

dr. R. Hes
mr. drs. T.F.M. Hooghiemstra
drs. J.J. Borking

With contributions from: P.J.A. Verhaar, T.G.A. van Rhee and
H.A.M. Luijff (TNO Physics and Electronics Laboratory – The Hague)

At face value

On biometrical identification and privacy

Registratiekamer, september 1999

Preface

New ways of doing business are developing at a quick pace. Activities that were once part of our everyday lives are more and more replaced by information technology. In the near future many transactions will no longer be performed by traditional methods, like face-to-face contacts or regular mail. Instead computer networks will be the new vehicles. As persons are physically separated, new and secure methods of identification and authentication are required. The most promising method certainly is biometrical identification, the use of unique human characteristics for these purposes. The widespread introduction of techniques applying biometrics can now be witnessed.

The promise of biometrical identification as a method for secure identification is accompanied by concerns about privacy. The biometrical data, by their nature as unique identifiers, may become a key to track a person's everyday activities. Also the biometrical data may reveal much additional information about a person, such as health status or race.

This report reviews the technologies available for biometrical identification. It also offers guidelines, both from a legal and from a technological perspective, how biometrical identification can be applied in such a way that the privacy of citizens is respected and protected. Applications can be configured to give data subjects the ability to control access to their own biometrical data, to safeguard the integrity of their personal information, and to protect their identity against theft or misappropriation. I hope these guidelines will help to preserve the human face of the information society.

Peter J. Hustinx
Chairman Registratiekamer

Reports in the series Achtergrondstudies en Verkenningen (Background studies and Investigations) are the result of enquiries carried out by or on behalf of the Registratiekamer. The Registratiekamer hopes that the publication of these reports will stimulate discussion and shape public opinion on social developments which have an impact on the personal privacy of the citizenry.

At face value – On biometrical identification and privacy
Registratiekamer, The Hague, september 1999

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form of by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the Registratiekamer.

ISBN: 90 74087 17 5

Print: Sdu Grafisch Bedrijf

Contents

1	Introduction	7
1.1	A brief outline of the report	8
1.2	Studies concerning privacy and technology	8
2	Biometrics: a technology scan	9
2.1	Biometrics for identification or authentication	13
2.1.1	Identification and authentication	13
2.1.2	Working of products	15
2.1.3	Characteristics used for identification or authentication	20
2.1.4	Comparison of reliability of different techniques	25
2.1.5	Acceptance of biometrics	26
2.2	Biometrics to expose emotions	27
2.2.1	Definition of 'state of mind'	27
2.2.2	How are emotions expressed in the human voice	28
2.2.3	How can emotional expressions be identified by software	29
2.3	Future developments	30
3	Legal aspects	32
3.1	Personal data or not	35
3.2	Processing personal data	36
3.3	Scope of the Directive	36
3.4	Processing of biometrical data	37
3.5	Information to be given to the data subject	35
3.6	Special categories of data	39
3.7	Consequences of qualification as special personal data	40
3.8	Security of processing	39
4	Biometrical identification and privacy-related issues	41
4.1	Biometrics for identification and authentication	44
4.1.1	Known identification or authentication	44
4.1.2	Unknown identification or authentication	45
4.2	Biometrics and emotions	47
4.3	Biometrics and technical restrictions of systems	47
5	Biometrics and Privacy-Enhancing Technologies	48
5.1	Privacy-compliant design of biometrical systems	51
5.1.1	Decentralising template storage and verification	52
5.1.2	Encryption of databases (if templates storage centralised)	53
5.1.3	Use of different human characteristics	55
5.1.4	Certification of products that contain PET	55

5.2 Unknown identification or authentication 56

6 Conclusions and practical directions 55

6.1 Recommendations 56

Appendix A Privacy-Enhancing Technologies

Appendix B Terminology used in Directive 95/46/EC

Summary

Samenvatting

Introduction

1

1 Introduction

The way in which individuals and organisations perform transactions is changing rapidly due to new information and communication technologies. The trust needed to come to an agreement during a transaction has long been based on personal contacts between the parties involved or on certain established institutions, such as family ties or the help of trusted persons, such as notaries. Parties involved in transactions generally wish to identify their business acquaintances. One way to do this, is by means of official identity documents, such as passports, containing a photograph. This presupposes that someone is presenting this document in person at some stage of the transaction process. With increasing use of information technology this method of identification is no longer practical.

The scale of economic activities has increased in the last decades, and geographical limits have become less relevant. This leads to long distance transaction, where transactions are made, while interacting only through computers and using networks for communication. These new modes of doing business ask for a way to secure trust. Since the parties involved cannot confirm their identities directly, different methods of identification or authentication are required. Examples are the use of tokens and secret passwords or PIN-codes. These methods however are susceptible to misuse and fraud, because tokens and passwords belonging to a certain person can be passed to another person. To make transactions more secure, stronger forms of identification are required. Some human characteristics, that are proven to be unique for every individual, can be used for stronger forms of identification, because they can not be passed to other persons. Examples of such characteristics are fingerprints, voice, iris, and signature. The discipline that studies these human characteristics is called biometry, or biometrics.

People have been identifying others by specific physical characteristics. Because of the uniqueness of these characteristics, it is possible to distinguish one person from the other, or to verify the authenticity of documents. Technologies have recently been developed that automate the capturing, or recording, and verification of various human characteristics. The rise of the techniques using biometrics can mainly be attributed to the quality increase of the sensors used to capture the characteristics.

At this moment an important transition is occurring: identification systems using biometrics are leaving the stage of specific applications within a limited setting. Instead, mass applications will be introduced in the coming years, for such general purposes as identification or authentication to control access to buildings and automatic teller machines. The numerous technical possibilities of biometrics promise more secure and efficient identification and

authentication in diverse settings. However, biometrics has to face considerable restraint or even opposition by the potential user community.

One aspect of user acceptance is the concern for privacy. The introduction on a large scale of identification systems that all use the same human characteristic may oblige citizens to present their human characteristic in many circumstances. Such ubiquitous use of the same unique identifier, e.g. a person's fingerprint, facilitates the assembly and accumulation of information related to this person. The human characteristic, potentially, becomes the key with which a dossier tracking a person's private life can be made. Practice shows that such accumulations of personal data will ultimately be used for unintended or even unlawful purposes. Moreover, some human characteristics may themselves contain additional sensitive information, e.g. on race or health, and therefore their proliferation is undesirable. Both aspects of these unique identifiers raise considerable concern: the function as a 'universal' key to personal data, and the function as privacy sensitive data. Some analysts sketch the doom of a society where biometrical techniques are applied for omnipresent surveillance.

1.1 A brief outline of the report

The report starts in chapter 2 with a short inventory of biometrics in general and identification or authentication methods using biometrics in particular.

Chapter 3 describes the most relevant legal aspects concerning the application of biometrics. The current legislation on the protection of personal data offers a normative framework to regulate the use of biometrical data. As starting point, the issue whether human characteristics come within the scope of the European Directive 95/46/EC is addressed. This study focuses on the practice of identification or authentication with the use of biometrics. A sketch is given how legislation translates into practice for identification with the use of biometrics, adhering to the relevant European legislation. In broad terms the results are valid in all member states.

After the normative framework has been sketched, the report addresses the possibility to limit the amount and use of generated personal data by means of technical solutions, see chapters 4 and 5. The application of Privacy Enhancing Technologies in the domain of identification with the use of biometrics is investigated.

¹ Hes, R. and Borking, J. (editors) e.a. (1998) *Privacy-enhancing technologies: the path to anonymity*. Revised edition. A&V-11. Den Haag: Registratiekamer, 1999.

1.2 Studies concerning privacy and technology

The Registratiekamer, in association with TNO-FEL, conducted an earlier study of technologies that could improve the privacy of individuals. The

results of that study are published in *Privacy enhancing technologies: the path to anonymity*¹. A summary of the results of this study is included in Appendix A. Two of the technologies studied were blind digital signatures and Trusted Third Parties (TTP's).

The Registratiekamer believes e.g. that (intelligent) agent technologies could jeopardise the privacy of individuals. However, these technologies might also be used to protect the privacy of individuals. A special privacy software agent could be developed to exercise the rights of its user, and to enable this individual to protect himself or herself against privacy intrusions with the aid of PET. Therefore, the Registratiekamer decided to study the privacy aspects of these agent technologies pro-actively. This study was also conducted in co-operation with TNO-FEL².

² Borking, J. e.a. (1999)
Intelligent software agents and privacy. A&V-13. Den Haag:
Registratiekamer, 1999.

Biometrics: a technology scan

2

2 Biometrics: a technology scan

According to the Penguin Concise English Dictionary biometrics stands for: 'application of mathematical and statistical methods to the study of biology'. Biometrics thus is about analysing biological observations with mathematical and statistical methods. The following examples illustrate the use of biometrics:

- 1 calculation of the average age of a specific part of a population;
- 2 calculation of the average length of a specific part of a population;
- 3 calculation of the average growth of certain plants;
- 4 calculation of the average propagation-time of certain animal-species.

The medical community has proven that certain human characteristics are practically unique for every individual. These characteristics can be physical, such as fingerprints and facial expressions. These characteristics can also be based on behavioural patterns, such as putting one's signature on a document or a specific keystroke pattern when typing documents. The use of this uniqueness has been applied since long in some specialised branches, like e.g. the identification of corpses by the police or the military using the uniqueness of the teeth, the bone-structure, fingerprints, or DNA. Recently, specific characteristics are more and more applied in the information security branch, to control the access of authorised users to a location, or an information system. The characteristics are used to identify and/or authenticate the authorised users.

It has also been proven that some of these characteristics are influenced by certain emotions which the owner of the characteristics displays. This aspect of biometrics has since long been applied in lie detectors. New developments concern the development of products that can be used to expose (hidden) emotions of persons one is speaking to, or negotiating with.

It should be emphasised that some human characteristics can be used to derive knowledge with far reaching consequences. DNA, for instance, could reveal not only the identity of a person but also his or her genetic properties, such as likeliness to develop diseases. A remarkable example is the use of genetic information derived from DNA of the entire Icelandic population by a pharmaceutical company¹. This illustrates the potential of biometrics applications. It was decided to focus this study on to the use of biometrics for identification or authentication purposes only, as these applications are being introduced on a massive scale, but products to expose emotions will be discussed also. The use of biometrics for identification (and/or authentication) and the exposure of emotions will be described in the next paragraphs.

¹ Schwartz, J. (1999). *With gene plan, Iceland dives into a controversy*. *International Herald Tribune*. January 13.

2.1 Biometrics for identification or authentication

It is of importance for the continuity of business processes of organisations to control the access to information systems and buildings. The protection of data consists of several aspects: the confidentiality, integrity, and availability of the stored data and the integrity of imported data. To ensure the confidentiality, (part of) the integrity, and (part of) the availability of data kept within an information system, only authorised persons should be allowed to gain access. To validate access to the information system, or building the authorisation needs to be inspected. This inspection is practically always combined with the release of the consumer's identity (identification).

To ensure the integrity of imported data the source of these data, and the communication means need to be reliable. To decide whether a source is reliable or not one needs to obtain credentials of the source. As in gaining access to a building or information system, the identity of the source is also released to decide if a source is reliable (identification). The next paragraphs describe how the identity can be verified (identification and authentication) by means of biometrics, and with what human characteristics this can be accomplished.

2.1.1 Identification and authentication

The authorisation, or the reliability of a person is often related to the 'identity' of this person. In general this 'identity' is a representation of the person's real identity. In other words: the 'identity' is in fact an entry under which a person is known to an organisation or an information system. This 'identity' needs to be unique, to make sure that this 'identity' can univocally be appointed to a particular living person. In order to gain access, or to prove his or her reliability (credentials), a person needs to present his or her 'identity'. This is called 'identification'. With identification, the existence of a specific 'identity' in a reference-source is verified (in case of access control such a reference-source is often called access-control-list).

The 'identity' can be represented by:

- 1 something a person possesses, like a key or a token (e.g. a chipcard);
- 2 something a person knows, like a user-id or PIN-code;
- 3 something a person is, like human characteristics.

Using only identification to grant access, or to declare a person as reliable can cause unnecessary risks. In such cases, 'identities' should be unique and only to be reproduced (for something a person knows), or shown/used (for something a person possesses or is) by the person the 'identity' belongs to. If other persons can reproduce the 'identity', these persons can gain access under

a false 'identity'. The loss of a token (something a person possesses), or the reproduction of this, may lead to unwanted access or the acceptance of unreliable sources. So, 'something a person possesses' can be seen as the weakest of the three ways to represent the real identity.

PIN-codes and passwords (something a person knows) can be forgotten, or guessed by others. To prevent guessing of PIN-codes, or user-id's, the production of these 'identities' needs to follow certain rules, such as: no use of family names etc., no use of existing words, and no easy combinations of figures or characters. Using these rules will not make it easier to remember several 'identities', and could cause problems for the right person to reproduce them.

Unlike 'something a person knows' and 'something a person possesses', human characteristics are basically irreproducible, or transferable to other persons. This is a major advantage of an 'identity' that consists of 'something a person is'. There is no need for the person to remember his or her 'identity'. He or she only needs to remember which characteristic to present. It should be noted that in all three cases it is possible to capture the representation of the real identity under compulsion of the person this 'identity' belongs to.

To obtain more confidence in the 'identity' one can perform an extra verification of his or her 'identity' (Is the person really who he or she claims to be?) This is called verification of the 'identity', also known as authentication. This can be accomplished by combining two or more details of 'something a person possesses', 'something a person knows', or 'something a person is'. One of these details can be used as the 'identity', while the other detail(s) can be used to perform a second check. When using two or more details, the 'identity' doesn't have to be kept secret, but it still needs to be unique. The other detail(s) still need(s) to be kept secret. After presenting the identifying information, the controlling organisation checks the reference-source if the 'identity' exists. The reference-source also contains the other detail(s), which are related to the 'identity'. Now, the organisation will verify the other detail(s) with what is given to them by the person.

