

2006-11-10

# The Biometric Society - Risks and Opportunities

Manfred U. A. Bromba

*Biometrics consultant, Bromba GmbH - Germany*

**Abstract.** The Biometric Society is defined here as a fictive future trend of the Information Society in which our daily life is dominated by biometric identification using a central data base. This has a lot of benefits for the users but at the same time enables a nearly total surveillance. Already today one can observe permanently advancing surveillance using data which are a by-product of state-of-the-art technologies and services. This kind of surveillance is claimed to be effectively usable as a measure against terrorism, although it is also suspected to favor democide. Possibly, since there is no proven stringency that total surveillance is incompatible with democracy, there is little resistance against the small steps towards it. This paper also treats technical feasibility of the Biometric Society. However, the question, whether the Biometric Society will ever become reality or even when this will happen, was not in the scope of the present investigation.

**Keywords.** Biometrics, identification, unique identifier, privacy, security, Information Society, total surveillance, democracy, fake detection

## **Preface: The Information Society**

Never before was it so easy to gather, to distribute, to collect, and to process information of all kind. This became possible as a result of the advances in technology, sensor technology, copy technology, storage technology, communication technology, computer technology, and applied mathematics.

Since all these advances will drastically change our life, the term "Information Society" has been created [1]. The impact of the Information Society on legal framework and privacy will be enormous. But many of us do not really perceive this because the change is a creeping process which often uses outstanding occurrences as justification. We are amid this process which yields a degeneration of liberal values, establishing as information surveillance, data retention, and censorship, while taking back banking secret and other rights. The question "Is this really a degeneration or is it a necessity for our survival?" disunites many people - and will not be answered in this paper. But I will take this opportunity to raise some fundamental questions by drawing an example of a future society which I have called "The Biometric Society".

The fictitious Biometric Society will be an occurrence of the Information Society. It is specifically based on progress in sensor technology, computer technology, and applied mathematics and cannot exist without the Information Society.

This publication is a combination of two presentations on the Biometric Society I held at the 5th meeting of the Biometric Identification Technology Ethics group in

Wroclav (Poland) which was dedicated to the topic "Future Technologies" [2] and the NATO Advanced Research Workshop on identity, security, and democracy in Jerusalem (Israel) [3].

## **Contents**

This contribution will be divided into three parts and considers the benefits, the risks, and the feasibility of the Biometric Society. The first part defines the Biometric Society and praises its advantages. The second part is something more nebulous and tries to examine the worst case risk of the Biometric Society. All these considerations remain useless unless there is a chance of realizability. For this question I will try to find an answer in the third part.

But before we start into the consideration of the Biometric Society, certain basics concerning biometrics and security are treated. For the fundamentals of biometrics the reader is referred to other sources [4, 5].

## **Biometrics as a unique identifier**

Biometric identification has become popular because it offers the chance to deliver a unique identifier for each person. While certain identity numbers are supposed to fulfill the requirement of uniqueness perfectly, biometric features are far from being perfect in this respect. The reasons are, e.g., non-perfect technology and fundamental natural limitations which greatly depend on the type of feature.

Today, it is possible for one fingerprint to separate more than 1 Million people while facial geometry as feature has its limit for less than 1 000 people. As a consequence and in contrast to fears of many data protection commissioners, surveillance systems with face recognition are (and possibly will ever stay to be) poor candidates for Big Brother scenarios! On the other hand, using more than one finger possibly allows separating the whole mankind.

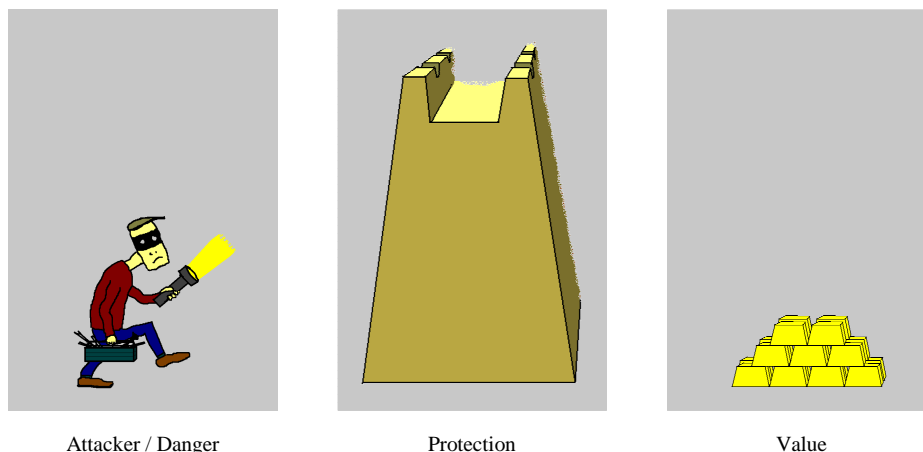
Unfortunately, it is just the property of uniqueness of an identifier which is also susceptible to misuse. For that reason, the Federal Constitutional Court of Germany has forbidden to use personal identifiers for the registration of all German citizens in 1983.

