Biometrics and privacy

Jan Grijpink[1]

Biometrics offers many alternatives for protecting our privacy and preventing us from falling victim to crime. Biometrics can even serve as a solid basis for safe anonymous and semi-anonymous legal transactions. In this article Jan Grijpink clarifies which concepts and practical applications this relates to. A number of practical basic rules are also given as a guide to proceeding in a legally acceptable manner when applying biometrics.

1. Introduction

The term 'biometrics' is taken to mean the identification of individuals based on a physical characteristic using information technology. Checking people's identities visually using a passport photo or a description would not normally be described as biometrics. We do however speak of biometrics if the check is performed using a computerised system. These days, information technology makes it possible to quickly digitise physical characteristics so that we can either depict them as an image or subject them to calculations. This can be done with the contour of a hand or a finger, a fingerprint or the pattern of an iris. Even variable physical characteristics can be used for biometric identification of an individual, such as his voice, the way he moves his hand when writing his signature, or his rhythm when typing certain words on a keyboard. Checking someone's identity biometrically involves comparing a previously measured physical characteristic with the result of a new measurement at the time and place of the check. The result of the previous measurement can be registered in the verifying authority's information system, or on a chipcard held by the person being checked.

Up to now only little use is being made of biometrics. This is first and foremost a consequence of its lack of familiarity, not least because the necessary information technology has not been available at a reasonable price for very long. But there are also prejudices against biometrics and all sorts of negative images about intrusion into people's private lives and damage resulting from crime. Uncertainty about the legal permissibility of using biometric data also plays a role here[2]. This should not come as a surprise, given that there are many conceivable biometric applications, each of which have different legal implications and effects on privacy. The question of whether the use of biometrics gives rise to additional risks or provides better protection and more privacy depends on the specific application. Upon closer examination, even the legal status of a biometric detail depends on the application. The purpose of this article is to make that difference more transparent, also in legal terms, in order to give a clearer indication of what the special significance of biometrics in an information society can mean to the protection of people's private lives and fraud prevention. A number of practical basic rules are also given as a guide to proceeding in a legally acceptable manner when applying biometrics.

---

[1] Dr *mr* J.H.A.M. Grijpink is Principal Advisor at the Directorate for Strategy Development of the Dutch Ministry of Justice. This article was written in his private capacity. He would like to thank Prof. *mr* J.E.J. Prins, *mr* A. Patijn, *mr* L. Mutsaers and H. van der Heijden for their contributions to this article.

[2] For this reason, on 18 May 2000 the Dutch Data Protection Authority organised an initial social discussion on the use of biometrics.

This article mainly deals with the use of biometric data with the purpose of checking someone's identity during transactions (admission, ordering, payment, agreement) using computerised systems, on the spot and instantaneous, both for the protection of individuals and for crime prevention. Certain biometric technologies such as DNA are not (yet) suitable for this purpose, and are therefore not addressed here. The use of biometrics in criminal proceedings, for the identification of mortal remains and in investigations into people's origin, descent or health also fall beyond the scope of this article.

Although biometrics provides both protection against fraud and other crime and the protection of people's private lives, the emphasis of this article will be placed on the privacy aspects. The article is laid out as follows. First of all, three examples are given containing elements that will later be placed in a broader perspective. The usefulness and necessity of biometrics are explained in paragraph 3. Paragraphs 4 and 5 discuss two general aspects: the legal status of a biometric detail and the various methods that can be used to check a person's identity. This will be followed by an explanation of the various characteristics of biometric applications, and some practical basic rules will be formulated. Some conclusions are given in paragraph 8.