Not all combinations of 'something a person possesses', 'something a person knows', or 'something a person is' are useful, especially when two tokens are used or two human characteristics. The following combinations are commonly used:

- 1 a user-id or client-number (something a person knows) for identification, combined with a PIN-code or a password (something a person knows) for authentication;
- 2 a token (something a person possesses) for identification combined with a PIN-code or a password (something a person knows) for authentication;

- 3 a user-id or client-number (something a person knows) for identification, combined with a human characteristic (something a person is) for authentication;
- 4 a token (something a person possesses) for identification combined with a human characteristic (something a person is) for authentication;
- 5 a token (something a person possesses) for identification combined with a PIN-code or a password (something a person knows), and a human characteristic (something a person is) for authentication.

Identification (and authentication) can be implemented in several ways, although these ways are subject to two limitations. The implementation extremes are incidental identification (and authentication) and continuous identification (and authentication). With incidental identification, the 'identity' of a person is only checked when gaining access to a building or information system. The same goes for deciding whether a source is reliable. Only at the beginning of a session the 'identity' is checked. When a person has accessed a building or information system, however, someone else can take over the activities of the identified person. This can be prevented using periodic or continuous identification (and authentication). With periodic identification, the 'identity' will be checked frequently during the presence in the building or information system, or during the existence of the session. When using continuous identification, the 'identity' is checked every moment (continuously) during the presence in the building or information system, or during the existence of the session. Some human characteristics in particular like the voice, or keystroke patterns, can be used to carry out continuous identification (and authentication).

2.1.2 Working of products

The system for using biometrics for identification or authentication consists of:

- 1 a sensor that records the human characteristic that is presented;
- 2 a verification device that identifies a user (identification), or verifies the identity of a user (authentication);
- 3 a template database where reference material for the identification or authentication of users is stored.

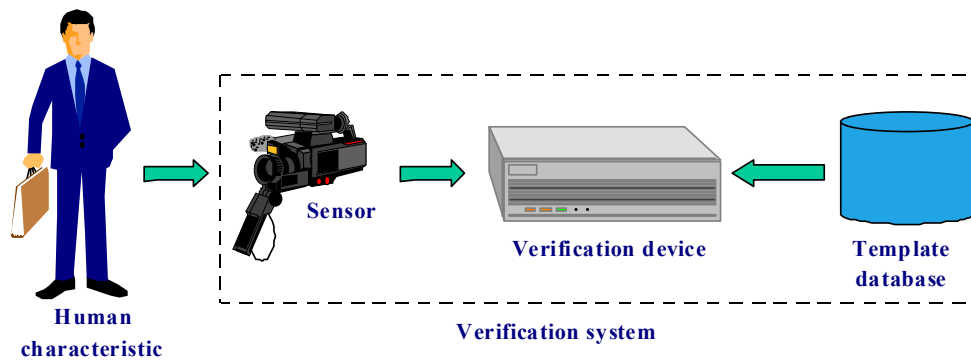


Figure 1. An example of a system using biometrics for identification or authentication: a verification system. The sensor, verification device and the template database do not necessarily have to be integrated. The three components can be physically dislocated: e.g. the template could be stored on a token (like a chipcard) and the user could hold the token for safekeeping.

The human characteristic presented by a user will be recorded using a sensor. The sensor translates the human characteristic into a digital representation, which is often called the biometrical bit pattern. This bit pattern will either be used for the identification or authentication of the user. To verify this bit pattern, the verification device needs to have a reference that is stored in the template database, to compare the bit pattern with. This reference, which is called a template, is generated during the initialisation phase. During this phase, the human characteristic of a future user is recorded several times, to allow the system to remove variations and deviations between the recorded bit patterns. The similarities in the bit patterns that stem from these recordings will be converted to the template (figure 2.a). During the operational phase the recorded biometrical bit pattern will be compared with the templates stored earlier in the template database.

When only the human characteristic is presented (identification), the verification system needs to check all templates that are stored in the template

database (figure 2.b). The template database and verification device need to be integrated.

If the human characteristic is used to authenticate the identity of a user, the identity of the user also needs to be presented to the verification system. The templates in the template database are stored in combination with the identity of the user. The verification device only needs to compare the presented bit pattern to the template that belongs to the identity given by the user (figure 2.c). In this case the verification system needs to be extended with a keyboard to enter an account name or a user-id, or a device to communicate with a token: e.g. a card acceptance device to communicate with a chipcard. The chipcard can also serve as a part of the template database, containing the template of the chipcard owner.

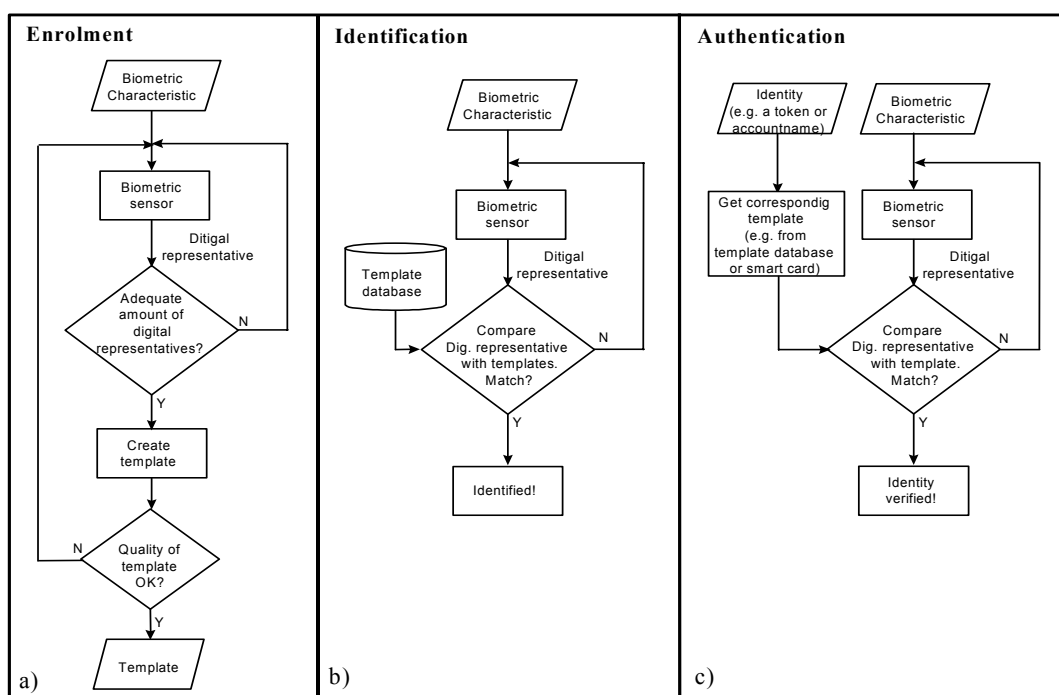


Figure 2: Possible diagrams for the enrolment phase and the operational phase: a) enrolment phase; b) operational phase of a system that uses biometrics for identification; c) operational phase of a system that uses biometrics for the verification of a given identity (authentication).

As mentioned before, two phases can be distinguished: the initialisation phase or enrolment phase, and the operational phase. During the enrolment phase, the system will define the templates of the users, while during the operational phase the system will identify or authenticate the users. Possible diagrams of these phases are given in figure 2.

During the enrolment phase, which is illustrated in figure 2.a, the template that is used as comparative material for the identification or authentication is created. First the human characteristic of a person has to be presented to the sensor. The sensor converts the human characteristic into a digital representation and records this. When creating a template, the conversion of the human characteristic into a digital representation has to be executed more than once. The similarities from the several digital representations are used to create the template. Figure 3.a gives a simplified example of how digital representations are used to create a template. The corresponding digits (bits) from the several digital representations that are equal to each other are used in the template. Corresponding digits that are not equal will not be used, and are illustrated in figure 3.a as an 'x' in the template. The 'x' can be seen as 'don't care' digits. The value of these digits is of no importance to the identification or authentication of individuals. After the template is created, the quality of the template needs to be checked. The template needs to contain enough digits that represent a value, other than 'don't care'. During this check the system also investigates if a comparable template does not already exist. If all checks out fine, the template can be stored in the template-database or on e.g. a chipcard.

Figures 2.b and 2.c both illustrate the operational phase, where figure 2.b describes a system that uses biometrics for the identification of individuals and figure 2.c describes a system that uses biometrics for authentication. The difference between figures 2.b and 2.c lies in how the system compares the digital representation with the template. For identification, the system checks if the digital representation is 'equal' to one of the templates that are stored in the template database. For authentication, the system checks if the digital representation is 'equal' to a specific template. In this case, the templates need to be stored in combination with an (database) entry, which needs to be supplied (identification) by the individual who will be authenticated.

b15	b0	
1 0 1 1 0 1 0 1 1 0 0 1 1 1 0 1		Digital representative 1
1 0 1 1 1 0 0 1 1 1 0 1 1 0 0 1		Digital representative 2
1 0 1 1 1 0 0 1 1 1 0 1 1 0 0 1		Digital representative 3
<hr/>		
1 0 1 1 x x 0 1 1 x 0 1 1 x 0 1		Template
a)		
b15	b0	
1 0 1 1 x x 0 1 1 x 0 1 1 x 0 1		Template
1 0 1 <u>0</u> 1 0 <u>1</u> 1 1 0 0 1 1 0 0 1		Digital representative 1
1 0 1 1 0 1 0 1 1 1 0 1 1 1 0 1		Digital representative 2
b)		

Figure 3: Simplified representation of a comparison-mechanism of systems using biometrics for identification or authentication: a) the creation of a template; b) the comparison of digital representations with the template.

When comparing the digital representation with the template, the digits of the digital representation corresponding with the template's 'don't care' digits will not be

taken into account. All other corresponding digits need to match. In figure 3.b digital representation 1 will be rejected by the system, because two digits do not match the corresponding digits of the template. Digital representation 2 will be accepted by the system, because all digits match the corresponding digits from the template.

Under certain conditions the system could fail. The system could produce digital representation 1 (figure 3.b) from the human characteristic of the person to whom the template belongs. Note that digital representation 1 does not completely match the template. It is also possible that the system produces a digital representation of a person who is not linked to the templates stored in the template database. The system may still accept it as a valid match. Conditions that can cause a failure are environmental conditions such as temperature variations and the presence of dust; and behavioural conditions such as stress and sweat.

A rejection by the system of someone truly linked to the template used for comparison is called a 'false rejection', and will decrease user acceptance of such a system. An acceptance of someone who doesn't belong to the template used for comparison is called a 'false acceptance', and could cause a security violation. The technical specifications of these tolerances are given with the 'False Rejection Rate' (FRR) and the 'False Acceptation Rate' (FAR). These two rates are related as illustrated in figure 4.

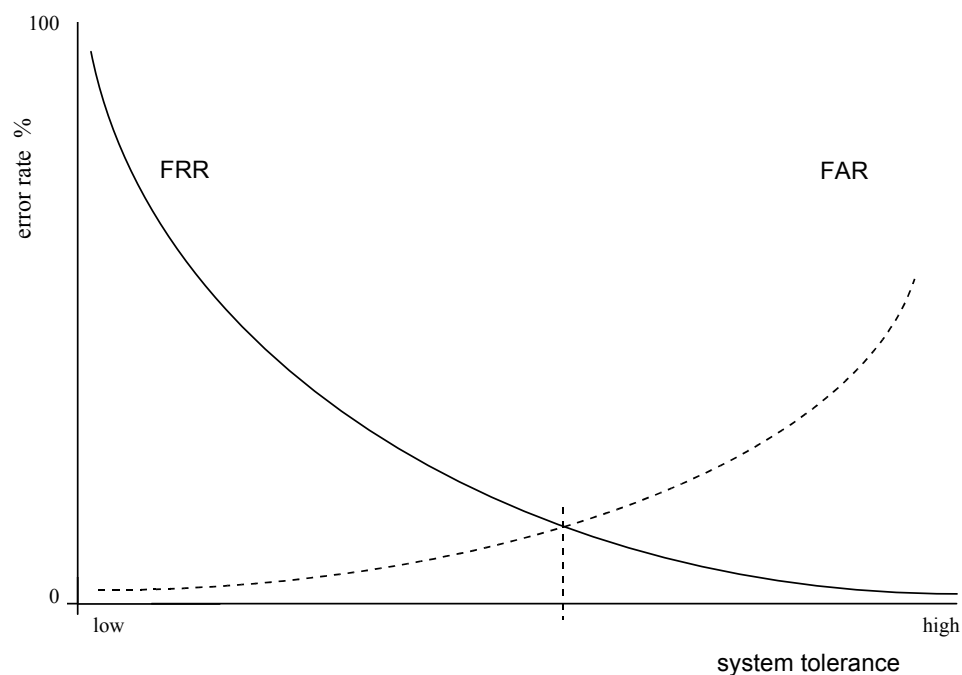


Figure 4: Relationship between FAR and FRR. The vertical axis represents the fault tolerance for the FAR and the FRR expressed in percentages. The horizontal axis represents the system tolerance that can be adjusted.

The default settings of most products are adjusted so that $FAR = FRR$. As shown in figure 4 it is clear that if the FRR is low, the FAR will be high, and if the FRR is high, the FAR will be low. With a product that is adjusted in such way that authorised users will rarely be rejected (FRR is low), the chance that unauthorised persons gain access will increase (FAR is high). A product that denies access to all unauthorised persons (FAR is low) needs to be very accurate. Such an accurate product will lead to an increased chance of the rejection (FRR is high) of authorised users. Depending on the security requirements of the system, in which the product that uses biometrics is integrated, these settings can be adjusted to obtain the required security level.

2.1.3 Characteristics used for identification or authentication

As mentioned earlier human characteristics can be divided into two categories: characteristics based on physical aspects such as fingerprint, facial features and DNA (physical characteristics) and characteristics based on behavioural patterns like signature and voice (behavioural characteristics).

