The meaningful, safe and reliable use of biometrics [1]

Prof. Dr J. (Jan) H.A.M. Grijpink

Ministry of Justice / Utrecht University
P.O. Box 20301
NL-2500 EH The Hague
j.grijpink@minjus.nl

Abstract: *This paper introduces the current results of the debates within the Netherlands Biometrics Forum (NBF) on the principles that lead to a meaningful safe and reliable use of biometrics. Biometrics is becoming an important element of our information society, but new technology is often initially used incorrectly. This is partly due to so-called fallacies of the wrong level. In practice, large-scale systems tend to work out differently compared with small-scale applications, thus presenting additional problems at that larger scale that should have been taken into account during design and development. That implies that the first major applications can confront us with worrying social risks for which effective solutions have yet to be found. This paper, therefore, proposes to explicitly use the concept of identity fraud (identity theft) as litmus test of any biometrics application. The point is made that excessive concern about privacy inadvertently exacerbates these social risks. It is made clear that the assessment criterion 'safety' implies the protection of privacy, but that this does not necessarily apply the other way round. Because current large-scale applications seem to have neglected major privacy and security risks, this paper is primarily meant to stimulate this debate.*

1 The Netherlands Biometrics Forum (NBF) [2]

The Netherlands Biometrics Forum (NBF) is a foundation that advocates the meaningful, safe and reliable use of biometrics. Having the international character of biometrics in mind it focuses on the Dutch situation highlighting both the interests of the public at large and of the professionals involved. The NBF attempts to create more awareness regarding what can and cannot be done with biometrics, and a clearer understanding of the opportunities and risks. It is desirable to ultimately achieve social acceptance of this technology. That calls for trust. The NBF is convinced that this trust cannot be enforced

---

[1] Jan Grijpink is Principal Adviser at the Dutch Ministry of Justice (Information Strategy) and professor of Information Science (Chain-computerisation) at the University of Utrecht. He is chairman of the Netherlands Biometrics Forum (NBF).

[2] www.biometrieforum.nl

but must rather be earned. During the past two years many professionals from the public and private sector and the scientific community in the Netherlands have worked on formulating key principles for the meaningful, safe and reliable use of biometrics in what is known as a position paper. This document is periodically updated on the basis of new experiences and insights. In this phase of development of the NBF's position, the NBF wants these principles shared and challenged.

2 Biometrics

The term 'biometrics' is taken to mean: automated recognition of individuals based on their behavioural and biological characteristics. These days, information technology makes it possible to quickly digitise behavioural and biological characteristics so that we can either depict them or subject them to calculations. This can not only be done with unalterable characteristics such as the contour of a hand or a finger, a fingerprint or the pattern of an iris but with alterable characteristics as well, such as a voice, the way somebody moves his hand when writing his signature, or the rhythm of typing certain words on a keyboard. Biometric verification involves comparing a previously measured characteristic against 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 chip card or another electronic document held by the person being checked.

Many people find it difficult to fathom the technology needed for biometric person recognition because it is based on the laws of probability and thus necessarily leads to a number of erroneous acceptances and rejections (the extent of which depends on the tolerances set by the operator himself). For that reason biometrics never offers complete certainty (100%) that someone is the right person. That way, biometrics also makes erroneous connections between people and their documents or data. The fact that biometrics cannot make any statements about the integrity of these documents and data or about the accuracy of the link itself implies that biometrics is unable to conclusively establish who somebody is. Contrary to what many people think, biometrics can only calculate the probability that somebody is the right person! This makes biometrics vulnerable to privacy and security concerns. [Gr01; Gr08].

3 The future of biometrics

The importance of computerised person recognition is becoming increasingly important in an anonymous information society characterised by increasing global mobility. As compared to administrative verification methods such as a PIN code, password or key, only biometrics is based on a person-related behavioural or biological characteristic as the point of recognition. Biometrics will ultimately become indispensable for sensitive work processes in the public and private sectors. Biometrics is especially useful when we need to know for sure that the person we are dealing with is the right person, or when someone wants to prevent his identity from being stolen and misused by somebody else.

That constantly sets different requirements for computerised person recognition, depending on the risks in a given context.

