Thomas Petermann
Arnold Sauter

February 2002

Biometric identification systems

Summary

TAB Working report no. 76

TAB
Office of Technology Assessment
at the German Bundestag

SUMMARY

The task of TAB was to carry out a »preparatory study« to obtain an initial screening of the field of biometric techniques and systems and attempt to establish the current status and make a provisional assessment of R&D activities, the evolution of the market and present and future applications (and their potential). Legal considerations – and specifically data protection and consumer policy considerations – make an initial assessment of biometric techniques and systems desirable.

FEATURES, TECHNIQUES AND SYSTEMS

»Biometrics« covers the recording and measurement of living beings and their characteristics. In the present context biometrics refers to the (automated) measurement of an individual (physiological or behavioural) feature of an individual for the purpose of (biometric) identification and hence differentiation from other individuals.

For »optimal biometric use«, human characteristics – whether physiological (passive) or behavioural (active) – have to be universal, unique, constant and (technically) recordable. From the practical viewpoint, the biometric techniques and systems working with these characteristics must be rapid, compatible with existing security elements, robust, accurate, safe, economic and reliable. None of the biometric characteristics currently used or available systems fully satisfies all requirements. Even so, there are numerous systems in operation worldwide in various application contexts, e.g. to check authorisation of individuals in e-banking and e-commerce transactions, or for access controls for sensitive areas (section IV.1). Most frequently used are identification of fingerprint, hand geometry, face, voice, iris/retina and signature/handwriting, the physiological, technical, economic and user aspects of which are described in section II.2.

Conventional systems cannot check passwords or PIN chip cards to see if the user providing correct data is also the lawful owner. As biometric techniques work with person-linked characteristics (which can neither be lost nor forgotten, and are not easy to steal), they promise a new dimension in quality, comfort and security in personal authentication.

Efficiency of biometric techniques

The efficiency of available biometric systems cannot be reliably assessed on the basis of what is often extremely contradictory information (section II.3). The blurring of the boundaries between potential and current actual capacity is one source of confusion. Despite the improvements achieved and the certainty that there will be further technological advances, reports of high standards already obtained in accuracy and reliability in biometric systems must still be approached with scepticism.

At national and international level a number of committees are working on defining criteria for the future evaluation of biometric systems, and existing techniques (which are often more prototypes) are being subjected to comparative practical testing in various pilot projects (section III.1). However, there is as yet no generally recognised method for comparing the strengths and weaknesses of the various biometric systems. In addition, the varying level of maturity of the different biometric systems makes comparative evaluation difficult. Such an evaluation would have to include logical and informative data on for example reliability, accuracy, sensitivity, acceptance, robustness, compatibility, simplicity and costs. An exact assessment of the strengths and weaknesses of a technique can only be made in a specific application context, and must be empirically designed with logical individual steps.

This is particularly the case if the biometric system involved is a far-reaching one, covering large user groups (voluntary or compulsory), e.g. within the framework of equipment for identity cards, where the highest standards are required of a well-founded evaluation of the potential systems. Regular reporting on the status of current pilot projects and (international) standardisation efforts would certainly be useful as a basis for further political treatment of the complex issues in general.

R&D ACTIVITIES

The status of research and development in the field of biometric systems could be rather more comprehensively surveyed in Germany, and the same applies for the promotional activities of the EU, although the picture at international level is exemplary. In North America and Asia there is a plethora of activities in the private and public sectors.

Particularly interesting are the pilot projects in evaluating biometric systems, which are studying both technical issues and consumer and data protection aspects. In Germany this applied or applies specifically to the BioTrust project, promoted among others by the Federal Ministry of Economics, and the BioIS project promoted by the Bundesamt für Sicherheit in der Informationstechnik (BSI – Federal Office of Security in Information Technology) (section III.1).

After a long period during which research into biometrics has been pursued in a number of Fraunhofer Institutes in particular, Federal promotional activities have been intensified overall in the last two years. Industrial activities in connection with biometric applications have also gained momentum in Germany, with increasing use of the possibilities of cooperation within EU projects. The Telekom subsidiary T-Systems Nova launched its own pilot project in 1999, and ekey biometric systems launched one in Austria in 2001. Of the European nations, the UK is regarded as particularly involved in public and private R&D. Under its current IST programme, the EU is promoting seven major projects on biometrics to the value of over €10 million (section III.2).