2. Some examples of the application of biometrics

The first example describes the checking of someone's identity biometrically using a chipcard. When this chipcard is issued, the card issuer has calculated a biometric template based on the future card user's hand contour, for instance, and has placed it on the chipcard. The card issuer can maintain a central register of all issued chipcards with the unique card numbers and the biometric templates of the card holders. This is not however necessary, as a reference template calculated on the basis of the unique card number and the accompanying template would be sufficient to establish at a later date whether the card is authentic and still contains the original biometric template. At the time of the check, the person being checked inserts his card into a reader, which, having verified that the card is authentic, compares the chipcard template with the result of the new reading[3].
When issuing the chipcard the card issuer can check the identity of the future card user on the basis of a valid identity card, but this is in fact unnecessary. In the first case, the card issuer knows who the card holder is. In the second case use could be made of an anonymous[4] chipcard that facilitates an accurate personal check without revealing precisely who the card holder is. Both types of checking a person's identity biometrically with a chipcard can be used, for instance, to authorise access or to establish a person's agreement to a transaction. This can be done off-line in a local application, or on-line as part of a central application operated remotely.

The second example illustrates that biometrics can also be used without a chipcard. The example is a museum application designed to prevent people from remaining in the building after it closes. This is an off-line local application of biometric recognition of visitors using a biometric template. The biometric template is linked to a one-off pin code selected by the visitor himself. This pin code is necessary because the 'point of reference' of a unique chip-

[3] The safest way of doing this is to compare the templates in the chipcard rather than in the chipcard reader in order to make it more difficult to imitate the verification.
[4] 'Anonymous' means that it is not possible to establish who somebody is. 'Semi anonymous' means that at least one authority knows who the card holder is, but this cannot be established by any other verifying authorities.

card number is not available in this application. The self-selected pin code indicates which templates have to be mutually compared. Without that pin code a comparison of templates is not reliable, because measurements of the same physical characteristics of the same person always show minor differences. For this reason, two measurement values that are in close proximity to each other do not necessarily originate from the same person. Because this application does not register any other information about the visitor and the one-off pin code is selected by the person himself, the visitor's anonymity is guaranteed. The application works as follows. A visitor can only enter the building once he has entered the self-selected pin code and the access computer has calculated a biometric template based on the shape of his hand, for instance. He will only be able to leave the building again once he has re-entered his pin code and the computer has not detected any major deviation between the biometric measurements related to that pin code upon his arrival and departure. The computer then deletes both the self-selected pin code and the two biometric templates. A check is made to establish whether all readings have been deleted every evening when the museum closes. If not, all visitors to the museum have not yet left the building. If a visitor is indeed found in the building after closing time, it is possible to establish whether that person is the one that the museum staff are looking for by checking with the biometric characteristic that remains in the computer.
In this example the use of biometrics is entirely anonymous, but accurately indicates whether a visitor has remained in the building after the museum has closed. By using the person-related character of a biometric detail we can electronically, without human intervention, establish that *the same* person has arrived and departed, without needing to know the exact identity of the visitor concerned. This emphasises the fact that an accurate check of a person’s identity can in principle even be made using an anonymous biometric detail. For the significance of biometrics for the protection of privacy, it is important to be aware that anonymous biometrics can be just as accurate as personalised and semi-anonymous biometrics, because the biometric characteristic is always person-related.

The third example is an application at an airport that is designed to detect suspect luggage, and to prevent people from being supplanted between the moment they check in and the moment they board the aircraft. At the moment that the passenger checks in, his biometric template is calculated and stored in a temporary file for the flight in question together with the (unique) numbers of the boarding pass and any luggage labels. When the passenger is due to board the aircraft, as part of the safety check the template is recalculated and compared with the template in the temporary file that accompanies that particular boarding pass. If the discrepancy between the measured values is too big, it is desirable to conduct a further identity check to establish whether that person has been supplanted. If the comparison shows that this is not the case, the biometric data are immediately deleted. If, at the time of departure, there is still an unmatched biometric detail left in the temporary register, the accompanying luggage can be traced and taken off the aircraft. This luggage apparently does not belong to one of the passengers who have boarded, and represents a safety risk. Because boarding passes are issued in people's names once proof of identity has been verified, this application makes use of personalised biometrics. However, if the personalised biometric data are deleted immediately after they have been used, this application of biometrics does not invade people's privacy. The advantage of personalised biometrics in this application is that in cases of doubts about someone's identity or unattended luggage, the airport staff immediately know whom they need to look for. In the event of a deliberate act, the biometric characteristic left behind can be used to prove who was involved in the incident.