Two examples [3]

1. A swimming pool organisation wanted to use fingerprint verification to exclude a certain group of boys that was repeatedly harassing girls. A worthy aim, but the devil is in the detail. All visitors (both male and female) were asked to register their fingerprints in the swimming pool's computer system. This application threatens the bright future of biometrics. First, if you have the fingerprints of the boys you want to exclude from swimming, it is sufficient to check the fingerprints of male visitors belonging to the relevant age group. [4] Second, if someone's fingerprint is included in the blacklist, he can be sent on his way. Therefore, there is no need to store fingerprints at all. There is no point whatsoever in checking and storing the fingerprints of girls. And the story gets even worse. A woman of 82 refuses to cooperate with having her fingerprints checked and is therefore banned from the swimming pool.

The NBF's position is this: biometrics must be necessary and the purpose is the deciding factor regarding the rights and wrongs of how biometrics is to be implemented and used.

2. A car rental company was having a lot of difficulties with cars being returned. Many rented cars were not returned or were taken to the wrong place. Biometrics looked promising, but must not be too expensive. A creative employee came up with a solution without the need for expensive electronics: the fingerprint was placed on the paper rental contract with gel, with the assurance that the paper containing the fingerprint would be returned when the car was brought back. This experiment proved to be a resounding success: during the experiment no stolen or incorrectly returned vehicles! All well and good. But watch out! This simple biometrics system was introduced elsewhere by the same company, too. A few months later this site's administration proved to be full of copies of rental contracts with fingerprints without there being any need for them!

For that reason the NBF calls for attention to be paid to a biometrics application as a whole, the development of an application in the course of time being just as important as practical details such as the contracts' administration.

These examples illustrate how easy it is to use biometrics incorrectly. This engenders unnecessary resistance among the public and undermines social acceptance. Because

---

[3] The examples in this paper are mostly taken from public sources, but some stem from private practice of the NBF's participants. They have all been used to underpin and test the NBF's position during the development of the NBF's position paper.

[4] Such a blacklist may be constructed and maintained under the European Data Protection Directive and Dutch national law if the culprit's fingerprints are taken after a case of misbehaviour and used during a limited period of time and if the list's purpose is clearly explained to the public and the boys involved.

biometrics will ultimately become indispensable to our information society, the NBF regards this as a problem. Both examples also highlight the importance of providing information to the public and organisations wishing to use biometrics. We must guard our biometric details jealously, certainly those which are derived from unalterable biometric characteristics such as our fingerprints. Once compromised, the problem will remain for a long time without the possibility of defending ourselves by altering that biometric characteristic.

4 Fallacies of the wrong level

In information science, in common with other social sciences, we often gain insights from small-scale applications, such as at the level of a person or an organisation. We then translate those insights – usually without a second thought – into large scale applications, such as at the level of a chain or a social sector. In doing so we are likely – often without noticing it – to make what is known as a fallacy of the wrong level, for insights are related to the level at which they are gained and are generally invalid at other levels (higher or lower)! [Gr05; Gr06a, Gr10]. That results in all sorts of assumptions and principles in large-scale systems being incorrect, so that these systems contain more shortcomings and risks than we think or expect.

Two examples: the biometric passport and the biometric visa

1. Our first example concerns the new biometric passport. This is based on the notion that somebody can accurately be verified by his fingerprint. This essentially small-scale notion should not automatically be extended to the national or international scale of border control. Otherwise it is uncertain whether the biometric passport delivers what is expected of it. Large-scale systems function differently from small-scale ones because on this scale there is no coordinating or enforcing authority. Moreover, large-scale systems involve huge numbers of stakeholders (members of the public, travellers and patients) and cooperating autonomous organisations and professionals that causes large-scale processes to be barely manageable. Despite all good intentions much goes wrong.

Biometrics, too, can be supposed to work differently at large-scale level (chain, sector, country) than one might think from small-scale ideas, and can sometimes be counter-productive. Imitating or counterfeiting the fingerprint on the passport can enable someone to get through the check without it being possible to find out afterwards who it was because traces left inherently point to the official holder, not to the identity fraudster. Scaling up without taking a closer look at the risks of the large-scale situation is therefore a risky undertaking. And even then it is advisable to scale up gradually. For instance, by first having a fingerprint check carried out at the moments of the application and the delivery of a passport without the fingerprints being stored in the passport. Then, in a later stage, one could also store the fingerprints in the passport on voluntary basis, to begin with for those wishing to travel to the US. And so on.

