 13 provides a checklist with practical directions, for those who want to build a privacy-enhanced product that processes biometrical data.

Figure 13: Aspects to take into account during the different phases of the design process of a product using biometrical identification.



take place during the implementation phase.