Fingerprint

The fingerprint is well known for its use to identify individuals. Positions of details, which are unique for every person, are used for identification. These details, known as minutiae, can be endpoints, junctions, arches, loops, and whorls in the fingerprint pattern. The fingerprint is practically stable from birth to death, and therefore, the template does not have to be updated frequently. However, the reliability of the identification or authentication is negatively influenced by a wrong placement of the fingerprint, by environmental conditions, such as dirt, and rain and by certain conditions of the finger, such as chaps, incisions or the quality of the fingerprint itself. According to E. Newham², the latter aspect is particularly sensitive to race, gender, occupation and age. Because of the smooth skin of persons that belong to specific races e.g. it can be difficult to produce a valuable scan of the fingerprint.

During the process of fingerprint recognition, a scan of the fingerprint is made, resulting in a picture of grey shades. In order to simplify the recognition, this picture will then be reduced to a black and white picture. This black and white picture will be used to define the details that will be used to create the template.

The use of fingerprints for identification or authentication is now well established, and many products are available. At first, devices using biometrics were developed to control access to objects and/or buildings. These devices needed to work independently (stand-alone devices). Nowadays, products are developed to control access to computer systems. This means that these devices can be integrated in computer systems, using this system's resources. Due to the dimensions of the fingerprint and the scanners used to record these prints, these products can also be integrated in peripherals, such as a computer mouse (BioMouse) or a keyboard (Secure Keyboard Scanner). This enables periodic or even continuous (identification or) authentication.

Banking organisations that plan to use the fingerprint as a replacement for the PIN-code, would like to introduce a so-called alarm-finger. The alarm-finger is a different finger than the finger that is used for the actual identification or authentication. When the alarm-finger is used, the bank will know that its customer is forced to present the fingerprint to the identification or authentication product. The enforcer must be under the illusion that the customer used the right fingerprint, so the banking services have to perform as if nothing is the matter. Meanwhile, actions to protect the banking services and the safety of the customer will be (need to be) taken.

Hand scans

The following details of the hand can be used for identification: finger length, the lines of the palm print (equal to a finger print), vein patterns on the back of the hand, hand geometry and finger geometry. For the method of vein recognition, a two-dimensional scan is made of the vein pattern. This scan will be transformed into a grey-scaled picture, and then stored in a template.

In case finger and hand geometry is used, the 3-dimensional shapes of respectively the finger and hand is captured. Details that can be used with hand geometry are the length of the fingers, the thickness of the hand, the shape of the hand and the brightness of the skin. The same details are measured for finger geometry, but only for two fingers instead of an entire hand. By measuring the brightness of the skin some information about the colour of the skin and probably the race can be extracted during the process of scanning. Contrary to the fingerprint, finger and hand geometry is not susceptible to incisions and chaps. Finger and hand geometry can still be influenced by major injuries of the fingers and the hand, and environmental conditions, such as dirt.

For finger and hand geometry, products are available (e.g. Digi-2 by BioMet Partners, and ID3D Handkey by Recognition Systems Inc.). Products that use palm print for identification or authentication are also available. DermoTrade offers the product Automatic Dermatoglyphical Identification System, which

uses the palm print for identification. The Papillon-7 (Papillon Systems), and RECOderm system (KFKI Computer Systems) are also products that use the palm print for identification, or authentication. For vein pattern recognition there are advanced developments that may lead to the release of products in the near future.

Eye patterns

One of the best ways of identification can be obtained by using certain characteristics of the eye. Both retina and iris contain unique and stable details that can be used for identification. With respect to privacy it could theoretically be possible to deduce sensitive information about the health of users because certain diseases influence some features of the eye. Iridology e.g. is a form of diagnostics, which makes it possible to recognise diseases by tracing abnormal spots, lines, and features in the iris. Official medical science attaches little value to iridology. This, however, may not reflect the opinion of many individuals, who may resist biometrical identification on basis of their belief in iridology or similar types of diagnostics.

In chapter 3 the report will discuss further the fact that biometrical data may contain other information about a person than strictly necessary for identification.

Several products for eyescanning are now on the market. The 2001 from EyeDentify uses the vein pattern from the retina for identification. The TC-2001 version can also be used for authentication. EyeDentify owns U.S. and international patents which protect the rights for exclusive use of retinal technology. IriScan developed the System 2100 that uses the iris for identification or authentication, and has also patented this technique. Iriscan, in co-operation with British Telecom laboratories, also developed a prototype hand-held Identifier. NCR will market this year an ATM with retina identification, replacing PIN codes.

Facial features

The face is a primary characteristic used for recognition of human beings. Difficulties of using this characteristic are changes of appearances, such as variations in facial expressions, or hairstyles. Details of this characteristic are: the distance between the eyes, the hairline, and the outline of the face. Also the colour of the skin can be measured and privacy sensitive information such as race can be obtained. Measuring only these details, it is still possible that identical twins will not be recognised as different persons. Therefore another detail, that is not visible for the human eye, can be used, such as the blood vessel pattern of the face. To record this detail different techniques, that range from infrared scans of so-called 'hot to pattern recognition based on neural networks, can be used. The colour of the skin does not influence the image of

the infrared scan of the face. Information about race can not be obtained from the infrared scan.

There are quite a number of companies that produce commercially available facial systems. Most of these products are based on the measurement of the distances between the eyes, the nose, and the mouth and the outline of the face. At this moment there are products that use the heat pattern of the face as measured by an infrared camera. There are also quite a number of companies that have facial systems under development, or that have facial recognition research projects. These developments and researches will probably lead to a notable amount of new commercially available products.

Ear pattern

The size of the ear, the shape and the outline are unique details that can be used for identification. With the help of a video camera a picture is taken from the ear which will then be used for further identification or authentication (verification). As far as known there are few products available that apply ear pattern recognition. One of these, created by ART Techniques called Optophone, is built into the ear part of a telephone.

Body scent

This characteristic consists of approximately thirty chemical substances that form a specific unique scent for every individual. An electric nose can be built, consisting of a number of chemical receptors that generate a difference in voltage in case a particular chemical substance is present. With the help of neural networks it is possible to disentangle specific scent patterns.

At this moment there are no commercially available products. Mastiff Electronics is developing a product that will probably be launched around the beginning of the new millennium. The Tufts University is discussing the commercialisation of a scent recognition system developed by laboratories in the chemistry and neuroscience departments of this University.

DNA

All human cells, except for the red corpuscles, contain a core of genetic information, which is unique for every individual. This is called DNA. Identification or verification using DNA is often used in forensic laboratories. The amount of material needed for such an analysis is very small; e.g. one hair is sufficient. At this moment, there is still a strong resistance against the use of DNA for identification and/or authentication in more common applications. This resistance lies in the fact that human cells need to be taken from the human body, as well as the potential (mis)use of additional information contained in the DNA.

Signature

Seals and signatures are behavioural characteristics and have been commonly used to identify the originator and to verify the authenticity of documents. There exist two methods to identify a person based on signatures. The first method compares already written signatures with a signature from a reference-source. The second method examines the dynamics of the signature when it is written down. Details of this characteristic are the writing rhythm, contacts on the surface, total time, turning point, loops, slopes, velocity and acceleration, and pen pressure. It is very difficult to imitate a signature that is controlled dynamically.

Most of the commercially available signature systems, and signature systems under development are based on dynamic signature verification. There are about ten products commercially available, and about the same number are under development.

Voice

As mentioned before, people can recognise acquaintances by listening to their voices. A voice obtains its unique character because of the unique sizes of the nasal cavity (or nasal passage), pharynx and mouth. Machines can recognise unique details of the human voice that cannot be heard by humans. It is therefore impossible for humans to imitate voices in such way that a machine fails to recognise this. Among the currently developed identification methods, voice recognition is probably the most advanced and of particular relevance to the telecommunications industry. Voice recognition or *speaker recognition*³ is a method to analyse features of a person's voice to identify the voice of an unknown speaker, authenticate a person or recognise a voice of a person in an environment with many speakers.

It should be noted that, unlike most other biometrics identification methods, speaker recognition often uses existing infrastructure and hardware, such as the telephone network and relatively cheap microphones. In all cases a person's voice is measured and compared to a previously recorded and stored *template* or *voiceprint* of his or her voice. The following cases should be distinguished:

- 1 Text dependent systems. Best results in recognising persons, in terms of failure rates, are obtained if the same words are used for input and for the template (think of a predetermined password or ID). When entered, this is matched to a stored voiceprint.
- 2 Text prompted systems. In these systems speakers are prompted to repeat randomly selected words, which are being matched to the template. An advantage is that impostors who use voice samples recorded on tape cannot mislead the system.
- 3 Text independent systems. In this case a person is asked to talk and his utterances are matched with the stored templates, containing completely

different words. This situation offers much more contingency, and hence the matching is more difficult, in particular if background noise is present or noisy telephone lines are used. On the other hand the potential of these systems is high: combined with a large database of voice templates, a text independent systems enables identification of many different persons in many circumstances.

Keystroke dynamics

Every individual has his unique pattern or rhythm of typing. The typing speed, the duration of a keystroke, time lapses between keystrokes, and time lapses when two keys are stroked simultaneously are details of a user's typing that can be used for identification. During the enrolment phase the average and deviation of these details are calculated and stored in a template for further use. Identification of individuals is easier when these individuals are trained typists.

³ Speaker recognition should not be confused with speech recognition, the interpretation of spoken commands by machines.

At this moment, there are at least two products that are commercially available. The first product (Electronic Signature Lock) is developed by the Electronic Signature Lock Corporation. The other product is developed by Trove Investments. This product (BioPassword) uses keystroke dynamics for the restriction of access to sites and services on the World Wide Web (WWW), and is integrated in the NetNanny software suite. There are a couple of universities and research laboratories that study keystroke dynamics, and are developing identification, or authentication systems using this technology. TNO-FEL in the Netherlands is one of the laboratories that develop a system based on keystroke dynamics.

2.1.4 Comparison of reliability of different techniques

Figure 5 shows a comparison of biometrics techniques with respect to several (most used) characteristics. Although the table does not capture all relative advantages and disadvantages, it does show that each characteristic has relative merits.

	<i>Reliability</i>	<i>Acceptance</i>	<i>Template</i>	<i>Costs</i>
<i>Fingerprint</i>	good	good	small	low
<i>Hand</i>	good	good	very small	moderate
<i>Eye</i>	very good	moderate	moderate	high
<i>Face</i>	good	good	small	moderate/high
<i>Signature</i>	moderate	very good	small	moderate
<i>Voice</i>	good	good	small	low
<i>Keystroke</i>	moderate	good	small	low
<i>DNA</i>	very good	poor	moderate	high

Figure 5: Comparison of biometrics techniques with respect to several characteristics.

As for reliability, all techniques will perform well under ideal conditions. However, reliability rates suffer under less than ideal conditions. The eye has very good reliability rates, where signature and keystroke have moderate rates. With respect to the acceptance of biometrics techniques the signature scores well, because it is used in a way similar to traditional signing. The acceptance of the eye scan methods is moderate because of the required short distance between the user's eye and the sensor. The next column, on the size of the reference template, shows that hand-scanning can work with small templates. Because the eye requires highly detailed pictures the particular template is fairly large. The last column represents a general overview of the costs of the biometrics systems. Most techniques are now available at reasonable costs, except eyescanning and determination of the facial heat pattern, which are relatively expensive.

2.1.5 Acceptance of biometrics for identification and authentication

The success of using biometrics for identification or authentication depends not only on technical specifications such as performance, reliability and stability, but depends also on the acceptance by the (future) consumers. One aspect of acceptance by consumers is ease of use. In some circumstances, biometrical identification will be much more convenient for the users than current methods. Ease of use in relation to identification or authentication using biometrics is dependent on several factors. One of these factors is the way in which the human characteristic needs to be presented to the system. The presentation needs to be in a natural way, and should not scare consumers away. Next to that, there has to be only one way presenting the characteristic to prevent a false rejection. Another factor is the time needed for the identification or authentication process itself. The process time needs to be acceptable to avoid annoyance of consumers.

Another aspect of acceptance concerns the risks that consumers can experience as owners of human characteristics. These risks concern the mutilation of body parts, by malicious people, to gain access to these characteristics, and thereby gain access to objects, buildings, or computer systems. These risks can be avoided by letting the system execute some checks, e.g. check the body temperature, or check blood circulation. Another risk that can be experienced concerns the enforced presentation of a characteristic, by malicious people, in order to gain access to an object, building, or computer system.⁴ To avoid this risk, an alternative entry should be available, which will give the impression that access is granted, while in the meantime an alarm is sent to the security-officer. One could also imagine combining access control with the measurement of emotions exposed by the user. If threatened, the user will

probably be nervous, or show some other kind of emotion. A difficulty of this method is to recognise if specific emotions are indeed caused by enforcement. A false alarm, because a user was stressed when he or she tried to gain access will lead to unwanted situations, and therefore the user acceptance of the system will decrease. In the next paragraph, emotions exposed by human characteristics will be described in more detail.

2.2 Biometrics to expose emotions

This paragraph will describe how biometrical data can be used to expose emotions of human beings. Therefore, the 'state of mind' will be examined in relation with the ability to recognise several emotional characteristics of human beings. The following items will be addressed in this paragraph: the definition of 'state of mind', how emotions are expressed in the human voice and how emotional expressions can be identified by software.

Definition of 'state of mind'

For the better understanding of this paragraph the definition of the term 'state of mind' should be clarified. Literally 'state of mind' means the status of the mind which depends on the condition/ position of the person concerned. In addition to the term 'state of mind', mostly the terms 'emotion' and 'mood' are used. Although the meaning of these terms are not the same as the meaning of 'state of mind', the former are mostly used in the scientific literature. This is because emotion has a solid correlation with the techniques used for detection of deception, with e.g. a voice stress analyser.

According to Webster's ninth new collegiate dictionary the following definitions can be applied to the terms 'emotion' and 'mood'. "Emotion: A psychic and physical reaction (as anger or fear) subjectively experienced as strong feeling and physiologically involving changes that prepare the body for immediate vigorous action." "Mood: A conscious state of mind or predominant emotion", or "A receptive state of mind predisposing to action."