2. The biometric visa, the second example, has already been introduced to keep out unwanted foreigners even before they come to the Netherlands. For that reason the fingerprints of the traveller are taken at the Dutch embassy in the country of origin during the visa application and sent to the Netherlands. If those fingerprints are included in the database of fingerprints of unwanted foreigners, the visa is refused.

Biometrics can in some cases be counterproductive at that large-scale level. Take a situation where a criminal network wants to send someone to the Netherlands for a criminal act. If the visa is refused, the network knows that it will either have to send someone else or choose a route where the checks are less well organised. That means that rather than the anticipated tighter grip on incoming passenger traffic, the target group of unwanted foreigners can imperceptibly become invisible!

It should be noted that for technical reasons it is not possible to place fingerprints on the visa as we are now doing with the passport. We therefore check visa applicants using the fingerprints in the database only. With these two variants of biometrics, if unforeseen problems arise in the future we can try out which of the two biometrics systems is the most flexible. It would of course have been better to carry out such an experiment beforehand, since once introduced it is barely possible to change a large-scale system such as this.

5 Identity fraud/theft as the touchstone for a biometrics application

By identity fraud we mean somebody with malicious intent deliberately contriving the appearance of an identity that does not belong to him, using the identity either of someone else or of a non-existent person. An identity fraudster has no need for a document or identity card: he can also use a personal number, a photo, an occurrence or a biometric detail because they all contain a suggestion on which people base their conclusion as to who they are dealing with. Identity fraud proves to be easy and does not involve too much risk. When carrying out identity checks we use barely any verification details other than those held by the person being checked. That reduces the chance of getting caught. And if someone gets caught, he has not (yet) done anything wrong! If the identity fraud succeeds nobody is the wiser, while the benefits can be substantial and of long duration. Official means of identifying people, such as an identity card, citizen service number or a biometric detail on the passport are of extra value to identity fraudsters because they must and can be used everywhere. Added to that is the fact that official verification procedures are known, uniform and predictable and can be inconspicuously observed in search of weak spots. Fallback procedures for situations in which the normal procedure cannot be followed (‘I've forgotten my passport...’ or equipment failure) are usually sloppy and improvised and can be triggered by the identity fraudster himself without the identity checking officer knowing, for instance by deliberately using a wrong or invalid token or ID document.

On the other hand, there is the weak position of the victim to consider. As the world becomes more digital identity fraud leaves more and more (technical) traces; but those

traces lead not to the perpetrator, but – inherent in the precise nature of identity fraud - to the victim, who is then faced with proving that he has *not* done something. For that reason the safe use of biometrics makes it necessary to substantially reduce the predictability of identity checks and sharply increase the quality of exception and emergency procedures. Indeed, biometrics should help to achieve that, too.

We therefore need to examine whether identity fraud is being prevented by biometric verification rather than made easier. [Gr04a; Gr04b; Gr06b]. This specific safety aspect of a biometrics application could be scrutinised with questions like the following. Can someone successfully pass through the identity check by imitating the biometric characteristic of the rightful holder? Can someone influence the check and get wrongly recognised as the rightful holder? Is it possible to obtain from the results of the check information that can be used with malicious intent (see the example of the biometric visa)? That is how the phenomenon of identity fraud / identity theft functions as the touchstone for *safe* biometrics. This safety assessment always relates to the biometrics application as a whole, including technology, organisation, procedures and not least the extent to which people cooperate or, conversely, have a vested interest in errors or misuse.

The NBF regards preventing identity fraud/theft as the touchstone for a safe biometrics application. Each biometric technology is in itself easy to mislead or to misuse. The NBF's position is therefore that it is necessary to make *simultaneous* use of several biometric details or technologies in combination with other data or resources since an identity fraudster will not be able to successfully make use of them all at the same time.