## **Security model**

Since security often is not really understood by those who like to use this term, security is defined here in a technical way. The use in more general concepts such as politics is straight forward.

Security generally is loosely defined as absence of risk or danger to a value. To understand what security really is, a simple three-part model may help which comprises

- a value to be protected against a danger,
- a protection to avoid damage to the value,
- and the danger.



Attacker / Danger

Protection

Value

**Figure 1.** Security Model (© Bromba GmbH)

For example, the value may be jewels, the protection a safe, and the danger a burglar who tries to steal the jewels. The same model works when human life is threatened by an attacker. In this scenery we have a lot of appropriate protection means: police, surveillance, flight passenger checks, etc. The type of protection varies with changing values. For example, if not a single person is threatened but a whole nation, the police is to be replaced by a defense army.

### *Security definition*

Security may be understood as the probability for a value not to suffer a damage or loss. Security is not a digital entity. In fact, it is quite reasonable to define security as a number which may vary between 0 and 100 %. This is achieved when defining security as the "inverse" of risk according to the relationship:

$$\text{Security} = 1 - \text{Risk}$$

Risk is technically defined as the product of two probabilities: the incidence rate for the damage and the extent of loss. As a result, security may be regarded as a probability, too. To quantify a probability practically, this cannot be done on the basis of a single event. Rather, a sufficiently large quantity of incidents is needed!

### *How much security do we require?*

For 100% security, it is sufficient that there is either no danger or a perfect protection. No danger at all means "not from this world" and a perfect protection can only be realized with indefinitely much money. So the question arises, how much security would be sufficient and how security can be quantified at least theoretically!

There are many possibilities to cope with the problem. Here we try the simplified approach that a value needs as much security that its mean natural lifetime is not significantly reduced by artificial damages.

For a human being the lifetime is about 100 years. If we assume a rectangular distribution (this is the most simple but surely not the most realistic approach), the mean

natural risk to die (which is a kind of inevitable damage) is 1 % per year. I think it makes sense to protect our life against artificial damages in such a way that the natural rate does not increase by more than, say, 1 %. That is, the artificial part of the yearly death rate should be smaller than 1% of 1%, i.e., 1:10 000, increasing the natural death rate from 1% to 1.01%!

#### *Examples for required security*

Is this a reasonable figure? Indeed, in Germany, the artificial yearly death rate without disease is about 4:10 000, where the probabilities for a deadly traffic accident, a suicide, or a deadly fall is about 1:10 000 each. This is accepted reality!

If we change from an individual to a nation as value to be protected, mainly the natural lifetime is different. If I suppose 10 000 years as lifetime of a nation, in contrast to 100 years for an individual, and again assume that the artificial risks should at least be a factor of 100 below the natural one, the *required security* raises from 0.9999 to 0.999999 per year! Maybe, this is an explanation - not a justification - for the fact that individuals seem to be the big losers in a war between nations!

#### *Security and colloquial language*

As a consequence of our security definition, there is a fundamental difference between security and protection. This is often confused in colloquial language and even by security specialists. For example, how do we have to translate a politician, who says that security must be increased by introducing more surveillance as a result of increasing danger by terrorism? Not the security has to be increased, it is the protection which must be improved, namely to keep security constant!

But the politician should not forget that he has it in his hands not only to improve protection. This can be very expensive. He may also manage that the probability of attacks is not increased by performing a dangerous politics which creates additional enemies and this way increases the threat potential.

If you are looking for examples, you may be tempted to consider the latest shocking terrorist attacks in Spain (2004) and UK (2005). But do not forget that security is a statistical phenomenon which never should be assessed on the basis of only a few events!

## **1. The Biometric Society and its benefits**

### *1.1. The Biometric Society – how does it work?*

In the Biometric Society, all actions and transactions are authorized by using biometric identification. As a result,

- no token nor any other credential is necessary,
- you cannot forget anything, and
- your identity can neither be stolen nor lost.

As a special requirement, all services shall be available worldwide.

The Biometric Society is not the only solution which fits to this description. Alternative systems using implanted ID chips will mainly do the same and deliver almost the same benefits.

In the following, the beneficial impacts on our life will be shown, regarding payment transactions, traveling by car, health care, communication, computing, entertainment, and law enforcement as important examples.