APPLICATIONS OF BIOMETRIC TECHNIQUES

There is a large and steadily growing number of reports on concrete use in numerous areas, particularly from the USA, but also from European and Asian countries. Until a few years ago, the use of biometric identification systems was almost exclusively limited to security needs, but gradually other areas of application have been opened up in companies and government agencies. The current and foreseeable areas of application can be broken down into five groups (section IV.1).

> user access control
> personal identification
> equipment access control
> electronic access to services (e-banking, e-commerce)
> other »convenience areas«.

Market assessment

The available economic data and estimates on the use of biometric systems often have a very limited and random appearance (section IV.2). Generally, they lack transparency, but in any case they do not give a complete picture. It is, however,

difficult methodologically to define, identify and quantify the actual »biometric« portion of an overall technology. Official statistics also fail to provide any basis for obtaining relevant figures on biometric products and services (scale of production, sales, employment etc). The companies involved also tend to follow a restrictive information policy. The status of diffusion, sales and market shares (national and international) accordingly remains extremely uncertain.

We can, however, say that there has been a rising trend in sales in the last few years, with the USA as the dominant market (accounting for c. two-thirds of sales), followed by Europe, Asia and Latin America. As so often, Asia is seen as an important future market, but growing demand is also expected in Europe. The technology which appears to be dominant in both turnover and the number of suppliers and systems is the fingerprint technique, although face recognition in particular is seen as having growing potential. The assumption is that there will be consolidation in the market as soon as individual systems and suppliers achieve significant market shares.

More accurate data would be needed for possible more specific promotion in biometrics. However, a prerequisite for this would be developing concepts and methods for improved collection of relevant economic statistics, broken down by actual biometric systems, peripherals and the nature and scope of application.

Consumer protection

World-wide R&D activities and the increasingly evident expanse of areas of use indicate the possibility that biometric techniques will soon become widespread in everyday commercial life. For this reason, questions of consumer protection, the legal framework and (in particular) data protection are becoming increasingly important.

If we want to make use of the possibilities of biometrics and control its risks, the design and application of biometric systems must satisfy certain criteria. This includes particularly a high level of security, comprehensive trustworthiness, adequate user friendliness and extensive social acceptability (section V. 1).

Security and trustworthiness

If biometric techniques are to make a contribution to the security of electronic applications, they themselves must meet high security standards. To ensure this, the various biometric techniques should be evaluated on the basis of their features, potential risk and area of application, and subjected to a comprehensive

risk analysis before widespread marketing. However, we are still far from developing consistent concepts of security for individual application scenarios which take into account consumer and data protection needs.

To achieve maximum possible trustworthiness it has, for example, been suggested that confidence commissions should be set up with the necessary technical expertise, independence and neutrality to review and guarantee a level of security agreed in collaboration between users, manufacturers, operators and the state.

A prerequisite for the review and corresponding certification of biometric system is the development of reliable criteria for evaluation which can be used for objective comparison of different techniques. The (world-wide) efforts on this are not yet complete. Generally acknowledged criteria would give users a guideline for selecting secure products while at the same time providing a compass for developing secure and trustworthy systems. For such evaluation criteria to gain widespread acceptance, they need to be developed by bodies which are independent of suppliers and include the developers.

User friendliness and social acceptability

Adequate user friendliness of biometric techniques requires that these be robust and suitable for everyday use, i.e. that they function reliably over long periods in large-scale use. At present, this is frequently not the case. For social acceptability, biometric techniques will have to demonstrate that their widespread use does not widen the »digital divide« in society, and also that no »mandatory biometrics« emerges. In terms of consumer policy, it is accordingly necessary to take measures to ensure that no user is excluded by biometric applications, e.g. it would be necessary to provide alternative (biometric and conventional) techniques.