6 Privacy and safety

The traces left by identity fraud lead not to the perpetrator but to the victim. Identity fraud thus seriously violates the victim's privacy. That is especially true of identity fraud with an unalterable biometric characteristic since this form of identity fraud can continue to follow someone for a lengthy period without there being much he can do about it. Official bodies initially regard the victim as the perpetrator because all of the clues point in his direction. That often leaves someone having to prove that he is not the perpetrator, which is often hard to do and wrongly leaves the victim under a cloud of suspicion. In the case of biometrics privacy is thus closely related to safety and reputation, depending on the how it has been misused. The discussion about *privacy* in the context of biometrics is therefore unlikely to abate any time soon, but it will however remain abstract for as long as the relationship with someone's *safety* is not expressly made. The point frequently made in discussions about privacy along the lines of 'I don't mind what they know about me, I've got nothing to hide' is put forward by people who have not yet faced a wrongful accusation. If that accusation is based on a misused unalterable biometric detail, the chances of putting up a good defence are not good. This is not a hypothetical risk. At present, virtually all biometrics applications are not safe, certainly in cases where an unalterable biometric characteristic is used on a large scale. The NBF's position is that those concerned about privacy should at this stage focus more sharply on the safety of the large-scale use of biometric personal details, taking account of the

application as a whole and of target groups with other interests. This concept of *safety* goes far beyond the standard privacy discussions concerning the *protection* of these sensitive personal details. [Gr06b; Gr08].With a view to large-scale safety, the NBF's position paper contains various requirements that will need to be met and can help us to assess the social acceptability of a specific biometrics application.

Example

The biometric passport provides us with an interesting example. In Germany, the discussion on privacy has led to two fingerprints being placed on the German passport without the government keeping a copy of any kind. As a consequence, the fingerprints of the person being checked can only be compared with the fingerprints on the passport. That seems fair enough at small-scale level, but it is completely inadequate for large-scale application. The German government then faces a situation where, after issuing the passport, it is no longer able to independently verify whether the fingerprints on it are still the original ones or whether the person present really is the same as the passport's official holder. For the first purpose integer copies are needed of the two fingerprints that have been put on the passport. For the second purpose one or two additional fingerprints of the official holder are needed that have not been put on the passport, because the ones on the passport can be imitated or counterfeited. In The Netherlands, therefore, the government has opted to store the fingerprint of four fingers in a municipal database: the two fingerprints on the passport and two others. The first two make it possible to verify the integrity of the passport, the second pair to directly – i.e. independently of the passport – establish whether the person present is the same person as the legitimate passport holder. If used correctly, these databases enable to detect and to prevent identity fraud.

In The Netherlands, too, the privacy discussion is fighting the biometric passport system's underlying municipal databases and is threatening the safety of our large-scale biometric passport system by making these integrity and authenticity checks impossible. Thus, concerns about privacy could inadvertently hugely increase the social risks of large-scale biometrics applications. It must be made clear to those with serious concerns about privacy that the assessment criterion 'safety' implies the protection of privacy, but that this is not necessarily the case the other way round.

7 Ten principles of meaningful, safe and reliable use of biometrics [5]

1. Biometric person recognition alone is not conclusive. Biometrics is based on probability theory and therefore leads inherently to a number of wrong acceptances and wrong rejections (the precise number depends on the tolerance parameters configured by an operator). Moreover, biometric characteristics and biometric data derived from them can be imitated and counterfeited.

[5] The most recent integral text of the NBF position paper can be found on www.biometrieforum.nl

2. Biometrics can only recognise people, it cannot establish identities. Biometrics can link a person to a document or detail, but that says nothing about the integrity of that document or detail, or whether the link is itself accurate.

3. Safety assessments are indispensable to safe and reliable large-scale biometrics applications. Owing to uncontrollable organisational and human factors, a large-scale biometrics application can only be rendered safe and reliable with an enormous additional effort. In practice, it is still not possible to achieve that. Safety assessments must always relate to the biometrics application as a whole, including technology, organisation, procedures and the extent to which people cooperate or, conversely, have a vested interest in errors or misuse of the biometrics system or the biometric detail.

4. The principle of "*at least three matches*". Biometrics quickly gains reliability and safety if the biometric characteristic is used in combination with another biometric characteristic or detail and a non-biometric detail, such as a PIN code. In principle, the use of a *separate* (= *disconnected*) biometric detail which, with reasonable effort, can be linked to the person involved must therefore be discouraged.