In *Toward the simulation of emotion in synthetic speech*⁵, the following distinction is made regarding to 'emotion' and 'mood': "Emotions arise suddenly in response to particular stimuli, and last for seconds or minutes, while moods are more vague in nature, lasting for hours or days. Although the onset of an emotion can usually be readily discerned from a preceding mood, it is impossible to define when an emotion becomes a mood; possibly for this reason, emotion is very often used as a general term incorporating the concept of mood also." Therefore, we will use the term 'emotion' for the purpose of state of mind in this report.

Emotions can be expressed in several ways, and with several human characteristics, or combinations of these characteristics. Human characteristics that have strong relations with emotions are e.g. the human face, the human skin, body scent, the placing of signatures, and the voice. It is possible to read from the look of someone's face in what emotional state that person is. It is also possible to recognise emotions when a person speaks. The human skin reacts on emotions by creating more sweat. This principle is used to create lie detectors. As stated earlier, the static and dynamic signature and the analysis of keystrokes are behavioural characteristics and are susceptible to the emotional state of a person.

Because voice recognition will be described in more detail to examine the privacy risk of biometrics, this study will focus on the determination of emotional expressions in the human voice.

⁵ Murray, I. and Arnott, J. (1993) *Toward the simulation of emotion in synthetic speech: A review of the literature on human vocal emotion*. Acoustical Society of America. (2) February 1993, p. 1097-1108.
⁶ Keifer R. (1966). *Polygraph versus voice stress*. September 11. www.polygraph.org.

How are emotions expressed in the human voice

Before the emotional expressions in the human voice can be described, clarity should exist on the various emotions and the way they originate. In Keifer, *Polygraph versus voice stress*,⁶ the following four basic emotions are addressed: happiness, sadness, anger and fear. All occurring emotions can be seen as a combination of one of these four basic emotions plus the information about what caused it, or to whom it is directed. Several scientists have come up with the following three-dimensional model:

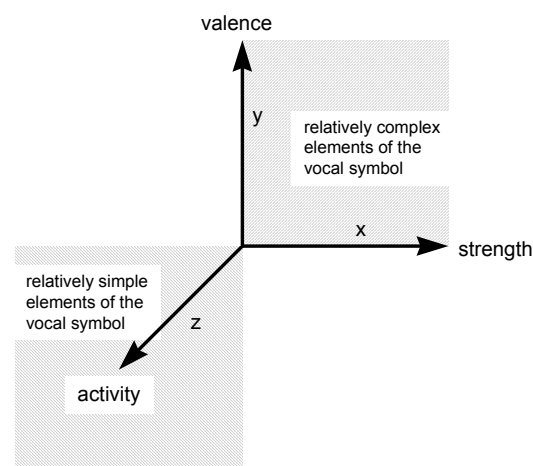


Figure 6: The three dimensions of emotion.

Figure 6 illustrates three axes that stand for the three most important properties of emotion, which are:

- 1 strength: corresponds to attention-rejection, distinguishing between emotions initiated by the subject and those arising from the environment (ranging from contempt to fear and surprise);
- 2 valence: corresponds to

positive-negative or pleasantness-unpleasantness (ranging from love and happiness to anger), and

3 activity: ranges from sleep to tension. The property 'activity' can be easily recognised. The other two properties are more difficult to detect, because these properties contain the real emotions.

Some scientists prefer other names for the axes, but generally figure 6 can be seen as a relative good basic assumption. Now it is possible to come to emotions such as: joy, tenderness, longing, coquetry, surprise, complaint, scorn and sarcasm. When the relation between these emotions and the human speech mechanism is examined, the expression of these emotions originates in the vocal cords. When a person speaks, the vocal cords vibrate in a specific frequency, called the speaker's main leading frequency. The pushed air from the lungs starts to vibrate in the same frequency and is flowing upward to the mouth and goes through the tongue, teeth and lips, thereby creating the speech flow⁷. When a person displays a specific emotion, the amount of blood in the vocal cords rises or drops depending on that emotion. This causes the vocal cords to produce a distorted sound wave. These distortions can then be analysed to determine the specific emotional state the person is in.

⁷ *Truster, your personal truth verifier*. User guide.

How can emotional expressions be identified by software?

The best known application for identifying emotions is the polygraph, also known as the 'lie detector', which is often used in the United States of America. The polygraph measures predictable changes in a person's body that are associated with the stress of deception. These changes include alterations in the heart rate, breathing, and electrodermal activity (emotional sweating). Other changes occur as well: the pupils get larger, digestion slows, the body's blood supply is redistributed away from the skin and gastrointestinal regions and toward the muscles, etc.⁸. These measurements are performed by several consecutive physical tests by connecting the subject to multiple sensors simultaneously⁹. The measures used by the polygraph were selected in the 1920s and 1930s because they were simple to record (as opposed to brain waves and gastrointestinal activity), they were sensitive, and they were accurate¹⁰.

⁸ *Truster, your personal truth verifier*. User guide.

⁹ Keifer, R. (1996) *Polygraph versus Voice Stress*. September 11, (www.polygraph.org.)

¹⁰ Murray, I. and Arnott, J. (1993) *Toward the simulation of emotion in synthetic speech: A review of the literature on human vocal emotion*.

Acoustical Society of America. (2) February 1993, p. 1097-1108.

About 25 years ago, serious efforts were made to analyse the human voice for the detection of deception. Meanwhile many devices are widely being marketed. Voice analysis offers many advantages over current polygraph methodology. Examinations can be conducted remotely, using a telephone, and shifted in time, using a tape recording. Voice samples can be recorded without discomfort to the subject, and can also be conducted surreptitiously and would be of great benefit in intelligence and counterintelligence investigations. But of course, the most important is the accuracy of such a device. To date the methods of voice analysis are not accurate enough to replace the existing polygraphs⁸.

Focused on the use of the human voice, Keifer⁹ describes a correlation between the so called primary emotions (anger, happiness, sadness, fear and disgust) and some vocal effects (speech rate, pitch average, pitch range, intensity, voice

quality, pitch changes, articulation). In the following figure these correlations are summarised.

	<i>Anger</i>	<i>Happiness</i>	<i>Sadness</i>	<i>Fear</i>	<i>Disgust</i>
<i>Speech rate</i>	slightly faster	faster or slower	slightly slower	much faster	very much slower
<i>Pitch average</i>	very much higher	much higher	slightly lower	very much higher	very much lower
<i>Pitch Range</i>	much wider	much wider	slightly narrower	much wider	slightly wider
<i>Intensity</i>	higher	higher	lower	normal	lower
<i>Voice quality</i>	Breathy, chest tone	breathy, blaring	Resonant	irregular voicing	grumbled, chest tone
<i>Pitch changes</i>	abrupt, on stressed syllables	smooth, upward inflections	downward inflections	normal	wide, downward terminal inflections
<i>Articulation</i>	tense	normal	slurring	precise	normal

Figure 7: “Summary of human vocal emotion effects. The effects described are those most commonly associated with the emotions indicated, and are relative to neutral speech”⁸

The described effects of the voice are examples of identifiable characteristics of the voice. It is very well possible that the voice has more useful characteristics. It is also possible that certain software products (like e.g. Truster) use different identifiable characteristics. Producers of these products often do not reveal which properties they use, so figure 7 has to be seen as a summary of possible properties.

2.3 Future developments

The number of applications that use biometrics will increase because of improved measurement methods and the continuous price reduction. Due to the improvement of the measurement methods, reliability rates will improve. Also the physical size of the sensors will decrease. Future applications using biometrics will be easily integrated with other (existing) systems/products. Examples of these developments are face recognition and iris scan (cameras on multimedia computers), as well as keystroke dynamics (no additional computer hardware needed). This also implies that these techniques can be used for the identification of persons, without the notice of persons that they are (being) identified, because the sensor used for this is not seen, or recognised as a sensor.

According to Patricia Oldcorn, of Software and Systems International (UK): ‘The latest versions of facial recognition software can be used in conjunction with closed circuit television surveillance systems to provide additional help in

the fight against crime. By comparing faces from scenes involving muggers, pickpockets, football hooligans with a database of known criminals, police forces can pinpoint likely suspects and take action when appropriate.¹¹

Because of the decreasing prices and the increasing number of products, the reliability rate will be a deciding factor when implementing high-security applications for military purposes and banking purposes, such as securing Automatic Teller Machines (ATMs).

Over the last decade the performance of identification or authentication systems using biometrics has increased enormously. Between 1987 and 1997 the verification processes have evolved from relative time consuming processes to processes with high performance results. This can be expressed by the size of the templates used for the digital representation of the human characteristics and the estimated time needed for the comparison of the digital representation with the template, used for authentication purposes. In 1987 the average template size was 2000 bytes, ranging from 18 bytes to 8000 bytes. The average time needed to compare digital representation and template was 8 seconds, ranging from 4.5 seconds to 10 seconds¹². In 1997 the average template size was reduced to 250 bytes, ranging from 9 bytes to 1000 bytes. The average time for comparison was reduced to 4 seconds, ranging from 3 seconds to 6 seconds.¹³ This change in performance can be explained by the increase in computer power, such as processor speed and access times for disk and memory and improved compression algorithms.

¹¹ Biometrics98, Exhibition and Conference flyer. (www.sibresearch.com/bio98)
¹² Maxwell, R. and Wright. L. (1987) *A performance test of personnel identity verifiers*. Sandia National Laboratories: Albuquerque.

If this trend persists, the following decade will result in an average estimated time for a template match of 2 seconds, and an average template size of approximately 30 bytes.

With respect to biometrics used for identification or authentication, it is expected that, especially for demanding applications, different human characteristics can be combined into multi-technique systems. It can be assumed that a person's fingerprint is independent from his/her eye pattern, so multi-technique systems can provide a better reliability. At this moment the Dutch Government studies the integration of the identification card with biometrics.¹⁴

With respect to biometrics used to expose emotions, it is expected that characteristics like voice, face and keystroke dynamics will have great influence, because these characteristics can be measured without the notice and consent of the persons involved. Especially, when working in multimedia spaces, where during a video-conferencing session all movements, can be seen by each of the participants, human characteristics including body language, can give more information than is intended.¹⁵ The measurement of exposed

emotions may be of value for electronic commerce, to influence the purchase pattern of customers. This will be stimulated by the earlier mentioned integration of biometrics with multi-media systems.

Legal aspects

3

3 Legal aspects

Identification or authentication using biometrics relies on information about individuals obtained with or without their knowledge. This chapter describes the relevant legal aspects concerning privacy. The European data protection Directive will be used as the basis for the discussion.¹ The definitions of the applied legal concepts are summarised in appendix B.

Eight questions will be addressed in relation to the Directive. Firstly, to what extent biometrical data is personal data. Secondly, when biometrical data can be seen as personal data and to what extent that biometrical data is processed. Thirdly, whether or not the way in which the biometrical data is processed comes within the scope of the Directive. Fourthly, what are the consequences if processing of biometrical data falls within the scope of the Directive. Fifthly, which information has to be provided to the person whose biometrical data are being processed. Sixthly whether or not this data belong to so called 'special categories of data' and, seventhly, what the consequences of this qualification are. The eighth issue concerns the security of processing.

3.1 Personal data or not

Article 2 (a) of the Directive:

'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

It appears that biometrical data can always be considered as 'information relating to a natural person' as it concerns data which provides, by its very nature, information about a given person.

In the context of biometrical identification it can also be argued that this person is generally identifiable, since the biometrical data is used for identification or authentication, at least in the sense that the person concerned is distinguished from any other person. In this approach, the identifiability of the person does not depend on the availability of other data which – jointly or separately – allow the person concerned to be identified. It should be noted also that the possibility of 'direct identification' by means of 'one or more factors specific to his physical identity' is expressly mentioned in the definition of the Directive.

In the previous chapter a description was given of the process of biometrical identification or authentication. Several stages in the processing of biometrical data were identified. The first stage is the capture or measurement of the

¹Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

templates. Subsequent steps involve the manipulation of these data, e.g. the measurements of certain features in a fingerprint and the storage of these in a table. A next stage could be the mathematical transformation of these data into a code.

There is no reason to think that what applies to the human characteristic itself, would not apply to the digital representation of that characteristic, the templates which are composed on the basis of these representations, and to any subsequent transformation. As the process continues, the amount of detail will change, but the unique link with the person concerned is kept. It is reasonable therefore to conclude that the data involved will remain personal data in most, if not all stages of their processing.

To determine whether or not the Directive is applicable, the question has to be answered when personal data is processed, and whether the way in which personal data is used falls within the scope of the Directive.

3.2 Processing personal data

The definition of the term 'processing' in article 2(b) the Directive is fairly broad:

Article 2 (b) of the Directive:

'Processing of personal data' ('processing') shall mean any operation or set operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

For example, identification using biometrics may involve the processing of personal data when an algorithmically processed biometrical data item (like e.g. a template) is stored or if information on a network is forwarded, as illustrated in figure 8 in chapter 4, of a 'hand geometry verification system that replaces the PIN code verification of a (credit) card banking system'.

3.3 Scope of the Directive

Article 3 (2) of the Directive:

This Directive shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

²The approach taken here, where it is considered if there is use of personal data as a personal activity would appear to us to be more effective than the approach used in the Dutch ITeR report '*Het lichaam als sleutel, juridische beschouwingen over biometrie*' (1997) which argues that there is no personal data in this context. (Kralingen, R. van , Prins, C. and Grijpink, J. (1997) *Het lichaam als sleutel*. ITeR, Vol. 8, Samson).

Thus, the Directive does not apply to purely personal activities, even when personal data is concerned. Arguably, some ways of authentication by means of biometrics can be considered as such.²

For example, there are now prototypes of extremely thin fingerprint readers embedded in chipcards. In this approach, the fingerprint is never communicated beyond the card, neither when the information is first recorded, nor when it is used. (See also section 5.1.1.) The card only gives a signal: the right person is holding the card, yes or no. This is comparable to entering a house with your own key. In this case it may be argued that the personal data remain in the personal domain.