3. Usefulness and necessity of biometrics

Biometrics derives its significance from the person-related nature of the physical characteristic that serves as the point of recognition. In comparison with the customary non-person-related methods to check someone's identity such as pin codes, passwords, electronic signature or encryption keys, biometrics therefore has a number of general advantages, which - depending on the application - make the recognition of an individual person accurate whilst simultaneously protecting people's privacy:

a. you always carry a biometric template with you, you can't leave it at home,
b. a biometric characteristic cannot be transferred to someone else unobtrusively,
c. a detached biometric characteristic cannot be traced back to the person from whom it originates without additional clues,
d. biometric techniques are not subject to recognition errors due to faulty observation resulting from preconceptions, distraction or tiredness, for instance.

These general advantages are however accompanied by some disadvantages. Because a biometric reading does not yield precisely the same template on each occasion, biometrics does not provide complete certainty in identifying the legal holder of a biometric characteristic. The more closely two measurements resemble each other, the more probable it is that both values relate to the same person. In biometric applications one can decide which measurement discrepancies are acceptable to be still able to assume that the values originate from the same person. But many biometric systems will consider two perfectly identical values as a fraud. Thus, if the measurement value of someone else closely resembles my measurement value, he may be able to pass himself off as me. The more accurately we configure the calculation, the less chance there will be of this happening, but the chance of my not being recognised increases accordingly! The extent to which this can be accepted depends on the situation and the application.

The advantages of biometrics over human checks are however of overriding importance:

- if we want to guarantee people's privacy when checking people's identities.
  A biometric check can even be accurate with the off-line, local use of an *anonymous* physical characteristic, with or without a chipcard;
- if one may expect many human recognition errors in a concrete situation.
  For instance, if one has to check large numbers of people quickly, over a long period of time or from a distance.

In situations where it is necessary to guarantee absolute privacy, or where there is a significant chance of mistaken identity or identity fraud or the consequences of this could be very serious, biometrics is indispensable. People are gradually becoming aware that the use of biometrics therefore has to be advanced, and that governments will have to do whatever they can to diminish the potential negative effects of biometrics.

4. The legal position of a biometric detail

To properly understand the social significance of biometrics, we need to make a distinction between a *person-related detail* (= derived from the body) and a *personal detail* (= can be traced back to a person). Many people intuitively feel that a person-related detail must also be a personal detail as defined by Dutch (and European) privacy legislation. An anonymous

biometric characteristic, i.e. a detached biometric template without anything in common with the source, cannot be regarded as a personal detail because it cannot be traced back to the person from whom the measured value originated, or this can only be done with disproportionate effort. A good example of anonymous biometrics is dirty glassware in a restaurant. It is a hopeless task to trace a fingerprint on one of the glasses to a restaurant diner who has already left. One will never be able to find him. This could explain why we don't concern ourselves too much with this glassware in practice.

A biometric personal characteristic is therefore by definition person-related, but is not necessarily a personal detail. The decisive factor regarding the legal position of a biometric detail is therefore whether it can be traced back to the right person, if necessary making a good deal of effort. For this purpose we have to look at the application as a whole rather than only at the biometric detail on its own, removed from the context. We therefore have to take account of all the surrounding technical, procedural and organisational provisions. If a biometric detail within an application is truly anonymous, it is safe so say that its use does not in legal terms fall within the constraints set by privacy legislation for the use of personal data. There are no legal obstacles to the use of anonymous biometrics. From the perspective of protecting people's privacy in society, anonymous and semi-anonymous biometric applications[5] in particular will in the future have major significance. For a biometric detail does not lose its anonymous character for a verifying authority if another authority - e.g. the card issuing authority - knows exactly who the person concerned is but may only reveal that information to a competent authority with the approval of the law or the court. Many biometric applications do however use biometrics registered in people's names (personalised biometrics), even if the purpose of the application can be achieved just as well with anonymous biometrics.