Relevant statutory provisions

Until recently, regulations in Germany dealing explicitly with the use of biometric techniques existed only with respect to the use of electronic signatures (section V.2). In May 2001 a new Signature Act (SigG) entered into force, and in July 2001 this was followed by the »Form Act« which recognised a »qualified electronic signature« as having the same validity as a handwritten signature.

While the Signature Act is deliberately formulated in a technologically neutral way, the Regulation on the Act (SigV) explicitly permits the use of biometric techniques: with respect to securing the signature key, the owner of the signa-

ture key has the option of identifying her/himself before using the key either in conventional ways through »possession and knowledge« (e.g. card and security number) or through »possession and one or more biometric features«. The Regulation supplements this with a specific level of security: in using a biometric technique there must be »adequate security that unauthorised use of the signature key is excluded and the equivalent level of security to the knowledge-based technique is provided« (section 15, para. 1 SigV).

From the point of view of consumer protection, this comparative reference to techniques based on the »possession and knowledge« principle has been subject to criticism for some time. This focuses particularly on the fact that the security of such techniques is widely disputed today.

The Regulation cited above means that Germany has a statutory framework for the use of biometric techniques in connection with electronic signatures and electronic legal and commercial transactions. In the process, the law explicitly opens up a field of application to biometrics which will probably become increasingly important in future. It remains to be seen in practice if this statutory framework is sufficient and suitable, or whether it needs to be developed further.

DATA PROTECTION

To the extent that biometric techniques rely on personal physical characteristics, questions of data protection arise (section V.3).

The most important legal basis for evaluating biometric techniques from the point of view of data protection is the newly-amended Federal Data Protection Act (BDSG). The purpose of this act is »to protect individuals from having their privacy violated through use of their person-related data« (section 1 para. 1 BDSG). In connection with data in biometric techniques, section 3 para. 9 BDSG is particularly interesting, as this cites »particular kinds of person-related data« and gives these increased protection. This includes »information on racial and ethnic origin, political opinions, religious or philosophical conviction, trade union membership, health or sexual activities«. Certain data in biometric techniques may use information which comes under this particular protective heading.

To the extent that person-related data is generated with the help of biometric techniques, these techniques are subject to data protection regulations generally.

This applies to both the public and private sectors. For the public sector, additional special regulations are needed for the specific areas.

Constitutional relevance of biometrics

IT using biometric techniques impacts a specific aspect of general privacy law – the right to self-determination where information is concerned. This impact is covered by data protection legislation. Human dignity can also be affected as an outstanding protected characteristic.

The constitutional right to self-determination where information is concerned guarantees the right of the individual to decide for themselves about release and use of their personal data. At the same time, limited state incursions into this right are permissible. However, state-imposed use of biometric techniques impacts more than just on these special protective areas. Because this uses physical and behavioural characteristics as a source of information, it is likely that a further aspect of the general right to privacy is at least affected. The limits to a violation of human dignity would be reached or crossed if the state required far-reaching recording and processing of biometric characteristics, creating the possibility of »registration« and »cataloguing the individual«.

If we share the view that the impact of biometric techniques can under certain circumstances go beyond the right to self determination where information is concerned to a further aspect of the general right to privacy, this implies that existing statutory permission to process data is not sufficient to cover this dual incursion. The result is that implementing biometric components in state procedures requires a separate decision by the legislature legitimising both aspects of the incursion – the specific biometric one and the incursion into the right of self determination where information is concerned.

System data protection

If and how far a specific practice in using biometric techniques satisfies the requirements of data protection legislation depends fundamentally on the intensity of the impact. Here, the Data Protection Act contains provisions which can serve as a guideline for techniques which minimise their impact:

> In principle, data must be openly collected, directly from the party involved, with their cooperation and informing them among others of the purpose of the collection, processing or use (section 4, paras 2, 3 BDSG). From this point of view, techniques requiring a high degree of cooperation to capture the raw data

are preferable to those which involve the subject less or even operate unnoticed.
> Under the heading »Data omission and data parsimony« attention must be paid at the stage of selecting and designing an IT system to ensuring that no or as little as possible person-related data is collected, processed and used (section 3a BDSG).
> Efforts must also be made for the purpose of data protection to use the possibility of anonymising and pseudonymising (section 3a BDSG).