3.4 Processing of biometrical data

The next question to be examined is what the legal consequences are if a human characteristic is a personal data item which falls under the Directive. In that case the conditions of the Directive will have to be complied with, for example the following general issues:

Article 6 of the Directive:

Member States shall provide that personal data must be:

- (a) Processed fairly and lawfully;
- (b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

and

Article 7 of the Directive:

Member States shall provide that personal data may be processed only if:

- (a) The data subject has unambiguously given his consent,
- or

- (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- or
- (c) Processing is necessary for compliance with a legal obligation to which the controller is subject
- or
- (d) Processing is necessary in order to protect the vital interests of the data subject,
- or
- (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed,
- or
- (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

Article 6 (a) for example means that the processing and collection of data must be done fairly. Hence, people have to be aware that identification by means of biometrics is used. Also article 10 is of importance in this respect, see section 3.5. Article 6 (b) means that when biometrical data for identification is processed with the aim of determining whether or not somebody is permitted to access a given system, the use of this data to determine the emotional state of the person concerned, or his or her race would in principle not be compatible with the purpose specified to the subject, i.e. biometrical identification. Furthermore, the objective of processing that personal data should be justified in accordance with article 7. The processing of the data is permitted if at least one of the conditions listed in article 7 is fulfilled.

3.5 Information to be given to the data subject

According to Article 10 of the Directive the controller has to provide the data subject from whom data relating to himself are collected, with at least the following information:

- 10(a) The identity of the controller and of his representative, if any;
- 10(b) The purposes of the processing for which the data are intended;

- 10(c) Any further information such as
- the recipients or categories of recipients of the data,
 - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
 - the existence of the right of access to and the right to rectify the data concerning him, insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

In the context of biometrical identification the consequence is that the technique may not be applied without the knowledge of the data subject, i.e. the person whose biometrical data are collected.

3.6 Special categories of data

Article 8 (1) of the Directive:

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.

In common practice special categories of data are referred to as 'sensitive data'. Can biometrical data now be considered sensitive data in the sense of the Directive and, more specifically, should they be considered as personal data concerning a person's race or state of health?³ Is the qualification as sensitive data dependent on the actual application of biometrics?

Several stages in the processing of biometrical data were identified. The first stage is the capture or measurement of the human characteristic and the creation of a template. In this stage the 'raw' or unprocessed template sometimes contains information which can directly be interpreted in terms of e.g. race or state of health. Examples are facial images showing skin colour or certain signs of illnesses. These initial templates can in those cases be classified as sensitive data.

Subsequent steps often follow in the processing, in which the original data are being manipulated. Whether these processed data still classify as sensitive data is questionable. In the first place, it is well possible that the specific characteristics that render the data special are not being used for the determination of the derived data. When a fingerprint pattern is determined, e.g. the skin colour might not be relevant in this manipulation. Secondly, it might not be possible to restore with reasonable means the template from these derived data. Also in this case a classification as sensitive data seems hard to justify.

³See: *Registratiekamer In beeld gebracht; privacyregels voor gebruik van videocamera's voor toezicht en beveiliging*, January 1997, p. 18: "In the context of video recordings it is significant that information about a person's race, sexuality or intimate behaviour or medical information is considered to be sensitive. A recorded image of a person always provides information about their race and will often also contain information of a medical nature. (R. de Korte, *In beeld gebracht, privacyregels voor gebruik van videocamera's voor toezicht en beveiliging*).

3.7 Consequences of the qualification as special personal data

For special categories of data, additional statutory requirements will have to be observed. The requirements with respect to the processing of sensitive data are stricter. The basic approach is article 8 (1) of the Directive, which *prohibits* the processing of such data. The Directive specifies in Articles 8(2) to 8(4) the specific cases in which this prohibition is lifted. The Member States have each implemented these exemptions in detail in their national legislation.

Exemptions may only be granted in clearly defined cases:

- 8(2)a The data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
- 8(2)b Processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- 8(2)c Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- 8(2)d Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or other non-profit-seeking body with a political, philosophical, religious, or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third without the consent of the data subject; or
- 8(2)e The processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise, or defence of legal claims;
- 8(3) Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
- 8(4) Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

The giving of 'consent' referred to in article 8(2)a should comply with the definition of the Directive (article 2h):

'the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'

Taken together, for systems using biometrical identification or authentication, the main boundary conditions are as follows. If raw or processed biometrical data is considered as sensitive data, in principle the processing is prohibited. In some cases the processing can still be justified if explicit consent is given. The analysis of the different stages of processing shows that often only the raw data can be classified as sensitive data. These data may generally not be stored. If these data are removed, however, it is hard to defend that the prohibition to further process the biometrical data will hold.

The special case should be noted when new applications emerge in which citizens are obliged to present their characteristics. If these biometrical data classify as sensitive and are subsequently stored in databases, the citizens' consent as defined above, 'a freely given specific and informed indication' does not apply. In that case additional legislation may be necessary.

3.8 Security of processing

The last issue discussed is relevant to personal data in general. Article 17 of the Directive concerns the security of processing:

17(1) Member States shall provide that the controller must implement technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The remainder of article 17 treats into some detail the responsibilities in case the processing is wholly or partly performed by another party than the controller himself.

Application of biometrics, like any processing of personal data, goes along with the obligation to take appropriate security measures. The technical solutions recommended in chapter 5 should be seen in the light of this obligation.

Biometrical identification and privacy-related issues

4

4 Biometrical identification and privacy-related issues

The previous chapter addressed the question whether biometrical data can be classified as personal data. It can be argued that, in the context of biometrical identification, this is generally the case, at least at some stage of the data processing, and hence the processing falls within the scope of the European data protection Directive. This has several implications for biometrical identification in practice.

In this chapter some privacy-related issues and concerns relevant to biometrics will be mentioned. Where appropriate the consequences of the legal framework are incorporated.

A general concern related to biometrics relates to the uniqueness of the measured human characteristics. Because of this, the biometrical data proper may become a key to databases that contain other personal data. The key to such databases is often a distinct, or unique, value of the person to whom the data refer. This value can simply be a person's name, or social security number, but also the (digital) representation of a specific human characteristic. If different sets of personal data are stored in several unprotected databases, the same specific human characteristic can be used as a key to combine the sets of personal data. The combination of these sets of personal data could reveal the identity of the person involved, because one or more sets contain the identity of the person involved, and now the identity is revealed to all sets; or the combination provides sufficient information to identify a specific person.

This issue of the linking of databases has been discussed in other contexts. It generally occurs when data related to the identity of a person, is stored and linked with other personal data within an information system. The issue is especially alarming when biometrics are involved, because of their unique character, as well as their expected application in common and frequently occurring transactions. A particularly important case is presented when a person does not have the option to refrain from using the system. Such dependencies frequently occur in the relationship between citizen and the local or central government.

According to the Directive (Art. 17) and corresponding (national) laws concerning the protection of personal data, biometrical data, as personal data in general, need to be protected against destruction, loss, alteration, unauthorised access and disclosure and against other forms of unlawful use. Chapter 5 will describe some of the technical and organisational measures to put this into effect.

However, with the use of biometrics for identification, authentication, or the exposure of emotions, explained in chapter 2, some other privacy issues are relevant. This chapter will address privacy issues related to the use of biometrics for identification, or authentication, and, to a lesser extent, for determining emotional states.

4.1 Biometrics for identification and authentication

In case of biometrics, the human characteristic measured is personal data that is uniquely related to the identity of a person. The linking of databases using the biometrical data as key, is a manifest risk as soon as a person uses a human characteristic to enrol to a system that uses biometrics for identification or authentication.

It should be noted that human characteristics can also be used in such a way that enrolment, identification or authentication take place without the persons involved being aware of it. Thus, the following cases should be distinguished: it is known that enrolment, identification or authentication takes place, or; it is not known that enrolment, identification or authentication takes place¹.

It is possible that persons are being identified or authenticated without being aware of it. There are several characteristics, like voice, keystroke, face, and body scent, that can be used in such a way that persons do not notice they are being identified or authenticated. This potentially leads to an undesirable type of secret surveillance.

As mentioned in the previous chapter, such collection without informing the persons involved is generally not allowed, because personal data must be processed fairly and lawfully (article 6a of the Directive). Moreover, article 10 of the Directive (see section 3.5) states that in case of such a collection of personal data the controller, the person or organisation applying the biometrical identification technique, has to reveal his identity.

4.1.1 Known identification or authentication

In this case, when enrolment, identification, or authentication processes use human characteristics, a person will recognise the moment that he is identified or authenticated, because he needs to present his characteristic in a specific way.

Imagine that the PIN-code used by banks for the authentication of their clients at ATMs is replaced by hand geometry verification. With the conventional (credit)card and PIN-code the clients could adopt, to some extent, pseudo-identities², by using different (credit)cards and PIN-codes. Because most

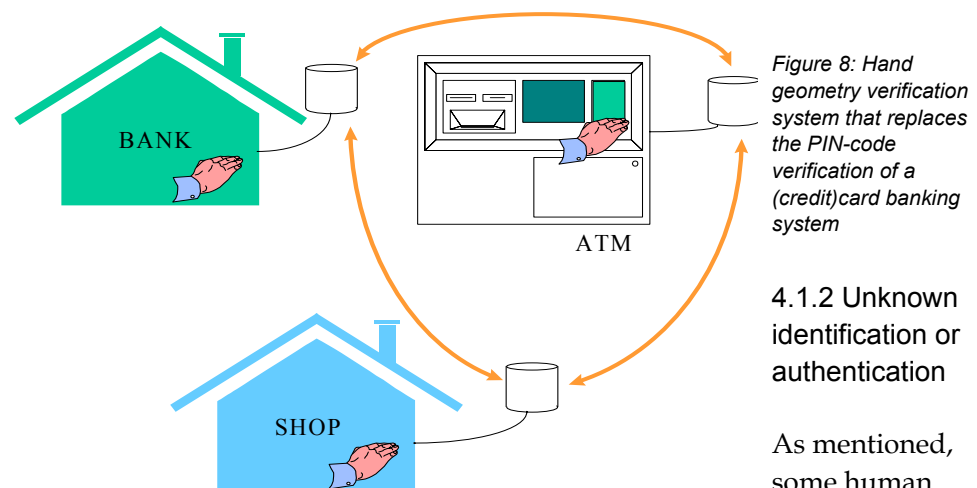
¹Borking, J. and Verhaar, P. *Biometrie und Datenschutz, Bedrohungen und privacy-enhancing technologies* in DUD (Datenschutz und Datensicherheit) no. 3/1999, p. 138-142.

²Hes, R. and Borking, J. (editor) a.o. (1998). *Privacy-enhancing technologies: the path to anonymity*. Revised edition. A&V-11, Den Haag: Registratiekamer.

products using hand geometry for identification or authentication are based on the right hand, changing pseudo-identities is not possible. Changing pseudo-identities is also pointless when using the same characteristic for identification or authentication to gain access to different locations or services. When using e.g. fingerprints for verification, it is generally not possible to change the fingerprint, because the present generation of fingerprint systems needs to be provided with the right index finger. Future systems could probably handle the fingerprints of more than one finger.

Each characteristic is unique and cannot be changed. Each pseudo-identity will be related to this unique characteristic, and therefore, the pseudo-identities are easily linked to each other. This is illustrated in figure 8. The customer of the bank needs to present his characteristic in order to handle his or her bank transactions, get money from the ATM, or obtain his or her goods from the store. In every case, the characteristic is recorded, transformed to a digital representation, and compared to the specific template. At every site (bank, ATM, and shop) details of all transactions are recorded, and stored in databases, including the digital representation.

In theory, the transformation of the characteristic will give the same digital representation each time the characteristic is recorded. This means that with the digital representation, information from the three databases can be related to one and the same person. To protect the privacy of the customers, it is desirable to limit the ability to link the different databases. This will be treated in chapter 5.



characteristics like the voice, keystroke dynamics, body scent, the face and the iris can be used to identify or authenticate a person without the person noticing this. This is most relevant for voice recognition.

Telephone companies, e.g., are looking for ways to identify or authenticate customers that want to use electronic commerce services offered by the phone-company, by means of their voice. In telecommunications there is a growing need for strong identification and authentication mechanisms³ in particular because of the geographical separation of parties connected by the telecommunications network. Also there is the need to fight the annually increasing levels of fraud. Phenomena like the cloning of mobile telephones (stealing the ID of a handset and copying it into another), enrolling for services under an alias without paying, and theft of subscriber lines from telephone exchanges can be mentioned. Voice or speaker recognition is a method that can be used for identification and authentication, and can be used to control access to the network and equipment, and access to the services delivered over the network.

At this moment, without the use of biometrics, a person who makes a telephone call using his own static telephone connection, or mobile phone, will automatically identify himself because of the subscriber-number. If the subscriber allows another person to use his telephone connection this other person will be identified as the subscriber. Authentication can take place by using PIN-codes, passwords, or pass-phrases, but these can be exchanged, or filched, so there is no real assurance. A person can make anonymous calls by using a pay-phone (public-phone).

³As for services delivered by means of the telecommunication networks, identification of customers is increasingly seen as an important element of sales and marketing. Having been identified unambiguously, personal data on an individual can be retrieved from databases and used for making on-line decisions on the way a person is treated. Also, a person's mental or emotional state derived from his or her voice can be used for sales and marketing purposes. Real-time analysis can potentially be used in a commercial context to influence behaviour of a client, e.g. in telephone sales. Whether this will become significant from a business perspective is difficult to judge; it has to be noticed that it can create a situation of asymmetry in which the client is not asked for consent.

When voice recognition will be introduced, it will be helpful against misuse of telecommunication services, but it will also limit the possibility for individuals to remain anonymous. Again, the human characteristic used is unique, and therefore, the telephone company could make a profile of each customer. It is also possible to use a system to identify customers instead of only verifying their identities. When the voice is used to identify customers, it will be more complicated to make anonymous calls at a later stage (see figure 9).