Many biometric applications are based on biometrics registered in people's names (personalised biometrics), even if the purpose of the application could be served just as well using anonymous biometrics. Biometrics will not realise its full social significance until we recognise and utilise the wide-ranging possibilities offered by the anonymous use of biometrics.

5. Recognition method and privacy

The implications of biometrically checking people’s identities for their privacy and the prevention of fraud is significantly determined by the method used for the recognition of an individual. We make two different distinctions.

The first distinction, identification or verification, relates to the envisaged knowledge concerning a person's identity. There are two alternatives:

a) establishing precisely *who* someone is (identification),
b) establishing whether a person is the right person, for instance the *same* person as expected (verification).

The establishment of a person's true identity involves an actual investigation into someone’s identity, and is therefore something that is rarely done in the Netherlands outside of criminal law enforcement and immigration. It is deemed sufficient to establish whether a person is the same person as expected, by ascertaining whether several pieces of information belong to the same person, for example. This is often erroneously referred to as 'identification': in actual

[5] 'Anonymous' means that it is not possible to establish who somebody is. 'Semi-anonymous' means that at least one authority knows who the card holder is, but this cannot be established by any other verifying authorities.

fact it yields no more than a verification. Verification is less far-reaching than identification because we remain unsure whether a person actually is *who* he says he is. But in many social situations, such as the museum example given above, this is sufficient. In that example, a verification provides sufficient guarantees against someone remaining in the building unnoticed after it has closed. By using the person-related character of a biometric detail we can electronically - i.e. without human intervention - establish that *the same* person has arrived and departed without needing to know the exact identity of the visitor. This emphasises the fact that an accurate personal verification can in principle even be made using an anonymous biometric detail.

The second distinction, inclusion or exclusion, relates to another basic approach to checking someone's identity:

a) we can *positively* establish whether someone is indeed the right person.
   This is referred to as the 'inclusive' use of a recognition technique;
b) we can *negatively* establish that someone is *not* the right person.
   This is referred to as the 'exclusive' use of a recognition technique.

In the actual practice of biometrics this difference has major implications, especially when it comes to comparing two images of a physical characteristic, for instance two fingerprints. A single point of difference is sufficient to exclude someone with one hundred percent certainty! On the other hand, inclusive use *never* gives one hundred percent certainty, even though that certainty does of course grow with each point of similarity that is ascertained. When using only one biometric template, it is only possible to perform an 'inclusive' check. If it is necessary to establish immediately that someone is *not* the right person (exclusion), at least two different templates have to be used. After all, in a case of mistaken identity, the chance of two physical characteristics being relatively just as close together is virtually ruled out. An accurate exclusion is thus just as possible as when using a single biometric image.

The 'exclusive' use of a biometric characteristic to establish that someone is *not* the same person barely penetrates into people's private lives, but inclusively establishing a person's identity does. Information technology does in fact make the least radical form of checking someone's identity biometrically, the *exclusive* use of *anonymous* biometrics, technically feasible. Therefore, from the a privacy perspective it is notable that there is in practice a spontaneous preference for the most radical form, the *inclusive* use of *personalised* biometrics. We see here a mission for those who endorse the issue of privacy.

6. Types of biometrics

Biometrics calls for tailor-made solutions: technical, organisational and legal. There are many different biometric techniques and forms of applications, but no single one of them is suitable for all problems relating to checking a person's identity. The legal aspects also differ between forms of application. There are no legal obstacles to certain forms because the anonymity that has been achieved renders superfluous other measures for protecting people's privacy. For other forms, wide-ranging legal requirements have to be met. It is not yet clear whether these will have to be strengthened in the future, but there is certainly no case for weakening them.