Active cooperation by those affected, parsimonious collection and use of data and technology-related high security in avoiding personal reference: these are the important components of system data protection as a (material) basis for effective data protection. Template-free techniques can make a decisive contribution towards this. These enable anonymisation and pseudonymisation of data, and ensure that the possibility of relating data to individuals is practically ruled out. Another contribution is decentralised storage of data, either in autonomous units or on a chip card which is in the personal control of those affected.

Recent legal developments

In the course of the intensive debate on measures to improve security since 11 September 2001, the use of biometric techniques was also explored. The legislature has taken action on this (section V.4). Passport and personal identity card law in particular was expanded by the recently passed »anti-terrorism act« (»Act to combat international terrorism«), which creates the possibility of computerised identification of individuals using biometric data in identification documents. A future Federal law will cover the »types of biometric characteristics, their details and the incorporation of characteristics and information in encrypted form […] and the nature of their storage, other processing and use«.

The Aliens Act also creates the possibility of using biometric characteristics on the above lines. Details are determined by the Federal Ministry of the Interior in a statutory instrument which is subject to approval by the Bundesrat (Higher House).

The »anti-terrorism act« establishes a parliamentary basis which clearly defines (for the citizen as well) the conditions, purpose and scope of the incursion into the right to self determination where information is concerned:

> The biometric characteristics to be used are explicitly specified as alternatives.
> The purpose of the stored data is explicitly determined.

> The introduction of identification papers using biometric characteristics for German citizens requires special legislation. The situation is different for identification papers for aliens, where a statutory instrument is the basis.

The concerns of the BDSG were met primarily by the fact that the passport or identity card holder must on demand be told the content of the (encrypted) data by the responsible agency. It is also explicitly provided that no »nationwide file« may be set up.

PROSPECTS FOR FUTURE DEVELOPMENT

Biometric systems and techniques are probably in a decisive phase of diffusion world-wide. There are numerous indications suggesting expansion into further public and private areas of application. The technological progress is unmistakable: the technical functionality of individual systems is increasingly maturing, showing improved capability. The trend in prices for many systems should encourage further diffusion. Individual basic components, such as sensors and chips, are increasingly available at good prices, and increased production will make possible further price cuts. On the supply side there has been a qualitative improvement, so that demand can be better stimulated and satisfied.

Prevailing legislation (specifically the Signature Act and Signature Regulation) is opening up a vast market for biometrics in electronic legal and commercial transactions. The »anti-terrorism act« has further opened the door to the market for security technologies. If state procedures in Germany (and Europe generally) initiate mass use of biometric systems, this would probably give the green light to other applications in business and the private sector. Consumer associations and data protection officials have always viewed biometrics critically, but also with favour. The potential of biometrics as a technology thoroughly compatible with consumer and data protection is emphasised – although combined with the call to developers and users to adopt technical and organisational solutions which meet the criteria of advanced consumer and data protection.

NEED FOR RESEARCH AND ACTION

In view of the likely increase in importance of biometric systems in commerce and society, there is substantial need for research, information, discussion and education. This need is summarised in section VI.

Improving the state of information appears particularly urgent in view of the pace of development. For further understanding of the future development of biometric systems, a comprehensive TA could, for example, be carried out. This would require a systematic and forward-looking analysis and assessment of the societal, economic and legal conditions and consequences of further growth in diffusion of biometric techniques, covering a horizon up to 2010. The analysis should also identify the need for political guidance. It would also be possible to integrate a moderated expert discourse, whose thrust and tasks are outlined in section VI.

The Office of Technology Assessment at the German Bundestag is an independent scientific institution created with the objective of advising the German Bundestag and its committees on matters relating to research and technology. Since 1990 TAB has been operated by the Institute for Technology Assessment and Systems Analysis (ITAS) of the Karlsruhe Institute for Technology (KIT), based on a contract with the German Bundestag

Office of Technology Assessment
at the German Bundestag

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Str. 10 · 10178 Berlin
Telefon: 0 30 / 28 49 10
Telefax: 0 30 / 28 49 11 19
e-mail: buero@tab.fzk.de
Internet: www.tab.fzk.de