5. It is important to actively discourage the trivial use of biometrics. The use of biometrics must be absolutely necessary for the envisaged purpose and not replaceable by other, less invasive or burdening measures.

6. A person subjected to a biometric verification has the right to be assured that a number of requirements have been met. The NBF operates a checklist of seven requirements that can be used as a test for the social acceptability of a biometrics application. [6]

7. It should be practically impossible to re-use biometric details in an application outside of it. Additionally, it must be possible to derive the originating application from the biometric detail itself.

8. The storage of biometric details should only be permitted if indispensable to that application in question. Biometric details should then be stored in distorted and encrypted form only.

9. It should only be permitted to link a file containing biometric details to external databases in situations provided for by law and on condition that there are no direct links to biographical details of the person involved.

---

[6] These rights are: the biometrics application is used only for its intended purpose, a simple and straightforward objections and complaints procedure, a fallback procedure proportionate to the risks involved, preventative measures against theft or misuse of biometric data, the operator's active support (compensation for damages and rehabilitation), disclosure as to who has had access to one's biometric details and explicit measures against a person who attempts to misuse or succeeds in misusing biometric details.

10. A mandatory register of large-scale use of biometrics. Large-scale biometrics applications should be registered, certified and monitored. The misuse of biometrically based identities should be reported to this register's manager who also has to guard against any unnecessary or non-secure storage of biometric details and to verify whether the operator of such a large-scale biometrics application has taken sufficient preventative measures against the theft and misuse of the biometric data he controls.

8 Concluding remarks

In this introductory stage of biometrics applications public acceptance and thrust are to be earned by the biometrics community. Two major aspects stand out: (1) our focus must be on avoiding teething troubles gaining experience with the use of biometric details at a smaller scale and (2) when biometrics applications are scaled up, more attention must be paid to assumptions and expectations that might not be valid at that level. Risk assessments must uncover the inherent security and safety problems and risk management must form an essential part of a biometrics application taking into account the extent to which people can be expected to co-operate or, conversely, have a vested interest in errors or misuse if they can get away with it. The NBF's position paper, therefore, highlights these aspects to stimulate social debate.

Bibliography

[Gr01] Grijpink, J.H.A.M., (2001). Biometrics and Privacy, in: *Computer Law and Security Report*, May/June 2001, vol. 17 (3) 2001, pp. 154-160. Oxford, UK: Elsevier Science Ltd

[Gr04a] Grijpink, J.H.A.M., (2004). Identity fraud as a challenge to the constitutional state, in: Computer Law and Security Report, vol. 20 (1) 2004, pp. 29-36. Oxford, UK: Elsevier Science Ltd

[Gr04b] Grijpink, J.H.A.M., (2004). Two barriers to realizing the benefits of biometrics: A chain perspective on biometrics, and identity fraud as biometrics' real challenge, in: Optical Security and Counterfeit Deterrence Techniques V, edited by Rudolf L. van Renesse, Proceedings of SPIE-IS&T Electronic Imaging, SPIE Vol. 5310, pp. 90-102

[Gr05] Grijpink, J.H.A.M., (2005). Our emerging information society: The challenge of large-scale information exchange in the constitutional state, in: *Computer Law and Security Report*, vol. 21 (4) 2005, pp. 328-337. Oxford, UK: Elsevier Science Ltd

[Gr06a] Grijpink, J.H.A.M., (2006). Criminal Records in the European Union: The challenge of large-scale information exchange, in: *European Journal of Crime, Criminal Law and Criminal Justice*, Volume 14 (2006) 1, pp. 1-19. Leiden: Brill Academic Publishers

[Gr06b] Grijpink, J.H.A.M., (2006). Identity fraud and biometrics: An assessment model for the use of biometrics, in: *Computer Law and Security Report*, vol. 22 (4) 2006, pp. 316-319. Oxford, UK: Elsevier Science Ltd

[Gr08] Grijpink, J.H.A.M., (2008). Biometrics and security: Trend report on biometrics: Some new insights, experiences and developments, in: *Computer Law and Security Report*, vol. 24 (3) 2008, pp. 261-264. Oxford, UK: Elsevier Science Ltd

[Gr10] Grijpink, J.H.A.M., (2010). Chain analysis for large-scale communication systems. *Journal of Chain-computerisation,* 1, 1-32