### *1.2. Payment transactions*

Cards such as credit cards, payment cards, and rebate cards as well as cash are completely replaced by biometric identification which is performed online and in real-time. Obtaining services by fraud is made impossible because always a unique biometric recognition together with a creditworthiness inquiry is performed before granting the service. As a result, neither tickets for bus, train, or flights, nor tickets for football games, concerts, and gyms are needed any more.

### *1.3. Traveling*

Before a driver starts the car, a biometric check proves the permission to drive under consideration of the car ID number. This can be achieved using wireless communication. This way, driving without permission, with stolen cars, or without sufficient creditworthiness is prevented from the very beginning. Only those types of cars can be driven for which an education has been performed. The personal assignment of the universal street toll is managed automatically on the basis of the driver and car data.

### *1.4. Health care*

Medical services are balanced biometrically without expensive and losable health cards. After biometric identification, the patient may inspect his health records everywhere and anytime. In the case of accidents, the rescue workers are able to inform about health data, blood type, immunizations, and allergies immediately. This is achieved with the aid of a mobile biometric identification on location and guarantees an optimum medical treatment. In the case of fatality, the large expense of a manual identification is replaced by checking the biometric features.

### *1.5. Communication*

Communication has grown to a basic requirement of our life. Especially internet and mobile communication have become indispensable. In the Biometric Society, emails and phone calls are exclusively processed using biometric identification. This makes the user independent on any hardware. Nevertheless, stolen hardware can be identified by a unique device ID! For addressing, only the data set of the biometric feature of the receiver is to be used. Names are not really necessary - they are merely needed for certain kind of direct inter-human communication. Certainly, also every sender has to identify biometrically. This way, spamming and phishing is effectively prevented.

### *1.6. Computing*

Secure computing will become self-evident, to avoid the infection of computers with viruses, Trojan horses, and other malicious software and to solve the problems of the entertainment industry with respect to unwanted use of their products. Biometrics ensures that only authorized persons are able to operate a computer and that all software can only be used with personal authorization.

Biometrics even allows for new license models. For example, if a certain person has licensed a software package, this person is allowed to use this software anywhere on any running system. Since only authorized persons are allowed to use it, a software may be copied and installed arbitrarily often without any loss to the software developer.

Secure data access can be achieved in a similar way as all data is personalized using biometric identification. Personal Information Rights Management (PIRM) is used to prevent content piracy and to retain authors' rights.

### *1.7. Entertainment*

Any kind of entertainment is authorized by biometrics. This has a lot of advantages. For example, since birth date is stored centrally, age verification is easily achieved.

Services like pay per view are managed by ordering a film using biometric identification. Like in computing, each data access is personalized while the data are free, may be copied as often as one wants, but remain inaccessible for the unauthorized. As a result, audio and video downloads need not necessarily be authorized by biometrics. Peer to peer (P2P) file sharing services are no problem for the content owners any more.

But how can I prevent unauthorized viewing and listening? Today, any transmission channel is secured using encryption techniques. Even the cable between receiver and monitor will be protected using HDMI (High Definition Multimedia Interface) [6]. However, this method does not prevent copying from screen, using an ordinary camera. So, several companies even think about disturbing the display output in such a way that the camera record becomes unusable.

Maybe, the problem will solve quite naturally if 3D TV becomes more popular and uses goggles. This way viewing video will be personalized. If the method becomes common enough, it will be combined with biometric identification to prevent unauthorized use of the 3D video (and audio) data. Here, iris recognition is the preferred biometric feature which naturally integrates into the goggles.

### *1.8. Law enforcement*

Cosmopolitans, who move outside the settled society standards, can effectively be sanctioned with restrictions of certain rights. Examples are prohibitions for shoplifters to enter a certain store, for hooligans to enter a football stadium, or refusal of border crossing for undesired aliens.

Since the network of biometric registration is densely tied, wanted criminals and terrorists may be localized immediately. This is accomplished by using the position data accumulated from shopping, traffic toll, mobile communication systems, and public transportation.

Obviously, this cannot be a solution against terrorism since only known terrorists are detected. Therefore, prevention will be used to solve the problem. Prevention can be realized using profiler agents which permanently investigate all data collected with respect to certain crime patterns or unknown anomalies. This is assumed to significantly reduce crime rate. (Contrariwise, Samidh Chakrabarti and Aaron Strauss stated in a scientific paper [7] that under certain conditions, profiling is less successful than random search, if a terrorist chooses an adapted counter-strategy.)

## **2. The Biometric Society and its risks**

I distinguish two kinds of risk, i.e., security related risks and privacy related risks. It seems that security related risks are solvable by technical means while privacy related risks need political and legal measures! While security shortcomings mainly affect property, privacy more directly targets a person.