In addition to the different recognition methods distinguished above, a distinction can also be made between various biometric techniques and aspects of application:

1. *Variable or fixed physical characteristics*
   Fixed physical characteristics can be more successfully copied and imitated than variable characteristics. A person can also himself change a variable physical characteristic without this being noticed, thus avoiding identification. This is useful if a person is under threat, but will generally fail to offer an adequate solution for situations in which it pays to pass oneself off as two different people. This will, for example, meet with success in an application which uses a biometric template calculated from a variable physical characteristic to prevent someone from presenting himself twice as a different person, thus acquiring two different authorisations. Adapting the variable physical characteristic results in two different templates, thus ensuring that this biometric check against double identities fails. A person can also ensure that he is not recognised by deliberately changing the movement he makes when writing his signature, in order to pass himself off as someone else in an emergency procedure. If considerable advantage can be gained by doing this, it is better to use an unchangeable physical characteristic when checking someone's identity.

2. *Image of a physical characteristic or a template calculated from it*
   With an image of someone else's finger tip, a person can pass himself off as someone else when checked. This approach could even be used to spuriously suggest someone's involvement in a transaction or action. These situations can not occur if use is made of a template for the purpose of checking someone's identity. A template is a biometric number calculated from a number of unique characteristics, found in a fingerprint, for instance. Because the other information contained in the image is not used in the calculation, it is not possible to retrospectively calculate the original image of the fingerprint from the biometric number (template). For this reason there is not much that can be done to cheat with a biometric template, certainly if it is difficult to establish who the measured value originated from and which formula was used to calculate the number. In the Dutch regulations no distinction is yet made between biometric images and biometric templates, but there are already countries that (want to) forbid the central storage of biometric *images*, or impose stricter regulations on the central storage of biometric images than will apply to the central storage of *templates*.

3. *Central or decentralised storage*
   At the one extreme, there is the decentralised storage of a single biometric detail on a single chipcard placed in the hands of the person from whom the biometric detail originates. This makes it possible, for example to check from a distance and off-line whether the actual user of the chipcard and its lawful holder are one and the same person. This is a possible use of biometrics that facilitates privacy-friendly applications. The other extreme consists of the storage of all biometric data in a single central file for on-line checking of people's identities. 'Central' in this context means that all stored biometric details can be directly accessed and compared with each other. The biometric details can be physically concentrated at the same location, but this is not necessary. This central file makes it possible to perform additional checks that would not be possible with separate chipcards alone. The administrator of a central file of biometric images can, for example, immediately establish whether a person is already included in the file, but under a different name. The distinction between central/decentralised is of legal importance because central storage involves more social risks.

4. *Anonymous or by name ('personalised')*
   If biometric data cannot be traced back to individuals (anonymous) there are in principle no (Dutch or European) legal obstacles to using them. There are no (Dutch or European) regulations that set requirements for applications that make use of anonymous biometrics. The situation is different when it comes to personalised biometrics. In this case the biometric detail is placed in someone's name, or the name can be established with some - but not disproportionate - effort. Dutch (and European) privacy legislation provides for various protection regimes that cover biometric personal data, depending on their degree of vulnerability and the purpose of their processing.

5. *Voluntary or compulsory*
   Compulsory co-operation with checking someone's identity using biometrics imposed by the government or by private bodies requires a legal basis. In the private sector the voluntary use of personalised biometrics is in principle permitted, unless the biometric characteristic can be used to establish someone's race or origin. Then only necessity counts. As long as this is not the case, it is sufficient to operate regulations in the area of contracts, in which people must work within the constraints of the privacy legislation if biometric personal data are used. But when is voluntary co-operation truly voluntary? This is not solely determined by market conditions, but also by the existence of a fully-fledged alternative facility without biometrics, so that true freedom of choice is possible. If on a really voluntary basis, even a public authority may use biometrics without such use being explicitly provided for by the law.

