WOLFGANG SCHREIBER

Biometrics – Applications, Costs and Risks*

The term "biometrics" has different meanings. Its broader definition refers to statistical analyses of biological observations and phenomena. In the current political debate and for the purpose of this article, it has another: biometrics refers to particular – mainly, physical – characteristics that are unique to an individual.[1] At least two biometric characteristics have a considerable history in everyday identification: the facial image and the signature. Furthermore, fingerprints are also used for identification purposes.[2] The biometric characteristics most frequently used in current and near future identification applications are

* This article is based on research performed within work package 4 of the Challenge programme (The Changing Landscape of European Liberty and Security, http://www.libertysecurity.org) which is financed as an integrated project by the Sixth EU Framework Programme. For a more detailed report on the research of work package 4 on biometrics cf. Lock, Peter/Schreiber, Wolfgang: The Economic Dynamics of Biometric Control Technologies, *Working Paper, Challenge Work Package*, Nr. 4, 2007 (http://www.peter-lock.de/frame.php?datei=txt/biometric.html&menu=home&view=screen&lang=en).

1 Cf. Lodge, Juliet: *Trends in Biometrics*. Briefing Paper (http://www.libertysecurity.org/article1191.html), 2006, p. 9. Lodge's regional differentiation (USA vs. EU) in the understanding of the term "biometrics" does not seem valid to me. In Germany, the broader meaning is applied in science while the narrower understanding is common in the public debate on identification technologies.

2 In this case certain cultural differences can be noted. Whereas in societies with high illiteracy rates fingerprints are often used instead of signatures, in the EU the taking of fingerprints is strongly associated with suspects in criminal investigations.

fingerprints, (digitised) facial images (2D or 3D), and the iris. Others are signature, voice and hand configuration. This is an incomplete list. A special case is human DNA, which is often not referred to as a biometric even though it is a unique characteristic of an individual. Its main difference to other biometric data is that DNA not only allows for the identification of a certain individual but provides links between individuals as well.[3] Common recognition techniques require two things: an optical device (e.g. a scanner for a fingerprint or a camera for a facial image or the iris) and software that uses an algorithm to reduce a fingerprint, the iris or characteristic points of the face to a digital code. This code may then be compared to one or more other digital codes to identify an individual.

Applications of biometrics

As stated in the tile, this article consists of three main parts, the first of which is the applications of biometrics. The best known set of applications is directly connected to the state. This includes, for example, the use of biometric data in passports and national ID cards for EU citizens or the creation of a biometric database for those applying for a visa to an EU member state. Continual, close cooperation between states and private agencies offers a second set of uses for biometric applications. These include airports where the state's customs officers or border police work with the airport's private security personnel. The airlines and their personnel constitute a third partner in this example. Other "state near" applications may be in the field of social security (e.g. the inclusion of biometric data on health cards) or in other social or public services (e.g. local traffic).

In the private sector, the most important application is generally understood as being for banking and financial transactions.[4] Debit and credit card PIN numbers as well as passwords used for online banking will be replaced by biometric data. Moreover, the use of biometrics in information technology will more generally replace access passwords for

3 Relatives or members of the same ethnic group have a chance of closer matches in their DNA.

4 BITKOM: *Zukunft digitale Wirtschaft*. Berlin, 2007 (http://www.bitkom.org), p. 20.

access to computers or particular applications. Also, access to and within work places shall be managed by biometric applications.[5]

In countries with significant social stratification, biometrics will be used in privatised spaces. The extreme cases are so the called gated communities that we especially find in South America, South Africa, parts of the United States, or Russia. These gated communities are residential or commercial areas that are guarded by private security and lower class access is restricted to those who work in these communities.

Finally, biometric applications will eventually be used by private users or households. In addition to computer access, this includes access to houses, flats or cars. Traditional keys will be replaced by biometric tools, and even within a household, biometrics may regulate access to certain devices (e.g. restriction on television programs for minors in a household).

To summarise: Biometric applications are already being applied by governments or, at least, decisions to do so are being taken by governments and parliaments. This is especially true for the introduction of e-passports and the issuing of visas. The situation with regard to national ID cards is very different. Whereas the plans of the British government are quite extensive and have forced intensive discussions in recent months,[6] in France the plans for electronic ID cards were stopped and the inclusion of biometrics has been blocked completely by the refusal of the Commission on Information Technology and Liberties (CNIL) to provide its approval.[7]. All other aforementioned applications have not yet been realized on a large scale. As well as government agencies, some private enterprises manage secure relevant buildings or areas through the use of biometrics. Tests with credit cards and other applications are currently being conducted.[8]

---

5 Lehman Brothers: *Security Annual 2006*. 2007 (produced by Jeffrey T. Kessler, sold by Sandra Jones and Company), p. 115.