### *2.1. Security related risks*

Since big values are moved, this may seduce criminals to steal an identity to take over foreign rights. There are many methods to fool a system with stolen identities – most of them can be met with known protection methods such as cryptography. Mechanical copies of biometric features are the most critical challenges in our case. As countermeasure, nearly perfect copy detection is essential. Interestingly, with a perfect copy detection, publicity of a biometric feature is no problem any more – especially, there is no necessity to keep biometric templates secret!

### *2.2. Privacy related risks*

With perfect copy detection and a tamperproof system, the knowledge of biometric template data does hardly affect privacy if we suppose that the template data exclusively carries identity information but no other information such as health data. The realization eventually has to guarantee that the biometric data stem from the original feature owner. The role of biometrics is only that of a unique identifier which enables easy database linking. This is a process which is mainly controlled by the operators of the identification application.

The real danger is the misuse of the identification application which collects and stores a lot of private information! For example, if the identification application is used to search for terrorist profiles, false assignments to innocents may be produced. And this issue may even question the whole application, respectively, the Biometric Society. This kind of risk can hardly be solved technically.

The privacy matter is treated now, while focusing on giving up privacy with respect to the biometric identification system, its operators, and possible governmental users.

### *2.3. The Biometric Society and privacy*

The central biometric identification system which is the heart of the Biometric Society enables nearly total surveillance by linking all transaction data!

This poses the following questions:

- Will total surveillance come along with the Biometric Society?
- If total surveillance becomes reality, will it really be dangerous?

All these questions cannot be answered today! But we should discuss the possibilities!

#### 2.4. Will total surveillance come?

Due to digitization of communication, it becomes extremely easy to create traffic data in form of log files. Due to advances in mass storage and computer technology, these log files can easily be stored and examined for all kind of information. It is very easy to use this traffic data for purposes, which are not in the intention of the feature owner. It's simply a software change.

As soon as something is technically realizable, there is a lot of demand to use these private data, especially for law enforcement, advertising, and criminal prevention.

Furthermore, it is extremely easy today to get the agreement for legal misappropriation of traffic data. There is little resistance from those who are affected. Commissioners for data protection have to do hard to stand up to government because their support from the public and media is surprisingly small. A delicate example is the continuing contempt of EU flight passengers' privacy by the EU Commission regarding personal data to be transferred to third parties with weak legal foundation. [8, 9]

Today, it cannot be predicted where the extension of surveillance stops. I guess this will be a one-way process which never ends and which will never reach total surveillance. The process can be compared with a mathematical series like 1, 2, 3, 4 ... which tends to infinity, but will never reach infinity. Alternatively, an inversion of this trend seems only be possible after a restart following a political disaster like that one in Germany 70 years ago.

#### 2.5. Is total surveillance dangerous?

From a security and safety point of view, surveillance of objects is an effective method to prevent accidents or crime.

Slightly different is the situation where people are monitored preemptively against crime and terrorism. In this case, surveillance and tracking directly affects privacy and is naturally rejected by many citizens. As for each achievement in modern technology, there are two sides of the medal:

- a) beneficial use for law enforcement, assumed in states which obey human rights
- b) misuse by governments which consciously ignore human rights and prosecute unpleasant citizens

The reason for a bad reputation is that surveillance is regarded as a means to keep totalitarianism alive by keeping down opposition. But is surveillance also a means to establish totalitarianism? This question cannot be answered by the author. But if the answer is "yes", the results are quite unpleasant.

Totalitarianism has been shown to correlate strongly with "democide". H. J. Rummel, a professor emeritus of political science at the University of Hawaii, has shown that totalitarianism, in contrast to liberal democracy, is positively correlated with democide in a statistical sense [10]. The term "democide" he created to express "murder by government", as has been experienced, for example, under the Nazi dictatorship of Adolf Hitler. This enables two conclusions:

1. totalitarianism is the cause for most democide, or
2. democracy has no chance to establish in environments which favor democide.

## 2.6. Observations

Most people agree that the most feared occurrence in life is an unwanted death. So I have collected some data which shall compare several reasons for unwanted deaths. All data refer to worldwide deaths per year. The figures are either recent data or have been averaged over a long time period [11, 10, 12, 10, 13]. A long-time averaging is reasonable in those cases where the data show strong yearly variations.

For comparison, the estimated total number of deaths per year will be about 57 Mio. people in 2006 [14] which is about ten times as much as the smoking bar in the diagram.