6. *Small-scale or large-scale*
   In a small-scale application, the uniqueness of the physical characteristic is less important because the chance of two individuals having virtually the same physical characteristic reduces as the target group becomes smaller. An important legal point is that the large-scale application of biometrics appears to qualify sooner for preventative government control or another form of regulation because the risks to privacy and the risk of falling victim to crime are more difficult to manage, and there are more opportunities to deliberately passing oneself off as someone else. Currently many biometric techniques are vulnerable to fraud and privacy issues if applied on a large scale. Small-scale applications are less risky and will in principle be more likely to promote privacy, certainly if a large number of small-scale applications are gradually developed which make increasing use of different biometric techniques and application types. A large number of small-scale applications offer a double advantage to the protection of privacy and the prevention of crime: one can reduce the consequences of an identity fraud that has not been detected to a minimum, and subsequently have more opportunities to unmask a successful impostor.

7. *Open or closed target group*
   A closed target group is one in which the people that pass a biometric checkpoint are expected to return to the same checkpoint within a short period of time. In a closed group of this nature, the chance of two virtually identical measurements arising that could possibly lead to mistaking a person's identity is smaller than with open target groups. Within closed groups a simple application using anonymous biometrics yields a check in which an outsider has very little chance of successfully passing himself off as one of the members of the group.

This list of the different aspects of biometric applications is not exhaustive. Its purpose is to point out that biometrics facilitates a wide range of applications, some of which give rise to few and some to many legal questions. Small, 'exclusive', anonymous biometric verifications are more suitable for promoting privacy. Moreover, there are few obstacles to these applications in legal terms, even when used voluntarily by public authorities. If applied on a large scale, many biometric techniques are vulnerable to fraud and privacy issues currently. Compulsory, large-scale applications of personalised biometrics therefore need not to be implemented without careful consideration and very strict security measures. Much attention should be given to the legal aspects of these applications. Already, the current Dutch (and European) privacy legislation provides for strict requirements for applications of this nature. Because the development of the technology is by no means complete, and the number of operational applications of biometrics is still limited, it is not yet possible to gain an overall view of the social risks involved. For this reason it is not yet clear whether governments in the European Union will impose further regulations on the use of biometrics in the next few years.

7. Basic rules for the use of biometrics

A number of basic rules can offer a frame of reference regarding the question of which biometric applications are legally acceptable. If in doubt about the legal permissibility of a concrete application, in the Netherlands advice can be sought from the Dutch Data Protection Authority.

The basic rules are set out below in the form of a checklist, which does not however profess to be complete.

1. *Sectoral boundaries*
   One of the fundaments of the protection of privacy is that data from a certain sector cannot automatically be used in another sector. The use of biometrics should therefore not automatically be permitted to exceed the sectoral boundaries that have come about in practice and been sanctioned by law. The sectors in question include banking, health care and, education, and, in the public sector, taxes or civil affairs. A biometric application therefore requires clear boundaries, regardless of whether it has a private or public character. Applications with a supra-sectoral character call for explicit public approval because the implications for the protection of privacy could become apparent only gradually and over a wider area than people may initially have anticipated. A regulation by law could supply the necessary approval.

2. *Clear, recognisable and permissible objective*
   The purpose of the use of biometric data must be made clear and recognisable to all involved, by displaying an explanatory text at the place of use, for instance. In the case of a government application, democratic decision-making usually results in sufficient familiarity because a generally binding regulation is usually required for the application. An unlimited objective is not sufficient to permit the use of biometric data, and neither is an application with several mutually irreconcilable objectives. The mutual balance of power between the customer and the company plays an important role when assessing the permissibility of the objective of an application in the business area.

3. *Proportionality*
   The use of biometrics should be proportional. In other words, there must be a reasonable relationship with the objective for which it is used. The use of biometrics should not in principle be chosen if the objective can also be reached using other, less radical means. Access to important buildings can be checked using the shape of a person's palm (protecting secrets, preventing theft or violence), but a less radical alternative must be sought for secondary schools. The objective should, for example, also justify the involuntary nature of a biometric application. The principle of 'anonymous biometrics, unless' could be regarded as an example of the application of the proportionality rule. If the job can be done without personalisation, anonymous biometrics must be chosen.