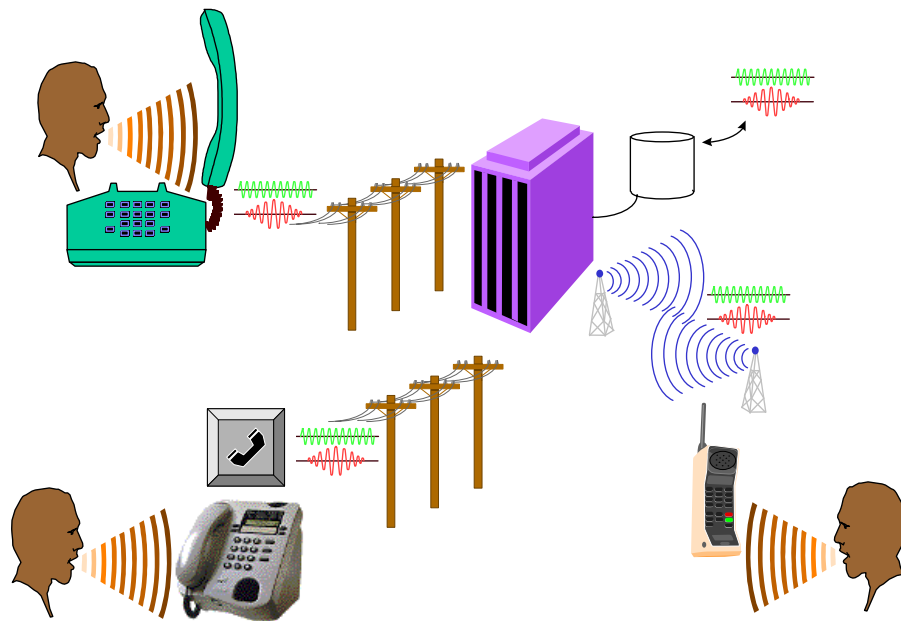


Figure 9: Using voice recognition to identify or authenticate people by means of telephone connections.

4.2 Biometrics and emotions

The extraction of emotions through the use of biometrics is a quite controversial issue. Such measurements would give an indication of a person's emotions at a specific moment in time. Because biometrics is used, the emotions are being registered in connection with a specific human characteristic, and therefore, a profile of the person involved could be generated and updated. It could also be possible to identify or authenticate this person due to the uniqueness of the human characteristic used for storage. In case the person involved is also identified, a more detailed impression/profile of the person's emotions can be obtained.

In that case, emotions and other personal data could be combined and processed, which leads to uses incompatible with the purpose for which the data were collected. See section 3.4 on article 6b of the Directive, where incompatible use is described in more detail. Note that extraction of emotions can, similar to identification or authentication, take place without the involved person being aware of it.

4.3 Biometrics and technical restrictions of systems

Even though some human characteristics might be unique, the techniques for measuring them have a built-in tolerance. This tolerance is due to the inaccuracy of the applied techniques and the different circumstances under which characteristics are presented for identification or authentication. This

tolerance results in the 'false rejection' of authorised persons, and in the 'false acceptance' of unauthorised persons. The technical specification of this tolerance is given with the 'False Acceptance Rate' (FAR) and 'False Rejection Rate' (FRR).

These two rates are related, see figure 4. If the FRR is low - few persons will be falsely rejected -, the FAR will be high - some unauthorised persons will be falsely accepted -, which means that the accuracy of the measurement will be low. However the user acceptance will be high. If the FAR is low - few unauthorised persons will be falsely accepted -, the FRR will be high - some persons will be falsely rejected -, which means that the user acceptance will decrease. In this case, the measurements will be accurate. Both false rejection and false acceptance can lead to privacy-related problems.

False rejection and social acceptance

It is known that certain groups of persons have human characteristics that are less pronounced than average or different in such a way that automated biometrical identification is not working properly with the current products. Such groups have an overall higher risk of false rejections. Potentially this can have a discriminatory effect if e.g. denial of service happens more often to members of such a group. The false rejection of someone, e.g. an employee in front of his or her colleagues, can also lead to unwanted reactions. These social aspects are of vital importance when introducing a new technology.

False acceptance and the quality of personal data

The false acceptance of an unauthorised person means that this person is granted access to a building, object, or information system on account of an authorised person. The personal data that will be collected will be assigned to the authorised person, and therefore, the quality of this person's personal data is affected. Maintaining the quality of personal data in an element of data protection and therefore, also from a legal perspective, relevant to the privacy discussion. See article 6(1)d of the Directive concerning the quality of personal data, and article 17 of the Directive concerning the required security measures to protect the quality of the data.

It is important to stress that, when biometrical systems are used, there is always a fraction of false acceptances. Corruption of personal data due to false acceptances will occur. The use of biometrics however might create the illusion that the personalization is always correct.

Biometrics and privacy-enhancing technologies

5

5 Biometrics and Privacy-Enhancing Technologies

The use of legal measures is one aspect of data protection. Legislation will be more effective if it is supported by technical measures. Different technological elements that help to improve privacy-compliance of systems can be grouped under the concept of Privacy-Enhancing Technologies (PET). These measures are an important element in minimising the risk of privacy violations, such as mentioned in the previous chapter.

From a privacy perspective, one end of the range of possible technical solutions, is to design facilities in such a way that a person can remain anonymous while using any services. When and how directly identifying data can be avoided within an information system, while still providing the desired services, is described in appendix A. In practice it is not always possible to stay anonymous. In some cases, identifying data has to be collected to provide the desired service. Generally, the personal data processed needs to be handled and protected according to the Directive. Following article 17 of the Directive, technical measures should be taken to protect personal data. In this chapter some of these will be described in more detail. The implementation of Privacy-Enhancing Technologies is a recommended approach.

Privacy-Enhancing Technologies can be utilised in systems for biometrical identification and authentication in the following ways:

- 1 The PET is integrated into the design of an information system, where the developer or owner of the system takes care of its proper implementation and functioning;
- 2 The PET is in possession of the person who wants to protect his or her own privacy. The person can in some cases take such measures himself.

This subdivision will be used to describe the measures that can be taken, and will be related to the issues that were mentioned in the previous chapters. Given the variation in properties of different human characteristics, some of the PET recommended in this chapter can not be applied to all biometrics systems. The description of the measures will state for which systems these measures can be applied, and which human characteristics they concern.

5.1 Privacy-compliant design of biometrical systems

When an individual knows that his or her human characteristic is needed for identification or authentication, this person has two choices: to present the characteristic or to refuse this. If there is no alternative way to obtain the services offered, the only choice the person has is to present the human characteristic.

In such cases where no alternative is present, the system should be equipped with some form of PET in order to guarantee the individual a certain level of protection of his personal data. The system owner is responsible for the integrated PET. In this case the measures could be:

- 1 decentralising of the template storage, and verification;
- 2 encryption of template-databases (in case of template storage in central databases).

5.1.1 Decentralising template storage and verification

By decentralising both the template storage and verification process, the biometrical data will be processed in an environment controlled by the individual or an environment from which no connection to a central database can be made.

Decentralised storage and decentralised verification on a token

When decentralising the template storage and verification of the presented human characteristic, it is necessary that the template and the verification process can be adequately isolated from the rest of the access control system. Using a chipcard, the template can be stored on the card and the comparison of the template and the card can handle the digital representation. The sensor also (and the rest of the biometrics product) needs to be tamperproof, so malicious bank employees, or shop employees can not retrieve the digital representation, or the template. The customer is anonymous and none of the generated data can be linked to other data concerning his or her identity. Therefore, it would be ideal if the sensor and chipcard could be integrated. Recent developments demonstrate that it is possible to integrate the sensor with the chipcard¹. Figure 10.a illustrates a possible implementation of such a product, while figure 10.b illustrates a product with a sensor that is integrated with the service.

Figure 10 describes the process of the identification or authentication to gain access to a certain desired service. In figure 10.a the human characteristic is recorded by the chipcard. The chipcard compares the obtained digital representation with the template, which is already stored on the chipcard. In this way all biometrical data (both the digital representation and the template) stay on the chipcard. The only information exchanged between the chipcard and the service is a positive or negative result of the identification or authentication process executed by the chipcard. This is illustrated by the authorisation code.

¹HSB cards and Cards Systems, Woerden, The Netherlands, private communication.

This case can legally be interpreted as a case of personal use, see paragraph 3.3 of chapter 3, following article 3(2) of the Directive. If this situation can be

created, the person can stay anonymous to the system, and the processing of these data is outside the scope of the Directive.

Decentralised storage and verification

Figure 10.b shows a situation where the sensor is not integrated with the chipcard, but is placed within the environment of the service. After the human characteristic has been recorded, the digital representation will be sent to the chipcard. To protect the digital representation, the product, or parts of it, used to provide the service need to be tamperproof. In this specific case both the sensor, the Card Acceptance Device (CAD), and the connection between them need to be tamperproof. Like in figure 10.a, the chipcard performs the identification or authentication process, and only gives a positive or negative result.

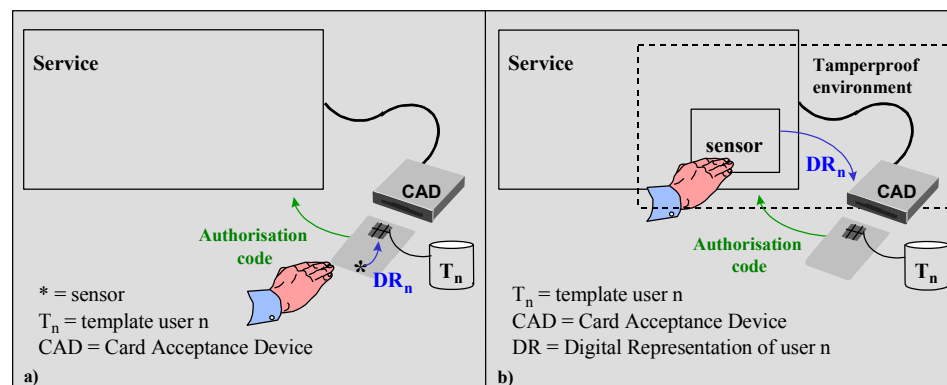


Figure 10: Illustration of measures to create a controlled environment for the processing of personal data.

a) illustrates the most desirable situation, where biometrical data remains on the chipcard. The only information exchanged between the chipcard and the service is a positive or negative result of the identification or authentication process executed by the chipcard;

b) illustrates a situation, where the sensor is integrated with the service. After the human characteristic has been recorded, the digital representation will be sent to the chipcard. The chipcard performs the identification or authentication process, and only gives a positive or negative result. In this second situation the product should be tamperproof, to prevent personal data from leaking.

This measure can be applied to all systems using all sorts of human characteristics, only if identification or authentication is obvious to the persons involved.

5.1.2 Encryption of databases (if templates storage is centralised)

In this case, template storage and verification of the template will still be centralised. It is desirable that all templates, and digital representations are being processed with mathematical manipulations, using different parameters for every biometrics product in use, to avoid the combination of personal data from several databases through the comparison of templates or digital representations. These mathematical manipulations could be encryption algorithms or hash-functions. Figure 11 illustrates that, when such

mathematical manipulations are applied, it is no longer possible to relate the personal data stored in different databases, at different locations.

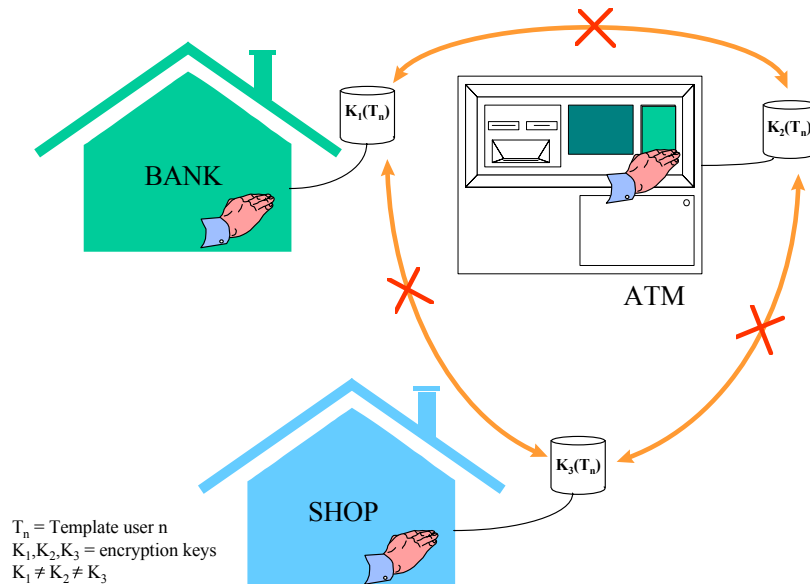


Figure 11: The use of mathematical manipulations such as hash-functions or encryption algorithms can prevent incompatible use of biometrical data. This method will protect the privacy of customers by protecting the recorded personal data against incompatible use.

² A hash function is a mechanism for mapping messages of arbitrary length to messages of small fixed length. These so-called hash-values of the message are intended to serve as compact representation images of the messages themselves. A basic requirement on hash functions is that they must be difficult to forge, i.e., knowledge of a hash-value alone should not allow the effective computation of a pre-image, i.e., a message that maps to this hash-value. One distinguishes between keyed hash functions (the so-called Message Authentication Codes (MACs)), i.e., hash functions that can be reconstructed once a secret value is known, and unkeyed hash functions (the so-called Modification Detection Codes (MDCs)), i.e., publicly known hash functions. Hash functions are usually denoted by the symbol h (or h_k , if it is a keyed hash function). If one uses this algorithm, the hash value provided over a message m is denoted by $h(m)$ (resp. $h_k(m)$).

Theoretically, the best way to do so is the use of one-way-hash-functions.² Before the template is stored in the template-database, the template is processed with this hash-function, generating a hash-value of the template. This hash-value will be stored in the template database. When verification of a human characteristic is needed, the digital representation of the characteristic will be hashed, resulting in a hash-value of the characteristic. If the hash-value of the template matches the hash-value of the characteristic the person involved is identified or authenticated. This method, unfortunately, will not work properly in practice, because of the difference that might occur between the digital representation of the human characteristic and the stored template, see also chapter 2.