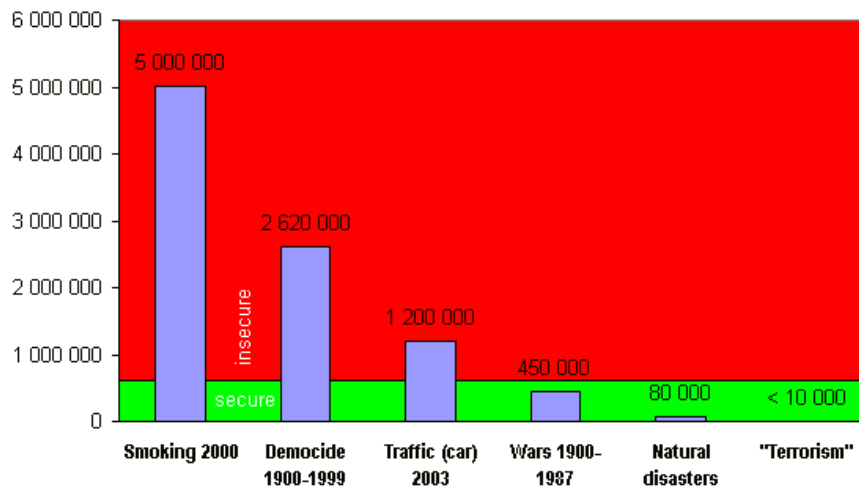


Figure 2. Worldwide deaths per year (recent or mean value) (© Bromba GmbH)

For many people it may be surprising that not terrorism or natural disasters are the reason for the most artificial deaths. Even wars are small in effect compared to traffic, democide, or smoking victims. Although the data may not be very reliable, changes by even a factor of 10 will not principally change this image. Since there is no commonly agreed definition of terrorism, I made the worst case assumption of 10 000 deaths per year. But even this pessimistic number is not able to show a visible bar in the diagram!

Note the border line between the red and green background which is defined by 1% of the natural death rate I have used to define the *required security*. This *required security* separates between "secure" and "insecure".

I must confess it was a surprise for me that for the chosen definition even the combined effect of wars, natural disasters, and terrorism does not qualify our world as an insecure world! And I have ceased to understand why terrorism shall really be a problem for this world while getting more and more concerned about certain reactions of democratic states.

Is it appropriate to directly compare the different reasons of deaths? I agree that there may be many reasons to exclude, e.g., (direct) smoking from this comparison. In

contrast to a terroristic murder, a smoking death is a silent death. In contrast to a traffic victim, most people are free to decide not to smoke. But if I, as a victim, have the choice to die through a traffic accident, possibly caused by a drunken driver, or by a terroristic assassination, I do hard to see the difference. Surely, the attention of modern media and the reaction of the public are quite different in both cases. The reason may be that humans tend to overemphasize seldom occurrences and to ignore problems they are accustomed to.

### *2.7. Comments*

Although the cause-of-death diagram only presents a worldwide average view and thus would actually need a more local consideration for an individual, this diagram provokes some critical comments. First, there seems to be a dramatic mismatch between real danger and felt danger. Second, there seems to be a dramatic mismatch between real problems and resulting activities.

For example, most German governments so far mainly acted for the German tobacco industry [15] when suing against the European tobacco product directive 2001/37/EC. In the meantime, other European countries like Ireland, Norway, Italy, Poland, and Spain felt responsible for their citizens and prohibited, for example, smoking in restaurants.

On the other hand, Germany was among the first to introduce the biometric passport with the justification to fight against terrorism, although most experts are convinced about the ineffectiveness in this special regard. And just the activities against terrorism often are suspected to help totalitarianism. Totalitarianism, however, is the medium for state terrorism and democide which is one of the real threats to humanity as shown in the diagram.

### *2.8. Conclusions on the risks of the Biometric Society*

From all the statements above, I draw the following conclusions:

- c) With respect to surveillance, biometrics is not the delinquent, it's only the accessory.
- d) Biometrics is not necessary to enable nearly total surveillance – but it can be very helpful.
- e) (Nearly) total surveillance in a democracy need not be a danger – but a successful coexistence has not yet been shown in practice.

## **3. The Biometric Society and its realizability**

### *3.1. System proposal*

A straightforward solution to the biometric identification system which fulfills the requirements of the Biometric Society is to use a central system with central data base. In principle, this can be concentrated on a single location. However, multiple locations are to be preferred with respect to reliability and vulnerability.

The operator should be neutral. He is responsible for the technical part and has only to obey the operating instructions which are to be derived from special international laws.

### *3.2. Storage and traffic requirements*

To estimate the storage and communication traffic requirements, we assume 100 identifications per person and day and 10 billion ( $10^{10}$ ) people worldwide. Then  $10^{12}$  identifications have to be performed per day.

Now assume 100 kB as sample size of a biometric template, where request and reference template shall have the same size. Then the storage requirement for the biometric reference templates will be  $10^{15}$  B = 1 000 TB = 1 PB. This is realizable today with 2 000 hard disks with 500 GB each!