4. *Subsidiarity*
   Subsidiarity means not having to take things 'higher up' unnecessarily. What an entrepreneur can do himself must not be done at trade level or by the government. What can be done by the municipal government should not be taken over by the provincial or national government. This general principle holds equally true for biometrics. What can be done at sectoral level must not be tackled with a general solution. If a biometric application can meet its objective without a centrally accessible biometric database, a biometric characteristic should be stored exclusively on a chipcard.

5. *Precise delineation of the target group*
   The target group of a biometric application must be clearly defined (in advance). This is especially important to the permissibility of the application and communication with that target group. This also determines the way in which the legal relationship between the parties can be substantiated. If the target group is the entire population of a municipality, the obvious approach will be to impose regulation via legislation or local by-law. If it concerns the personnel of a company or the clientele of a shop, the rules and agreements could be laid down in the employment contract or general terms and conditions respectively. A precise description of the target group facilitates (external) monitoring of the data collection process.

6. *Security*
   In Dutch law a breach (only) becomes an offence if the biometric detail is protected against unauthorised alteration or perusal. A lot of attention should therefore be paid to the security of the application. Procedural and organisational safety risks must also be addressed.

7. *External supervision*
   It may be desirable to have the use of biometric data supervised by an independent party. This is important in cases where the law calls for demonstrable due diligence on the part of the administrator.

Partly in view of the limited practical experience and technical development, it is not yet possible to give an indication of the limits to the use of biometrics. This brief set of basic rules could be further developed on the basis of the practical applications used by the government and the business community. Biometrics require tailor-made solutions, also when it comes to the law.

8. Conclusions

We summarise some of our conclusions. Biometrics will in due course be of great significance to the protection of privacy and the prevention of crime. People are gradually becoming aware that the use of biometrics therefore has to be advanced, and that governments will have to do whatever they can to diminish the potential negative effects of biometrics.

From the perspective of protecting people's privacy in society, anonymous and semi-anonymous biometric applications in particular will in the future have major significance. For a biometric detail does not lose its anonymous character for a verifying authority if another authority - e.g. the card issuing authority - knows exactly who the person concerned is but may only reveal that information to a competent authority when required to do so by law or by court order.

No new rules or measures are needed for anonymous biometrics as such[6]. It is not yet clear which legislation or governmental intervention is required for semi-anonymous and personalised biometrics. Does the central storage of personalised biometric images have to be subjected to restrictions or forbidden, as has already happened in some countries? Will the legal obligation for people to prove their identities have to be extended to the issuers of biometric chipcards with a view to combating identity fraud? If so, regulations and measures will be needed to legally and practically enable the card issuers to verify the accuracy of the proof of identity presented to them.

The person-related nature of biometrics by no means implies that it is impossible to tamper with a biometric verification. The actual sensitivity of biometrics to privacy intrusion and fraud differs between situations and depends on the selected combination of technique and method of application, including the surrounding organisation and procedures. Emergency procedures triggered by the malfunctioning of an electronic verification system are notoriously problematic. In these cases people invariably fall back on defective methods with a significant chance of errors occurring, such as a visual identity check based on a photograph or directly deriving information from an unverified or unverifiable document. Insiders know how prone people are to seeing what they expect to see, and how difficult it is to differentiate between lookalikes. Moreover, it is important to bear in mind that - unlike the situation in the analogue era - it is not the verifier but the person being verified who has the upper hand. After all, he is one hundred per cent certain of being able to activate an emergency procedure, by imperceptibly using someone else's chipcard, for example, or by pretending that he has lost his card. The security and the reliability of a computerised biometric recognition system depend only partly on the biometric technique itself, or the information systems involved.