Encryption is also an important instrument for protection of data. Every product needs to use different encryption and decryption keys to prevent the combination of personal data from different (template-)databases, see figure 11. A problem arises when encrypted templates are compared to encrypted representations, because of the possible differences between templates and representations. Therefore, the encrypted templates stored in the template-database need to be decrypted before they will be compared to the plain digital

representation of the human characteristic. To prevent others from taping the digital representation, or the plain template, and replaying these, the products need to be tamperproof.

These measures can be used for each biometrics system using any human characteristic.

5.1.3 Use of different human characteristics

As mentioned earlier, a person can use different pseudo-identities combined with different characteristics when gaining access for different systems. With pseudo-identity 1 the person can use the right eye, and with pseudo-identity 2 the person can use the index finger of the right hand, while for pseudo-identity N the ring finger of the left hand could be used. This method can only be used if products use a type of human characteristic of which people have more than one, like eyes, or fingerprints, an example of this method is given in figure 12.

The person can also choose to use pseudo-identities. It is necessary that more than one characteristic is needed, and can be recorded by the system. Think of the ten fingers (ten different fingerprints), and two eyes. In this case, the individual has some control on the release of his or her identity.

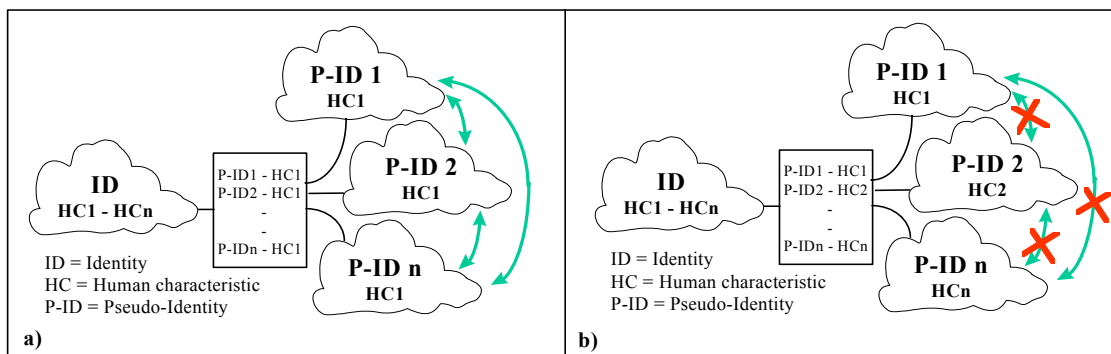


Figure 12: The use of different human characteristics can prevent incompatible use of personal data, because the key to the various recordings can differ: a) describes the fact that use of the same characteristic for different services will easily lead to the combination of various recordings, because the unique characteristic can be used as a key; b) on the other hand, shows that the use of different characteristics, and thus different keys, will leave no relation between various recordings of personal data.

5.1.4 Certification of products that contain PET

The integration of PET in products that use biometrics for identification, authentication, or exposure of emotions to guarantee adequate handling of personal data is not enough. Future users need not only be aware of the

presence of PET, but they also need to trust these products. An increase of trust can be reached if these products are being evaluated by an independent institution. These evaluations will lead to the certification of products with an indication of the guaranteed level of trust.

The evaluation and certification of these products also needs to be executed in conformity with an internationally agreed evaluation and certification scheme to receive an internationally accepted certification. Crossborder acceptance of biometrical product will be improved as well.

5.2 Unknown identification or authentication

We noticed in chapter 3 that the Directive obliges organisations to announce whether personal data, including biometrics, are collected when a person uses a certain system; e.g. when making a telephone connection to a service using voice recognition, an announcement should be made, before the actual identification or authentication takes place.

When it is not known to a person whether he is being identified or authenticated, he can take preventative measures himself. A possibility is the use of scramblers that modify the human characteristic in such a way, that he cannot be identified or authenticated. A person can use voice scramblers, in a preventative way, when he is not sure about whether or not the system will execute an identification or authentication. This 'digital handkerchief' should scramble the voice of the person in such a way that each time the scrambler is used a different voice is heard. This method can only be applied to products that use the human voice for identification or authentication. There are no practically feasible measures to protect individuals from identification or authentication by products using other human characteristics.

Resuming, the instruments an individual has to influence whether his characteristics are collected are quite inadequate. The responsibility of designers of biometrical systems, and of the organisations wishing to apply these, should therefore be stressed.

6

Conclusions and practical directions

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;

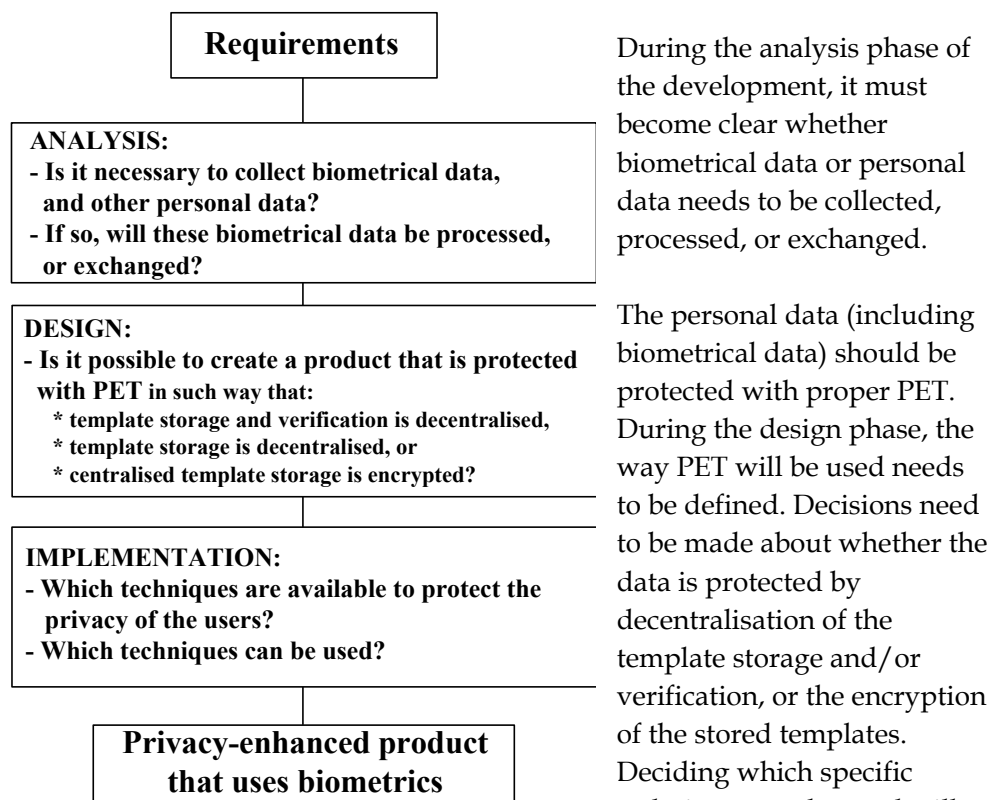
The individual whose human characteristics are measured may consider the following:

- 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.

Appendix A Privacy-Enhancing Technologies

Conventional information systems generally record a large amount of information. This information is often easily linked to an individual. Sometimes these information systems contain information that is privacy-sensitive to some individuals. To prevent information systems from recording too much information the information systems need to be adjusted.

There are a number of options to prevent the recording of data that can be easily linked to individuals. The first is not to generate or record data at all. The second option is not to record data that is unique to an individual (identifying data). The absence of such data makes it almost impossible to link existing data to a private individual. These two options can be combined into a third one. With this third option, only strictly necessary identifying data will be recorded, together with the non-identifying data.

The conventional information system contains the following processes: authorisation, identification and authentication, access control, auditing and accounting. In the conventional information system, the user's identity is often needed to perform these processes. The identity is used within the authorisation process, for instance, to identify and record the user's privileges and duties. The user's identity is thus introduced into the information system. Because in a conventional information system all processes are related, the identity travels through the information system.

The main question is: is identity necessary for each of the processes of the conventional information system? For authentication, in most cases, it is not necessary to know the user's identity in order to grant privileges. However, there are some situations in which the user must reveal his identity to allow verification of certain required characteristics.

For identification and authentication, access control and auditing the identity is not necessary. For accounting, the identity could be needed in some cases. It is possible that a user needs to be called to account for the use of certain services, e.g. when the user misuses or improperly uses the information system.

The introduction of an Identity Protector (IP), as a part of the conventional information system, will structure the information system in order to protect the privacy of the user¹. The IP can be seen as a part of the system that controls the exchange of the user's identity within the information system. The IP offers the following functions:

- 1 Reports and controls instances when identity is revealed;
- 2 Generates pseudo-identities;

¹See also Common Criteria for Information Technology Security Evaluation. Version 2.0. Part 2, chapter 9, Class FPR: Privacy. ISO IS 15408 (8 June 1999).

- 3 Translates pseudo-identities into identities and vice versa;
- 4 Converts pseudo-identities into other pseudo-identities; combats misuse.

An important functionality of the IP is conversion of a user's identity into a pseudo-identity. The pseudo-identity is an alternate (digital) identity that the user may adopt when consulting an information system (see figure 14).

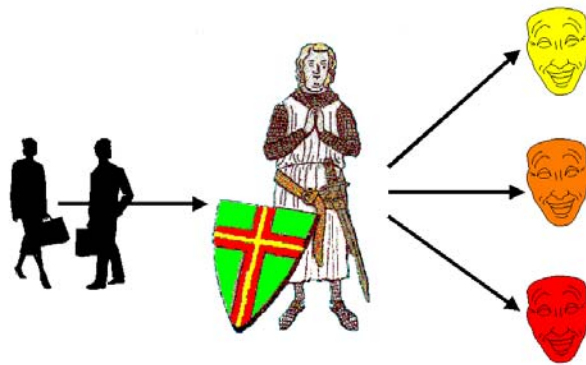


Figure 14: The identity protector separates the identity and pseudo domains.

The user must be able to trust the way his personal data is handled in the domain where his identity is known. The IP can be placed anywhere in the system where personal data is exchanged. This offers some solutions for privacy-compliant information systems.

Techniques that can be used to implement an IP are: digital signatures, blind digital signatures, digital pseudonyms, and trusted third parties.

To design an information system that protects the privacy of the user, the design criteria shown in figure 15 need to be considered (see next page).

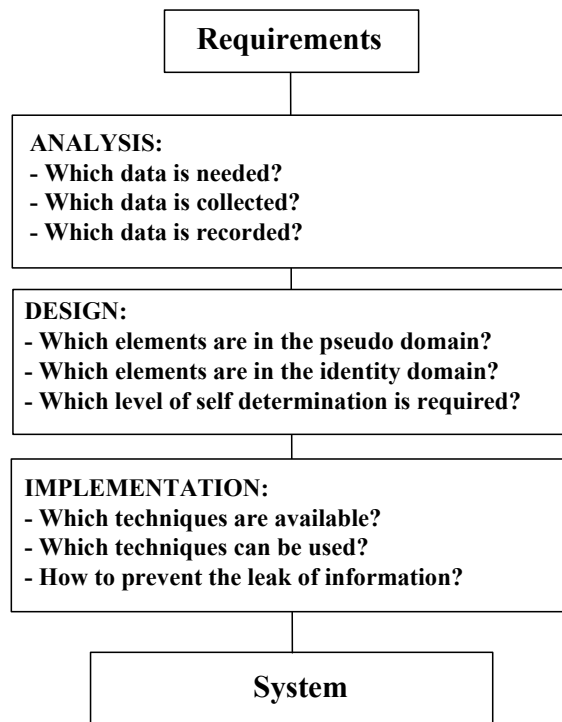


Figure 15: Aspects to take into account during the different phases of the design process of a privacy information system

Appendix B Terminology used in Directive 95/46/EC

In chapter 3 a short overview is given of the relevant legal framework. To facilitate the interpretation of the articles from Directive 95/46/EC the definition of the legal terminology, insofar as quoted in the current report, is listed here.

Article 2 Definitions

For the purposes of this Directive:

- (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
- (c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
- (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
- (f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
- (g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
- (h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Human characteristics, such as fingerprints and eyes, are increasingly being used for identification and authentication of persons. Such techniques for identification and authentication techniques are now being introduced for common purposes, like access control to buildings, personal computers, or commercial services.

The uniqueness of each human characteristic will help to ease many problems inherent in traditional methods of identification and authentication. This is especially relevant because, nowadays, more and more transactions are being performed without direct contact between the parties involved, making use of computers and computer networks. Increased security of transactions, ease of use and a better control of fraud are strong arguments to use human characteristics for identification. This form of identification or authentication is also known as biometry, or biometrics.

The widespread use of biometrics is, however, accompanied with a major concern for the privacy of the individuals involved. This report presents the results of study on biometrics and privacy, performed jointly by the Data Protection Authority of the Netherlands ('Registratiekamer') and the Netherlands Organisation for Applied Scientific Research - Physics and Electronics Laboratory (TNO-FEL).

This report starts with a description how biometrics can be used for the purpose of identification and authentication. An overview of the currently available technologies is given. Next the report addresses the legal framework for the processing of personal data, as given by the European Directive 95/46/EC. From this Directive it follows that, in the context of biometrical identification, the recordings of human characteristics generally classify as personal data.

In some special cases these personal data can be classified as processed in a purely personal activity, which implies that the Directive is not further applicable. In most cases the processing is within the scope of the Directive. Some of the main consequences for biometrics are: (a) persons should know that the collection of personal data takes place (b) the data collected for a certain purpose, e.g. identification, may not be used for incompatible purposes, such as determination of health condition, emotional state or race.

Some personal data are classified as sensitive in the sense of the Directive. In the report it is argued that some human characteristics can be classified as such sensitive data. These data should adhere to a stricter regime, which is 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 to protect the privacy of the persons concerned.