The traffic resulting from sending the request templates then will be  $10^{17}$  B per day. This is assumed to be the amount of the worldwide internet traffic today [16]. With distributed systems such traffic should be realizable within several years from now.

### *3.3. Processing power requirements*

For the processing power requirements we start again with 100 identifications per person per day and 10 billion ( $10^{10}$ ) people worldwide which results in  $10^{12}$  identifications a day. Furthermore assume 1 million ( $10^6$ ) operations per comparison. Then  $10^{16}$  operations per identification are necessary!

This results in  $10^{28}$  operations per day or about  $10^{23}$  operations per second. If  $10^{10}$  operations per second are possible with one PC (or  $10^{14}$  for a supercomputer [17]) this results in the need of  $10^{13}$  PCs or  $10^9$  supercomputers! But I am far from giving up!

### *3.4. How to achieve the necessary processing power*

If the template comparison is replaced by dedicated hardware to calculate the whole result within one clock cycle, i.e., when it is  $10^6$  times faster, the processing requirement is reduced from  $10^{23}$  to  $10^{17}$  operations (Ops) per second, resulting in  $10^7$  PCs or  $10^3$  supercomputers. Now there are two ways to solve the remaining lack:

- Wait for advances in computer technology:
  - Required:  $< 10^{17}$  Flops (floating point operations/s, assume Flops = Ops)
  - Available today:  $> 10^{14}$  Flops [17]
  - Available 2016:  $> 10^{17}$  Flops (assuming annual doubling)

- Or look for intelligent identification strategies:

Most individuals have a limited action radius. For example, if succeeding identifications are done within an imaginary circle of 1 million people, search may be successful after 1 million identifications instead of 10 billion. This will save a factor of 10 000 in this example so that only  $10^{12}$  Flops are required. And this is feasible today!

### *3.5. Biometric requirements*

Regarding the biometric performance, we again assume 10 billion ( $10^{10}$ ) people worldwide performing 100 identifications per person and day. Furthermore, let us assume 1 biometric feature per person enrolled. Finally, the error that two persons be

confused should be less than 1 per day. To estimate the required performance with respect to False Acceptance Rate (FAR), we make two assumptions:

- *Assumption 1*: If the identification would be completely deterministic, an FAR of slightly smaller than  $10^{-10}$  is required to guarantee that no two features are equal. This error rate does not increase with the number of identifications because no new fingerprint pairs are compared. This is assumed to be the best case. In reality it can only be reached when using unique ID numbers instead of biometrics.
- *Assumption 2*: If the identification would be “completely statistic”, an FAR of  $10^{-22}$  is necessary (coming from  $10^{12}$  identifications against  $10^{10}$  references). This is assumed to be the worst case approximation. It is too pessimistic because of dependencies between the comparisons.

Both cases will help us to find out suitable biometric characteristics which have to perform somewhere between the two extreme cases.

### 3.6. Which biometric feature is usable?

Due to large performance differences in different biometric features, not every feature is able to satisfy the extreme requirements of the Biometric Society. We will only discuss the three most common biometric features here.

If a (verification) FAR of about  $10^{-10}$  would be sufficient, then

- Face recognition is far away from being usable
- Fingerprint recognition will be possible with one or two fingers
- Iris recognition will do without any problem

If a (verification) FAR of about  $10^{-22}$  should be required, then

- Face recognition again is not possible
- Fingerprint recognition now should be possible with three fingers
- Iris recognition should be possible with two irides

It must be remarked that a usage of more than one feature per person will further increase technical requirements because it multiplies the number of comparisons per second!

### 3.7. Fake detection

Despite of numerous different claims, a nearly perfect fake detection is one of the great unsolved problems in biometric identification today. We have to distinguish three different types of fake detection.

*Liveness detection* is necessary to prevent identification with dead body parts. The challenge is twofold:

- First, a measure for liveness has to be found in order to be able to detect it.
- Second, it must be guaranteed that detected life really belongs to the feature owner and not to the impostor.

*Copy detection* is a basic requirement to prevent forgery with copied features. Also, it is necessary in order to detect copied features which are tied to living bodies.

A problem that has been neglected so far is *volition control* to prevent unconscious or enforced identification.

### 3.7.1. Fake detection example: fingerprint

Let us consider the present situation with fingerprint as an example. Today, all systems can be fooled if the liveness detection method or the copy detection method is revealed! Even the best fake detection methods known so far will increase the False Rejection Rate (FRR) considerably. Here are a few examples. Note that the optimum method depends on the sensor principle!