The design of a biometric application involves a large number of implicit choices that determine the effectiveness of the application, its sensitivity to fraud and the consequences for personal privacy. These should not be left to the technicians. Many biometric solutions are still sensitive to fraud and privacy issues when used in large-scale, personalised applications. This is why small-scale, anonymous biometric verifications are presently of strategic impor-

[6] This does not imply that no new law is required for anonymous legal transactions, also if use is presently made of anonymous biometrics. The scope for anonymous legal transactions in Dutch law is presently limited. The world-wide character of electronic markets does in fact call for a firmer legal basis for anonymous legal transactions. See: Jan Grijpink and Corien Prins, *New legal rules for anonymous transactions?* (to be published shortly).

tance. Moreover, there are few obstacles to these applications in legal terms, even when used voluntarily by public authorities.

The recognition methods of *exclusion* ('that is *not* him') and *verification* ('he is *the same* person, but I don't know who he is') can effectively be combined in small-scale applications, certainly if the target group is more or less closed. In these cases simple technology and procedures are sufficient. If it is possible to keep the biometric detail anonymous, decentralised off-line checking of people's identities can also be effectively done by a small organisation using a small-scale application of its own. This provides adequate protection in many practical situations. There are in any event no legal problems regarding these types of biometric applications.

A large number of small-scale, sector-restricted applications offer a double advantage to the protection of privacy and the prevention of crime: one can reduce the consequences of an identity fraud that has not been detected to a minimum, and subsequently have more opportunities to unmask a successful impostor. In addition, sector-restricted applications offer more legal protection against unlimited linking of personal details using biometric templates, because Dutch (and European) privacy laws give rights (complaint, correction, removal) that can be independently exercised in every sector, thus reinforcing each other. Within a small-scale application the voluntary use of biometrics can be more easily handled because non-biometric exceptions for people who really object to this method of checking one's identity can be better controlled. These considerations illustrate that biometrics requires tailor-made solutions.

The Hague, January 2001

The Dutch version of this article was published in: Privacy en Informatie, 2000, nr 6, pp. 244-250

References:

Robert van Kralingen, Corien Prins and Jan Grijpink, *Het lichaam als sleutel*, ['The body as a key'] legal considerations of biometrics, ITERseries no. 8, Samson, Alphen aan de Rijn, November 1997
Dr mr J.H.A.M. Grijpink, *Identiteitsfraude als uitdaging in een informatiesamenleving*, ['Identity fraud as a challenge in an information society'] in: Security 12, no. 4, April 1999, Amsterdam, Keesing Bedrijfsinformatie
Dr mr J.H.A.M. Grijpink, *Biometrie als anonieme bewaker van uw identiteit*, ['Biometrics as an anonymous guardian of your identity'] in: Security 12, no. 5, May 1999, Amsterdam, Keesing Bedrijfsinformatie
Dr mr J.H.A.M. Grijpink, *Identiteit als kernvraagstuk in een informatiesamenleving*, ['Identity as a key issue in an information society'] in: Handbook for Fraud Prevention, Samson, Alphen a/d Rijn, November 1999, chapter Fraud and integrity, no. E 4010
Dr mr J.H.A.M. Grijpink, *Wie is wie in een informatiesamenleving*: ['Who's who in an information society': 'the case for a chain approach'], in: Management and Informatie, 8th volume, no. 2, May 2000, Samson Bedrijfsinformatie, Alphen a/d Rijn
Dr mr J.H.A.M. Grijpink, *Recht en biometrie, juridische spelregels voor biometrische toepassingen*, ['The law and biometrics, legal rules of play for biometric applications'] in: Security Management, 5th volume, Samson , September 2000
Dr mr J.H.A.M. Grijpink, Checklist Biometrische Persoonsherkenning [Biometric recognition of individuals: in a quest for tailor-made solutions], in: Checklists Information Management (loose leaf), Ten Hagen & Stam, Den Haag, December 2000 (the English text can be downloaded from http://www.interpol.int).