6 Schmitz, Patrice-Emmanuel/Huijgens, Ronald/Flammang, Marc: *Biometrics in Europe. Trend Report 2007*, 2007 (http://www.europeanbiometrics.info/images/resources/121_58_file.pdf), pp. 35–38

7 Schmitz et al, op. cit. (fn. 6), p. 30

8 The first real biometric credit card was introduced 2006 in Singapore (cf. Citigroup: *Annual Report 2006* (http://www.citigroup.com), pp. 4, 8f). For more general observations on "test markets" like Dubai or Singapore cf. Lock, Peter: *The Economic Dynamics of Biometric Controls or the Need to Consider a Plan B*, 2007.

Several reasons are used to justify the development of the above-mentioned applications:

1. The use of biometrics ensures identification. Fingerprints are unique and, therefore, can be related only to one human being
2. It is more difficult to forge biometrical data
3. Ensured identification makes forgery more difficult and, thereby, provides more security
4. Ensured identification and more difficult forgery will result in less fraud[9]
5. Airport passenger check-in will be less strenuous because the use and control of biometric data can save time[10]
6. Customers will be relieved because the use of biometric data for access to bank accounts, computer networks, etc. means that s/he will not be required to remember more or less difficult passwords and/or PIN codes

To a certain extent, these reasons are based on myths. The first myth is that of ensured identification. Like any other identification procedure, errors are common place. On the other hand, it is quite reasonable that biometric error rates will be lower than those for other procedures; this is especially true with regard to the facial image identification by a customs or police officer. The second myth is the difficulty level involved in forging biometric data.[11] Forgery's difficulty level is not a fixed or unchanging. Rather, there is a competition between forgeries and security's technological possibilities, innovations and countermeasures. Striving to forge is also a question of how much can be gained by forgery. Biometrics may provide more security against everyday crime and fraud, but it is questionable how exactly the introduction of biometric applications will – at least, in the long run – affect terrorism or organised crime.

(http://www.peter-lock.de/frame.php?datei=txt/turinrev.html&menu=home&view=screen&lang=en), pp. 6, 10.

9 Schmitz et al, op. cit (fn. 6), p. 12

10 Heintze, Dorothea: Wie bei James Bond. Fingerabdruck und Gesichtsscan: Im Geschäft mit der Biometrie liegen deutsche Anbieter weltweit vorn. *Die Zeit*, 09.03.2006 (http://images/zeit.de/text2006/11/Biometrie.html)

11 Schneier, Bruce: Master Card. *Bulletin of the Atomic Scientists*, March/April 2007. p. 55f

Costs of biometrics

After dealing with actual and probable applications, let me now turn to the second part of this article: the implementation costs of biometric applications.

First, we have to understand that it is practically impossible to obtain only the costs of biometric applications within larger security systems. For example, air traffic is one of the fastest growing businesses worldwide. Therefore, airports around the world are expanding and implementing the most up-to-date technology in their new facilities. In order to avoid the use of different security systems, older technologies in the existing parts of airports may be replaced.

If we look at the costs for e-passports within the European Union, we will find striking differences. The new British passport will cost 66 British pounds,[12] which is approximately 130 Euro. The new German passport will cost 59 Euros.[13] So, a Britain applying for a passport will have to pay twice the amount as a German. We can also compare the fees for passports before and after including biometric data. In the U.K. the difference is approximately 47 Euros whereas the difference in Germany is 36 Euros. If we take the German figures and assume that approximately two-thirds of the German population possess a passport (i.e. ca. 50 million), we can estimate an additional cost of 180 million Euros per year in Germany. Of course, the fees for the new passports reflect only part of the costs for the introduction of biometrics. Other costs – for example, for implementation of respective devices at airports – will be covered by airport fees that will ultimately result in slightly higher ticket prices.

Let's have a short look at the market for biometrics. Worldwide revenue for the biometric industry is actually around 1.5 billion USD.[14] Lobby groups predict annual growth rates of 30 per cent;[15] market analysts provide figures of 15–20 per cent. In Europe, the German market

12 Lodge, op. cit (fn. 1), fn. 7

13 Rötzer, Florian: *Was wird ein biometrischer Ausweis kosten?* 01.06.2005 (http://www.heise.de/tp/r4/artikel/20/20200/1.html)

14 Lehman Brothers, op. cit. (fn. 5), p. 116

15 IBG (International Biometric Group): Press Release. *Biometrics Market and Industry Report 2006–2010*, 2006 (http://www.biometricgroup.com/press_releases/pr_2006_BMIR_2010.html) and IBG (International Biometric Group): *Purchasing Information. Biometrics Market and Industry Report 2007–2012*, 2007 (http://www.biometricgroup.com/reports/public/market_report.html)

is leading with total revenues approximating 100 million Euros. To place this figure in a larger context: the contribution of biometrics to European GNPs is actually 0.002 per cent.[16] The biometric market is, therefore, quite small. Even under the assumption of the highest growth rates, this will also be true in the future.

