Biometrics: the Solution for a Safer Society?

Lipika Bansal

UNIVERSITEIT VAN AMSTERDAM

Biometrics: the Solution for a Safer Society?

Lipika Bansal – 9719091

Amsterdam, July 2007
Master thesis Science & Technology Studies
Faculty of Social and Behavioural Sciences
Universiteit of Amsterdam [UvA]
Supervisor: Prof. Dr. Cees J. Hamelink

Foreword

Before starting this masters program Science and Technology Studies [STS], I was almost certain I wanted to write my thesis on biometrics. With this theme in the back of my mind, I came across STS. I immediately decided that this was the study I wanted to do. I wanted to have a critical look at the technological impact of biometrics on western countries. My motivation letter to the study coordinator – Arend Benner said that I was "particularly interested to investigate how security technologies in western countries are applied and realised". I would like to learn more about the increasing security related technologies, such as biometric passports, cameras for.

When we had to choose our supervisor Dr. Amade M'Charek happily offered to guide me through this ordeal. I told her about my interest in biometric technologies and about a few cases in the Netherlands I had read about. One was the VeriChip; VIP-members could choose for an implanted chip, in order to have special services. In the other two settings biometric technologies have been implanted at the entrance of a disco and a swimming pool for visitors. These are 'opposite' technologies; in one case a technology is inserted in the body – external details are stored within the body, whereas in the other two cases bodily information is inserted in a technology, the body data is stored in an external database.

Unfortunately my supervisor fell ill. Meanwhile Arend Benner guided me every two weeks to get me motivated again. Dr. Sher Doruff from Waag Society advised me to explain more explicitly the case studies I had done. Eventually Prof. Cees Hamelink took up the task to guide me through this enormous mission.

Hereby I would like to thank the following people for their guidance and support during my thesis: Prof. Dr. Cees J. Hamelink, Dr. Amade M'Charek, Dr. Sher Doruff, Arend Benner, Buro Jansen & Janssen. Moreover I would like to thank Logica CMG, Dartagnan, Secure Access Road B.V., Alcazar, De Fakkel and Baja Beach Club for their time and effort for cooperating and arranging respondents for my research. Without their help, I would not have been able to complete my thesis successfully. Finally I would like to thank my parents, sister, and my friends for stimulating me to complete my thesis.

Content

Abstract

We can see an increased use of biometric technology in our everyday lives. The attacks on the WTC at 9/11 have jumpstarted many developments in this field. Even though the argument of safety is usually used to create acceptance for this technology, the main reason is usually found in marketing objectives. Instead of a more secure society, the loss of privacy as a result of this technology should be considered a threat. This thesis is about uncovering the real effects of the rising popularity of biometrics and the motives behind it.

In western high technology societies data is continuously related to our daily activities. It is collected, stored and exchanged.
In this thesis I try to answer questions regarding the effects of biometric technologies in contemporary high-tech societies, since these technologies are seen as the solution against terrorist attacks and other threats. But what we can see is that these technologies create a risk for a democratic society.

In order to answer the main question: *Which functions do biometric technologies have in society and how do end-users eventually internalise these technologies?* I have chosen three real-time case studies. From these case studies [implemented in public space] it becomes clear that there are different motives behind industry and small private enterprises in promoting these 'security' technologies. It is clear that end-users are willing to give up their personal data easily in exchange for a more secure environment. Moreover there are some dangers which we as public should be aware of:
There is an ongoing trend of increased control; these biometric technologies increase the capacity to discriminate and sort people in different groups and classes; the technology can be outwitted.

Keywords

Biometric technologies, security, Alcazar, De Fakkel, Baja Beach Club, Secure Access Road B.V., VeriChip, Big Brother, surveillance, panopticon, informaticised body, rhizome, social sorting, dividuals, consumer effects, internalisation

1 Introduction

1.1 History of Authentication

For a long time authentication procedures in government service provision were of course paper-based. The means of authentication, such as the passport, birth certificate or drivers licence, were used as an official proof of the individual holder's self-declared identity. Slowly this checking of paper-based proof took place in face-to-face citizen-to-government relationships [Lips, M, Taylor, J., and Organ, J., 2005]. Now that we live in a digital era of technologies our society facilitates the development of an 'e-government' service domain. New forms of authentication have come up and are required for situations in which the digital citizen's identity must be checked as part of an assessment of service entitlement. With the introduction of identity management [IDM] there is much fear about surveillance of citizens and other privacy intrusions; logically these new systems are expected to be of an intrusive character.

1.2 History of Identification

During the French Revolution administrative bodies could check and verify the level of honesty of travellers on the basis of their passport and watch dubious or foreign people who would need 'particular' attention. A distinction was made between 'true citizens' and 'non-citizens'. This leads to the establishment of a civil status which determined that an individual only existed as a citizen, if the identity had been registered by municipal authorities.