- Temperature is easy to be circumvented by temperature equalization
- Skin conductivity is very unstable and mainly increases FRR
- Skin impedance is not very specific
- Dielectric constant of skin is easily forged by gelatin
- Pulse measurement takes several seconds and may be too lengthy
- Measurement of the change of oxygen content of blood together with pulse detection may easily be circumvented by fingerprint foils which cover a finger of the forger

### 3.7.2. Fingerprint fake detection: a possible solution

Most fake detection methods fail in the case somebody covers his finger with a transparent artificial fingerprint foil. However, this should be manageable by using a real 3 dimensional sensing method. Possible candidates are ultrasonic sensors which create a 3D image of the whole interior of the finger. Besides the fingerprint which mainly represents the surface of the finger, an image of the internal skin layer structure is delivered. This should reveal artificial cover foils with false fingerprints and should also indicate the proper function of the blood circulation.

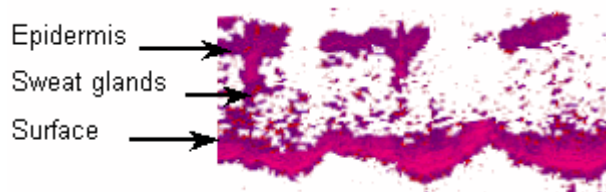


Figure 3. Cross-section through the human skin of a finger (© Siemens AG)

Two principles for ultrasonic sensors are known. Optel proposes a single source ultrasound generator while Siemens favors an ultrasonic generator array on a silicon chip. Both methods are still looking for commercial realization.

### 3.7.3. Micro-machined ultrasound transducers

The high resolution ultrasound sensor from Siemens is based on micro machined ultrasound transducers which use the pulse-echo principle at 30...50 MHz. It is using a surface micro machined membrane array within a standard CMOS semiconductor process. A 300  $\mu\text{m}$  matching layer serves as coating. The advantages are

- Real 3D finger image of surface and subsurface structures such as epidermis
- Recognition of sweat glands and their activity
- Easy detection of artificial layers as copy detection
- Liveness detection by Doppler effect from pulse changes

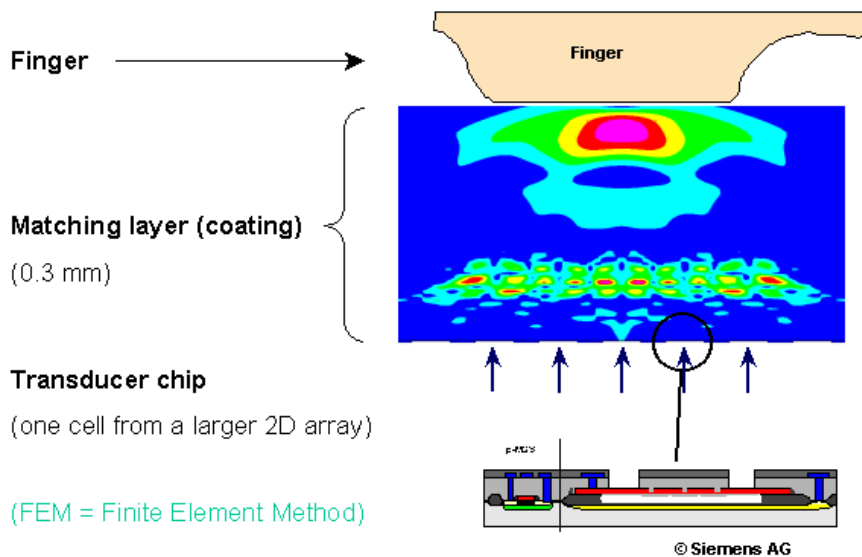


Figure 4. FEM simulation of the sound field (Siemens)

### 3.7.4. 3D data processing

Suppose a raw 3D image of 256 x 256 x 256 pixels with 8 bits each. Then the file size amounts to 16 MB per image without temporal information! Transmission from sensor to processing unit should be performed within 0.5 s, resulting in a speed of 256 Mbit/s. This is achievable with USB 2.0. The required processing power of about 25 GOPS (Giga operations per s) will be provided by future PCs.