When we look at the market structure, we find very dynamic developments on the suppliers' side. Five years ago most companies that specialised in biometrics were small in size and innovative; they were often founded by small groups of computer scientists. Additionally, the leading electronics and computer technology producers had small branches for biometric applications. Actually, a concentration in biometric development is currently taking place. Investment companies like L-1 Identity Solutions acquired many of the formerly small sized companies and have become the leading supplier for biometric implementations.[17] Larger companies sought co-operations with smaller ones, expanded their branches for biometrics or acquired smaller companies. Despite the tendency towards concentration, the biometric market is quite far from being monopolized by a few companies.[18] For example, in the latter half of 2006 about 12 contracts were signed between European states' agencies and providers of biometric technologies. Only two providers were able to obtain more than one contract.[19]

However, demand is still dominated by states and state agencies. The realisation of various states' biometric agendas is the driving force for the recent and ongoing developments by biometric suppliers. To quote one of the leading investment reports: "the first real U.S. and foreign government orders for biometric systems are critical not just for making the biometric providers (eventually) profitable, but for creating the reference sites and beta tests that will be required for the holy grail of biometrics to become reality: major adoption by commercial users."[20]

16 BITKOM, op. cit. (fn. 4), p. 22
17 Lock/Schreiber, op. cit. (fn. *), Appendix I
18 Especially, there is little evidence for the assumption (e.g. Hayes, Ben: *Arming Big Brother. The EU's Security Research Programme.* Amsterdam, 2006) that a security-industrial-complex is in the making. For a detailed discussion of the differences to the military-industrial-complex cf. Lock/Schreiber, op. cit (fn. *), pp. 19–30.
19 Schmitz et al, op. cit. (fn. 6), pp. 28–38
20 Lehman Brothers, op. cit. (fn. 5), p. 11f

Therefore, governments still play a crucial role in the market for and the implementation of other biometric applications.[21]

Risks of biometrics

The last section will deal with risks connected to the implementation of biometrics. There are at least three dimensions to the problems concerning the use of biometrics. The first one is the technological dimension. Like every identification procedure or system, biometrics are not foolproof; technically speaking, on the one hand, there are False Acceptance Rates (FAR) and False Rejection Rates (FRR) on the other. But error rates are not a serious argument against the use of biometric technologies. High error rates cited in the literature criticising biometric applications are often one or two years old, refer only to certain systems tested and, therefore, often do not reflect the actual state of technology.[22] Furthermore, the combined use of two or more biometrical characteristics reduces error rates significantly. Of course, there cannot be a system without errors, but the alternative to biometrics is identification by human beings, i.e. by police or customs officers based on a passport picture or pictures of certain suspects. It seems reasonable that here the rates of error would be much higher.[23] On the other hand, the belief in the infallibility of a biometric identification system represents a serious risk.[24]

A more technical problem is the question of storage. How and where should data be stored? From the point of view of data protection, the storage of biometric characteristics on a chip – and only on a chip – is preferable. Storage of pertinent characteristics in databases is susceptible and open for manipulation, misuse and illegal access.[25] But the decision

21 For Germany cf. BITKOM, op. cit. (fn. 4), p. 26

22 BSI (Bundesamt für Sicherheit in der Informationstechnik): *Untersuchung der Leistungsfähigkeit von biometrischen Identifikationssystemen – BioP II. Öffentlicher Abschlussbericht*, 2005 (http://www.bsi.de/literat/studien/biop/biopabschluss2.pdf); Deutscher Bundestag: Sicherheit der biometriegestützten Reisepässe. Antwort der Bundesregierung auf eine Kleine Anfrage, Drucksache 16/161, 09.12.2005, p. 3

23 In addition, some people may "appear" more suspicious in the traditional identification procedure by human beings because of their skin colour, their hair style or their type of clothing.

24 Schaar, Peter (ed.): *Biometrie und Datenschutz – Der vermessene Mensch*. Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 27. Juni 2006 in Berlin, Bonn 2006, p. 8

25 e.g. Schneier, op. cit. (fn. 11), p. 56)

to store the biometric data necessary for passports only on a chip does not exclude its storage in databases as well. Any use of a chip containing biometric data includes the risk that this data will be copied and stored in a database. This may be the case if current legislation changes so that storage in databases will be allowed in future. Furthermore, passports are mainly for use in foreign countries. The legislation of such a country may already allow copying[26] or may even require the storage of biometric information in a database.[27]