Until now the process of personal identification has been relatively constant; the passport holder shows his or her passport to the authorities and verifies the document carrier is the person shown in the information, including photograph, included in the document. Throughout the 20th century West-European bureaucracies introduced the passport as an official public means for establishing the national identity of a citizen crossing national borders and soon after this authentication process became common to all Europeans. By issuing passports nations have the exclusive right to authorise and regulate the movement of people. The first passports and passport controls were not to regulate citizens' access to spaces, but rather to prevent people from leaving their home territory.

In the 20th century governments had the desire to regulate immigration and restrict immigration of specific national groups and stimulate economic opportunities for their own citizens and be able to protect their own country for suspicious people in times of war. After the Second World War, controlling the international movement of people became widespread. This led to a global authentication system in which passports issued by various national governments were recognised as official proof of a citizen's personal identity.

1.3 Current Situation

In order to understand how these surveillance systems developed and became part of the 20th century; one briefly has to understand the history of surveillance in modern times. Surveillance is practiced with the perspective to enhance efficiency, productivity, participation, welfare, health or safety. Therefore social control is hardly a motivation for installing surveillance systems; it is rather an unintended consequence [Lyon, D., p. 673, 2003]. From the earliest days of a nation state, the aim was to consolidate state power against others and maintain the position of elites, rather than to use raw informational power to keep subjects in line. Currently governments say that [biometric] national identity cards will help to combat fraud, illegal immigration, organised crime and terrorism. Critics on the other hand insist that this will be ineffective expensive and intrusive [Guizzo, E., p.42, 2006].

The influence of these new forms of authentication shows us citizen – government relationship; individuals are seen as citizens or non-citizens, customer or non-customers, authenticated citizens or non-authenticated citizens. People are categorised systematically having access to virtual territories or kept out of them. This citizen sorting opens the possibility to check on a remote distance and validate whether people should have access to service in a variety of ways, hidden to the end-consumer. Since consumers are usually not aware of these IDM systems they are generally 'accepted'. Consequently various parties can look for ways to serve customers better and develop long[er] lasting relationships with them. This means that companies and others will use databases to provide regular customers with a discount or proactively provide them with information relevant to customers.

1.4 Biometric Technologies

Quite a few industries did well after the September 11 2001 attack. One of the biggest 'winners' is the biometrics industry. Security measures include a number of surveillance devices and systems. After September 11th companies and governments that already had an interest in surveillance systems now had a reason and public support for implementing these technologies of surveillance [Lyon, D., p. 666, 2003]. They are intended to increase safety, by predicting and pre-empting danger and by restricting access to a given country or site, only accessible to eligible people.

Biometrics, also known as personal identification technologies, is an industry that is concerned with the measuring and regulation of life. Biometric providers convey powerful messages by persuading to use biometric access control systems. Access to systems and areas is still regulated through something you have, like a card or something you know, like a PIN, but both these methods are unstable and insecure. It is argued that it is better to link the access code to something you are, which is non-transferable: your body.

Biometrics is a major growth sector of the Information Technology industry. Biometric technology is increasing at a rapid pace. Biometrics has become a 'buzzword' in today's society, related to matters of security and privacy [Simpson, I., p.1, 2006]. Biometric technologies are being developed to combat problems of identity theft, fraud and terrorism. Many argue that biometrics could be the solution to all problems of security, if properly implemented, as the only way to get access to restricted areas would be to have the exact physical characteristics of that person.

The goal of biometric technologies is to correctly identify a person in a manner so that it is accurate and foolproof [Migani, C., p.1-2, 2005]. If this system becomes as widespread has hoped, this would also give information about an individual's whereabouts, and daily habits to be looked up in a few minutes, giving away one's own privacy.

The strange thing is that there is hardly any concern being expressed about how quickly we are being 'forced' to connect our bodies into various networks of regulation, given the relation of criminality and biometrics [Fuller, G., p.1, 2003]. In the public sphere several biometric systems have been implemented for security purposes, even before September 11. Schiphol and Heathrow were the first airports trialling biometric systems. Moreover anyone who wants to travel to the U.S. from 2004 or Britain from 2005 must have a biometric encrypted in their passport or visa document.

So slowly we are moving into a situation, through the politics of crisis and fear, in which biometrics quietly becomes a part of the information architecture of everyday life. Anyone resisting to 'connect' their body into a global network of tracking and control will simply not gain access.

Seeing the current developments and technological advances, one can only expect an increase in the use of biometrics by private companies as well as in public for safe and accurate identification. More so we still see technology as a saviour and as a solution for all problems [Lyon, D., 667, 2003]. Technological solutions are called upon before other more labour-intensive and human-oriented surveillance methods. It is especially surprising, since after September 11th the monitoring technologies did not seem to have provided warnings.

1.5 Biometrics no more SF

I would like to follow real time applications, and research the usage of various authentication technologies and how customers got convinced of the reliability of the biometric technology. In 2005 the first swimming pool in the Netherlands - Ridderkerk has implemented a biometric entrance system. The device scans the face and fingerprint.
There are also various discos in the Netherlands using biometric devices at the entrance. One of them is in Rotterdam, the Baja Beach Club, using an implanted chip for customers; also used to pay beers automatically when their chip is scanned.