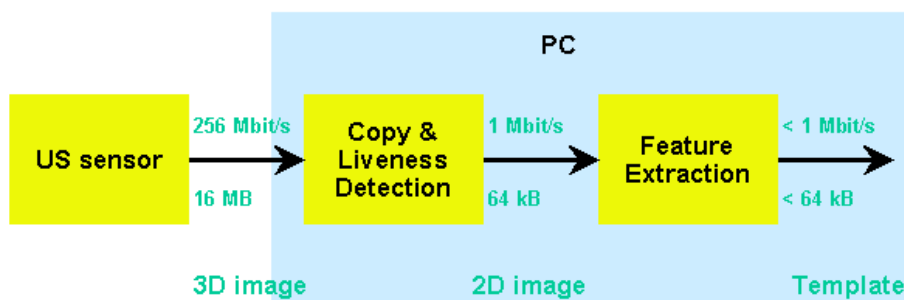


Figure 5. Schematic of a 3D processing chain (© Bromba GmbH)

### 3.8. Availability of biometric features

The next hurdle towards the Biometric Society is the fact that not every biometric feature is reliably measurable anytime. This is expressed in the "Failure to Enroll Rate" (FER) which specifies the part of biometric features that actually cannot be registered. Since this temporal failure may also happen after successful enrollment, it can prevent identification, too. In this case it is called "failure to acquire".

For fingerprint, the FER is about 5% for the whole population and smaller than 1% for an office population, with declining tendency for improving sensor equipment. For iris recognition, the FER also strongly depends on the sensing hardware. For expensive hardware, the FER is below 1 % for office workers. Unfortunately, there is no chance to reduce the FER to similarly low values as the verification FAR.

We did not discuss the effect of FRR which may be reduced to very small values by multiple identification trials. In principle, the FRR should lie in the same range as the FER. As a consequence, if no work-around methods are provided, this could eventually prevent the Biometric Society.

### 3.9. Introduction scenario

For that reason, the question is fundamental whether the Biometric Society needs a perfect system, or not. The answer is possibly no, the system need not be perfect, because it should be manageable

- to start with smaller units, e. g., country-wide instead of worldwide. This reduces all technical and biometric requirements.
- to allow alternative methods for identification to reduce enrollment requirements
- to allow for voluntary participation to eliminate acceptance problems
- to restrict the system to transactions of low value to reduce the demand for perfect liveness and copy detection.

## Summary

To summarize, there is a good chance for the Biometric Society to be technically achievable. The advantages are unquestioned. The risks are imaginable but unpredictable. And that will be the real challenge!

## References

Hyperlinks last visited 2006-11-04

- [1] Europe's Information Society - Thematic Portal [http://europa.eu.int/information\\_society/index\\_en.htm](http://europa.eu.int/information_society/index_en.htm)
- [2] M.U.A. Bromba, The Biometric Society - Fiction or Inescapable?, Biometric Identification Technology Ethics (BITE), V. MEETING: FUTURE TECHNOLOGIES, Wroclaw/Poland, 2006-03-24, <http://www.bromba.com/knowhow/BITE.htm>
- [3] M.U.A. Bromba, The Biometric Society - Risks and Opportunities, NATO Advanced Research Workshop - Identity, security, and democracy - Jerusalem 2006-09-02/04, <http://www.bromba.com/knowhow/ARW2006.htm>
- [4] Jain, A.; Bolle. R.; Pankanti; S. (Editors), Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.
- [5] M.U.A. Bromba, Bioidentification FAQ, <http://www.bromba.com/faq/biofaq.htm>
- [6] HDMI Homepage, <http://www.hdmi.org/>
- [7] S. Chakrabarti; A. Strauss, Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System, MIT, 6.806: Law and Ethics on the Electronic Frontier, May 16, 2002, <http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm>
- [8] S. Kreml; C. Morris, EU and US reach interim agreement for the sharing of passenger data, heise online, 2006-10-06, <http://www.heise.de/english/newsticker/news/79116>
- [9] C. Morris, Court finds no legal basis for passenger data to be given to US, heise online, 2006-05-30, <http://www.heise.de/english/newsticker/news/73653>
- [10] R.J. Rummel, Homepage, <http://www.hawaii.edu/powerkills/>

- [11] WHO Fact Sheet EURO/07/03, Copenhagen, 17 December 2003, [http://www.euro.who.int/mediacentre/FactSheets/20031212\\_1](http://www.euro.who.int/mediacentre/FactSheets/20031212_1)
- [12] German Wikipedia: Verkehrstod, <http://de.wikipedia.org/wiki/Verkehrstote>
- [13] German Wikipedia: Naturkatastrophe, <http://de.wikipedia.org/wiki/Naturkatastrophen#Katastrophenstatistiken>
- [14] The World Factbook, CIA, <https://www.cia.gov/cia/publications/factbook/geos/xx.html>
- [15] T. Reichart; U. Stoll; I. Wohsmann, Tabakverband blockiert Werbeverbot, ZDF Politik & Zeitgeschehen, <http://www.zdf.de/ZDFde/inhalt/29/0,1872,3904477,00.html>
- [16] BeSpacific homepage, <http://www.bespacific.com/mt/archives/001999.html>
- [17] TOP500 Supercomputer Sites, <http://www.top500.org/lists/2005/11/>