Another technological problem may be the use of biometric data for different types of identification. Nowadays, if someone has knowledge of one of my credit card's PIN codes, this person can only misuse this particular card. But what happens when every identification process occurs via the same tool, e.g. a fingerprint? If someone is able to forge this piece of information, he may gain access to additional debit or credit cards. And what happens if access to someone's house or car is managed solely by his fingerprint? Today, he can receive a new key or PIN code. Of course, he cannot receive a new fingerprint.[28]

A second problematic aspect of using biometric data is that of inclusion or exclusion. To a certain extent, biometric data can only replace existing systems. On the other hand, every IT system allows it to handle more data and, therefore, especially expand the number of excluded persons. A very actual example of inclusion or exclusion is related to international regulations. States which meet the requirements of the US government with regard to their passports and the information contained in them are included in the US visa waiver scheme. On the other hand, all other states – and, of course, their citizens – are excluded from it. A similar problem may be observed on the level of the individual. Within so called frequent flier programs, persons may be registered after they underwent a security check. Participating in the scheme will allow a faster check-in, with fewer security checks, for those registered for each flight.[29] Identification will be achieved through the use of biometrics applications, of course. The questions of inclusion and exclusion are quite obvious in this scheme.

26 Deutscher Bundestag, op. cit. (fn. 22), p. 2
27 In this regard the EU is a striking example with the storage of biometric data of all visa applicants.
28 Heintze, op. cit. (fn. 10)
29 Schmitz et at, op. cit. (fn. 6), p. 8

But frequent flier programs still include another dimension: one of trust and distrust. A "frequent flier" who has undergone the required security check seems to be a trustworthy person. But what about those people, who are "frequent fliers" by the fact that they often fly but are not – or don't want to be – registered within a frequent flier program? And furthermore, what about those who fail the security check?

Another aspect of trust/distrust – and the last point in this paper – is the existing and even growing distrust of a segment of society vis a vis security policies.[30] To illustrate, I will refer to a current discussion in Germany.[31] Politicians have seemed to be entirely concerned with questions of security for quite some time. They do not, however, seem to be concerned in questions of civil liberties. At least since September 11, 2001, new demands for security enhancement measures are continuously being posed. Examples in recent years include the desire to permit the downing of kidnapped planes[32] or extensive security checks for all personnel working within the 2006 FIFA World Cup stadiums. Just recently the Federal Minister of the Interior demanded a list of security measures deemed necessary by him.[33] These included:

- police agencies' access to databases of local authorities, e.g. where data collected for the issuing of passports are stored, especially digitised passport pictures
- extending the amount of time providers of phone or internet connections must store data
- online search of personal computers by police agencies (of course, without knowledge of the computer owners)

30 And of course the distrust of the respective politicians vis a vis parts of their societies

31 For more general discussions with reference especially to British and French examples cf. Lodge, Juliet: Communicating (in)Security: A Failure of Public Diplomacy, *Challenge Research Paper*, Nr.3, 2006 and CCNE (Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé): *Biométrie, données identifiantes et droits de l'homme*, 2007 (http://www.libertysecurity.org/IMG/pdf_avis098fr.pdf).

32 A respective law was, according to a judgement of the Bundesverfassungsgericht (Federal Constitutional Court), not in line with the German constitution.

33 One reason for this preoccupation with security measures might be the state's loss of control caused by globalisation and transnationalisation (cf. Ceyhan, Ayse: Technologie et sécurité: une gouvernance libérale dans une contexte d'incertitudes. *Cultures & Conflicts*, 64 (2006), pp. 11–32).

- use of military personnel and devices to assist police or to take over police duties, especially pertaining to guarding relevant security sites
- storage of the fingerprint data collected for the issuing of passports in local authorities' databases

To conclude, as indicated during the actual discussion on security policies in Germany: Biometric applications are only a minor concern at the moment.[34] Most observers agree that the Federal Minister of the Interior put the storage of fingerprints in databases on his agenda only for bargaining purposes. The opposition in parliament deals with biometrics mainly in technical terms and presses for more data protection, but it articulates no general objection against the use of biometric data for identification purposes. Even in the current yearbook on the state of fundamental rights in Germany,[35] none of the more than 40 articles deals with biometrics.[36]

34 This is especially the case for non-state applications of biometrics. Peter Lock (op. cit. (fn. 8), p. 3) stresses the necessity to pay more attention to private sector activities (cf. also CCNE, op. cit. (fn. 31), p. 8f).

35 T. Müller-Heidelberg et al (eds.): *Grundrechte-Report 2007. Zur Lage der Bürger- und Menschenrechte in Deutschland*. Frankfurt am Main, 2007.

36 Interestingly, the front cover of the book shows the biometric identification by an iris scan. Therefore, it may be concluded that for the authors of the yearbook as well as for the concerned German public biometric identification seems to be one of the strongest symbols of a policy of securitization and a risk for civil liberties.