Besides privacy risks that apply to personal data in general, additional privacy issues are associated with the use of biometrics for identification or authentication:

- 1 Each human characteristic is unique, and therefore, its digital representation can be used as a key to search databases that contain personal data.
- 2 Certain human characteristics can be used for identification, and for other purposes such as the exposure of emotions, without the persons involved knowing this.
- 3 The quality of personal data can be at risk, because of the technical restrictions of the technology for biometrical identification.

Privacy-Enhancing Technologies (PET) can be applied to minimise or eliminate privacy risks associated with biometrics. The following measures could be taken:

- 1 Decentralisation of the template storage and verification process. In some cases the processing of personal data can be confined to a closed environment and the processing can legally be seen as a purely personal activity.
- 2 Encryption of databases: the protection of personal data, in case of central storage can be enforced by using different encryption keys and algorithms to encrypt the personal data (including biometrical data) in different databases.
- 3 Use of different characteristics: both previous measures should be integrated into the system. If a system does not contain these measures, individuals can use different pseudo identities and different human characteristics to identify and/or authenticate themselves.
- 4 Individuals could use countermeasures, such as scramblers to randomly distort the results of the recording of the characteristic. Such countermeasures have limited value and can only be used for certain characteristics, like the voice.
- 5 Certification of the privacy-compliance of biometrical identification products will guarantee an adequate handling of the personal data of the future users.

The report concludes with a set of design-criteria for a privacy-compliant design of identification or authentication systems that use biometrics.

Samenvatting

Binnen de informatiebeveiliging is de exclusiviteit van gegevens een belangrijk kwaliteitsaspect. De belangen van een bedrijf of van een persoon kunnen ernstig geschaad worden als onbevoegden toegang kunnen krijgen tot informatie. Het controleren van de toegang tot informatie is dan ook cruciaal. Hiervoor is het nodig om te weten wie toegang probeert te krijgen: wat is de identiteit van de persoon (identificatie) en kan deze identiteit bevestigd worden door vergelijking met een ander betrouwbaar gegeven (authenticatie).

Handelingen waarbij vroeger de betrokken personen fysiek aanwezig waren, worden tegenwoordig via computers en netwerken verricht. Dit is vaak een economische en efficiënte manier van zaken doen, maar het nadeel is dat je er moeilijk zeker van kunt zijn met wie men eigenlijk zaken doet. De huidige vormen van identificatie en authenticatie zijn immers fraudegevoelig. Vaak wordt gebruik gemaakt van authenticatie door middel van een voorwerp, bijvoorbeeld een pasje, of iets wat alleen de juiste persoon behoort te weten, bijvoorbeeld een wachtwoord. Geen van deze methoden is volledig persoonsgebonden. Een pasje of code kan immers worden overgedragen of in handen van onbevoegden komen. Hierbij valt te denken aan het aannemen van valse identiteiten of het gebruik van andermans PIN-code. Het gebruik van biometrie kan de kwaliteit van de identificatie en authenticatie verhogen, omdat lichaamskenmerken immers nagenoeg uniek zijn en niet overdraagbaar aan derden.

Vormen van biometrische identificatie

Biometrie is een verzameling van technieken gebaseerd op het meten van kenmerken die uniek kunnen worden toegeschreven aan de drager daarvan. Het unieke van deze kenmerken maakt deze geschikt voor identificatie, het vaststellen van iemands identiteit, en authenticatie, het vaststellen dat iemand is wie hij of zij claimt te zijn.

Op het moment zijn de meest geavanceerde toepassingen het gebruik van vingerafdruk, netvlies en iris, gezichtsvorm, hand- en vingergeometrie. Uit andere kenmerken, zoals lichaamsgeur of het DNA-profiel kan eveneens de identiteit van een persoon worden bepaald. De inzet van deze middelen voor toegangscontrole is echter vooralsnog niet aan de orde. Wel worden bepaalde gedragskenmerken voor identificatie gebruikt. Voorbeelden hiervan zijn de herkenning van de stem, de manier waarop iemand een handtekening zet, of de specifieke aanslag van het toetsenbord.

Het proces van biometrische identificatie en authenticatie kent een aantal stappen. Er moet altijd sprake zijn van een eerste vastlegging. In principe is dit een eenmalige gebeurtenis, waarbij het biometrische gegeven gemeten wordt

en toegeschreven aan de juiste persoon. Dit oorspronkelijke gegeven wordt nu vastgelegd in een template, bijvoorbeeld in een database of op een chipcard. Overigens zal dit template doorgaans geen 'afbeelding' van het lichaamskenmerk zijn, maar bestaan uit een aantal specifieke meetpunten.

In de gebruiksfase presenteert iemand zijn lichaamskenmerk aan een sensor. Het lichaamskenmerk wordt gemeten en vergeleken met het template. De meting zal altijd een zekere onnauwkeurigheid hebben en daarom afwijken van het template. Wanneer de overeenkomst tussen de meting en template groter is dan een van tevoren gespecificeerde drempel, zal de persoon worden geauthenticeerd.

Biometrische identificatie en privacy

Bij alle voordelen als beveiligingsmiddel kent biometrie voor identificatie ook een keerzijde. Juist de belangrijke eigenschap van lichaamskenmerken, namelijk dat ze uniek verwijzen naar een persoon, zorgen ervoor dat de privacy van die persoon in het geding komt. Wanneer immers verschillende gegevens over die persoon op verschillende plekken zijn opgeslagen kan aan de hand van het biometrische kenmerk worden achterhaald dat die gegevens allemaal bij die persoon horen. Door samenvoeging van de bestanden kan een gedetailleerder beeld ontstaan, zonder dat de betrokkene dat weet of daarvoor toestemming heeft gegeven. Wanneer dezelfde biometrische gegevens worden gebruikt voor allerlei verschillende handelingen, wordt het mogelijk om iemands leven voor een groot deel te traceren. Zeker bij toepassingen in de relatie overheid-burger is dit een punt van zorg omdat meestal de burger geen alternatief heeft. Bijvoorbeeld bij het plan om het paspoort uit te rusten met een biometrische kenmerk zal hier terdege rekening mee moeten worden gehouden.

Een ander punt van aandacht is dat biometrische gegevens vaak meer informatie bevatten dan direct voor identificatie of authenticatie nodig. Zo is het soms mogelijk om uit de lichaamskenmerken ook iets af te leiden over de gezondheidstoestand, of over het ras. Ook kan, bijvoorbeeld uit de stem of bij gezichtsherkenning, informatie worden afgeleid over de emotionele toestand. Dit laatste, het principe van de aloude leugendetector, zou gebruikt kunnen worden als hulpmiddel bij verkoop of afstand, waarbij de emoties geanalyseerd worden om het verkoopproces te stimuleren. In dergelijke gevallen kan meer informatie worden afgeleid dan waar iemand toestemming voor heeft gegeven.

Wettelijk kader voor de inzet van biometrische identificatie

Er is in Nederland (nog) geen speciale wetgeving over biometrische identificatie. Er is echter wel algemene wet- en regelgeving die bepaalt aan

welke voorwaarden biometrische identificatiesystemen moeten voldoen. Hierna wordt heel beknopt ingegaan op drie aspecten van deze regelgeving.

persoonsgegevens

Ten eerste zijn biometrische gegevens *persoonsgegevens*, primair omdat ze bedoeld zijn om mensen van elkaar te onderscheiden, en vallen derhalve onder de daarvoor relevante wetgeving. Op het moment geldt de Wet persoonsregistraties (Wpr) waarin de omgang met persoonsgegevens geregeld wordt. Er is een nieuwe wet in behandeling, de Wet Bescherming Persoonsgegevens (WBP). Gelet op de parlementaire behandeling is de verwachting dat deze rond de jaarwisseling in werking zal treden. De nieuwe wet is in grote lijnen gelijk aan de Europese richtlijn van 24 oktober 1995. Op hoofdlijnen kan uit de richtlijn daarom bepaald worden aan welke eisen biometrische identificatie in ieder geval moet voldoen. Bijvoorbeeld geldt het volgende algemene beginsel:

Artikel 6 van de richtlijn:

De Lid-Staten bepalen dat de persoonsgegevens:

- (a) eerlijk en rechtmatig moeten worden verwerkt;
- (b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

Artikel 6(a) betekent bijvoorbeeld dat het verwerken en verzamelen van gegevens op een eerlijke manier dient te gebeuren. Mensen moeten dus weten dat er biometrische identificatie plaatsvindt. Artikel 6 (b) betekent bijvoorbeeld dat wanneer biometrische gegevens worden ingewonnen om vast te stellen of iemand bevoegd is tot toegang tot een systeem, het onverenigbaar met dat doel zou zijn als deze gegevens gebruikt worden om de emotionele toestand of het ras van de betrokkene te bepalen.

Overigens zijn er bepaalde gevallen denkbaar waarbij de richtlijn niet van toepassing is. Artikel 3 (2) van de richtlijn luidt: De bepalingen zijn niet van toepassing op de verwerking van persoonsgegevens die door een natuurlijke persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden worden verricht.

Als het dus een puur persoonlijke activiteit betreft, dan is de richtlijn niet verder van toepassing, ook al gaat het om een persoonsgegeven. In dit verband kan de authenticatiemethode van belang zijn. Zo zijn er prototypen van een flinterdunne vingerafdruklezer, ingebed in een chipkaart. Bij deze opzet komt de vingerafdruk dus noch tijdens de eerste vastlegging van de gegevens, noch tijdens de gebruiksfase buiten de kaart. De kaart geeft alleen een signaal af: de juiste persoon houdt de kaart vast, ja of nee. Het is te vergelijken met het openen van een huis met de goede sleutel. In dat geval kan gesteld worden dat

de persoonsgegevens in het persoonlijke domein blijven en de richtlijn niet verder van toepassing is.

bijzondere gegevens

Het tweede belangrijke aspect in de regelgeving is die van de *bijzondere gegevens*. Bijzondere gegevens zijn bijvoorbeeld gegevens over iemands ras of gezondheid. De basisregel is dat de verwerking van bijzondere gegevens verboden is. Er moet dus ook nagegaan worden of de specifieke toepassing van biometrie die wordt gebruikt ervoor kan zorgen dat een persoonsgegeven een bijzonder gegeven wordt.

Artikel 8 (1) van de Richtlijn luidt:

De Lid-Staten verbieden de verwerking van persoonlijke gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen.

Vormt dit nu een wezenlijk beletsel voor inzet van biometrische identificatie? Als uit een template geen volledig signaal meer is af te leiden (het algoritme kan niet 'terugrekenen' en het volledige oorspronkelijk (analoge) signaal reconstrueren), geldt dat het template wel als persoonsgegevens maar misschien niet als een bijzonder gegeven is aan te merken.

beveiliging

Het derde aspect in de regelgeving dat van belang is voor het verwerken van biometrische gegevens, is *beveiliging*. Artikel 17 van de richtlijn geeft aan dat persoonsgegevens moeten worden beschermd tegen allerlei vormen van onrechtmatig of onzorgvuldig gebruik. Deze wettelijke verplichting tot het nemen van beveiligingsmaatregelen geldt op grond van de classificatie als persoonsgegevens uiteraard ook voor biometrische gegevens.

Biometrie verantwoord toepassen

De invoering van biometrie betekent kansen en bedreigingen. Hoe kan hier op een verantwoorde manier mee worden omgegaan? Allereerst moeten de wettelijke randvoorwaarden, zoals hierboven uiteengezet, in het oog worden gehouden. Maar het is ook belangrijk dat de techniek voor biometrische identificatie zodanig wordt ingezet dat de privacy zo min mogelijk bedreigd wordt. De Registratiekamer hanteert het begrip Privacy Enhancing Technologies (PET) als verzamelnaam voor technische maatregelen om het gebruik van persoonsgegevens te vermijden of te beperken.

Als eerste moet altijd onderzocht worden of er voor het beoogde doel nodig is om personen te identificeren of dat een authenticatie volstaat. In veel gevallen is het immers helemaal niet noodzakelijk dat iemand zijn identiteit prijs geeft. Soms kan het voldoende zijn om vast te stellen dat iemand inderdaad degene

is die een bepaald recht mag uitoefenen, bijvoorbeeld een lidmaatschap. Daarnaast kan er gezorgd worden voor een decentrale opslag van templates. Ook de cryptografische beveiliging van gegevens verdient aandacht.

Op hoofdlijnen gelden voor verantwoord biometrie de volgende vragen:

- 1 Welke gegevens zijn echt nodig voor het doel?
- 2 Worden de gegevens rechtmatig ingewonnen? Is de betrokken persoon geïnformeerd?
- 3 Is er sprake van 'bijzondere gegevens'?
- 4 Wat gebeurt er met de oorspronkelijke biometrische gegevens? Worden deze verwijderd?
- 5 Zijn de biometrische gegevens zo opgeslagen dat ze niet meer terug te voeren zijn tot de oorspronkelijke gegevens?
- 6 Is het mogelijk om de meting van de gegevens en de verificatie decentraal te laten plaatsvinden?
- 7 Is de beveiliging van templates voldoende?
- 8 Rechtvaardigt het doel een eventuele centrale opslag van biometrische gegevens?

Conclusie

De komst van biometrische identificatie is een belangrijke trend binnen de beveiliging. Verantwoorde inzet van biometrische identificatie betekent dat rekening wordt gehouden met de wetgeving voor de bescherming van persoonsgegevens. Ook is het belangrijk dat een identificatiesysteem technisch zo worden ingericht dat een minimale hoeveelheid persoonsgegevens wordt ingewonnen, en dat de verspreiding van die gegevens voorkomen wordt.

Registratiekamer

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag
Telefoon 070-381 13 00
Fax 070-381 13 01
mail@registratiekamer.nl
Internet: www.registratiekamer.nl

R. Hes
T.F.M. Hooghiemstra
J.J. Borking

At face value

On biometrical identification and privacy

Achtergrondstudies en Verkenningen 15