Looking from this viewpoint one can see that these technologies are not imposed by the government, but rather that these technologies are provided by companies, producers of private businesses. These devices then are applied and integrated in these private firms for their day-to-day functioning. Eventually decisions are made by individuals to use these technologies. Apparently end-users do not have many problems in accepting these biometric technologies. It is possible that these technologies do enhance the 'safety' feeling among the citizens, as only people who have a membership are allowed to enter or in the second case, where people get themselves 'chipped' as part of a new lifestyle or belonging to a certain group; an exclusive member of a certain club/ bar/ disco.

1.6 Subject Matter

This thesis will try to look the effects of biometric technologies in contemporary high-tech societies. Nowadays we are interwoven in all sorts of communication and transaction networks, not realising what this could mean and how they could possibly affect our day-to-day life. I will try to argue my statement: *safety is usually used to create acceptance for these technologies, but the main reasons are for marketing objectives,* by using three real time case studies. In these three cases various biometric technologies have been implemented in public space for 'security' reasons. During my investigation it will become clear that there are usually different motives hidden behind the usual line of reasoning, which is security. It has been proven that people are ready to give up everything in exchange for their safety. It is clear that in this case people are driven by fear and are willing to hand in their privacy and jeopardising their civil liberties. Thus one can see that there are two opposite arguments regarding biometric technologies. Various groups, driven by industry believe in these technologies as the solution for all security and fraud problems, against privacy and civil liberty groups, which pose that the citizens' civil liberties are at stake.

1.7 Main Question

My main question is: *Which functions do biometric technologies have in society and how do end-users eventually internalise these technologies?*

1.8 Relevancy

1. **Scientific relevance:** As explained above there are two contradictory opinions [industry, governments and private companies versus privacy and civil liberty groups] on biometric technologies and its implication on society.

   This research is also significant for its choice of biometric technologies. I am comparing two rather 'opposite' technologies. These two technologies are particularly interesting, because in the one case bodily information is inserted in a technology and this becomes the authentication tool; the body data is stored in an external database, whereas in the second case, a technology is inserted in the body

and the external details are stored within the body; the implanted chip is linked to your personal identity. In one technology the body is used as data [the fingerprint and face scan]. It is taking critical identity data, invading the identity and privacy of individuals, whereas in the other case study people receive an implanted chip. In this case data is inserted in the body, augmenting the body to push data and information out. It gives the body 'something extra'. This is another form of invasiveness.

2. **Social relevance:** Secondly the social relevance is that the usage of biometric raises huge ethical questions, such as the protection of privacy or the reliability of the technology itself. As mentioned before, people and privacy advocates are concerned with the safety of these technologies. Even though various pilot studies are conducted in the Netherlands; one does not hear much about the eventual outcomes of these studies in the media. In order to come to understand the matter, it is important to investigate the pros and cons of biometrics and accordingly make estimations about the effects of these technologies. One should have a critical stance when adopting such technologies in society and have a closer look at it.

1.9 Research Objects

In order to answer my main question, I will interview various groups. Firstly I will interview companies who produce and provide biometric technologies.
Questions will be like:

- Why are such technologies used?
- Are they easy to standardize?
- Are they easy in their usage, portable, cheap etc.?
- Are they secure?
- Can you see an increase in your sales in the last year?
- What kind of customers do you have?
- Why do you especially have such customers?

Next I will interview firms, companies who actually have implemented, integrated these biometric devices.
Questions will be like:

- Why did you buy this particular technology?
- Do people refuse to become member of your club?
- What do you do with the data?
- How do you store it?
- What kind of customers do you have?

Eventually I will interview the end-users.
Questions will be like:

- Why did you become member of this particular club?

- What kind of feeling does it give you?
- Do your friends come here too?

2 The Impacts of 9/11 on Security Policies

2.1 International Landscape after 9/11

After 11th September 2001, the war on terror has become a political top priority globally. Worldwide, actions are undertaken to increase a sense of security. With these increased security controls and zero tolerance policies, one can perceive a proactive lobby for more pre-emptive safety measurements such as, more 'blue' on the streets, the obligatory ID card, surveillance camera's, biometrical passports; these are seen as the solution against crime. Heavy anti-terrorist legislation aimed at domestic protection measures is taken. One of the main methods proposed are the enhanced surveillance operations. Public money is poured into policing and security services. Moreover high-tech companies are offering technical solutions to prevent such attacks from happening again [Lyon, D., Privacy Lecture Series, 2001]. This has changed the everyday landscape, as these new technologies like iris scanners at airports, closed circuits television [CCTV] cameras are introduced on streets and squares in our daily lives.

The media also plays a role in enhancing a certain feeling of insecurity and fear among the general public. People are continuously confronted with images and coverage on terrorist acts, crimes and violence, causing distress among public [Ziegler, R., Mitchell, D.B., p.175, 2003]. But what does it mean to be in a completely safe environment? Is that what we are looking for: a completely protected society?

The more we are protected, the less secure we feel; nowadays there is no public space without some danger, but total control is not the answer. Each degree of freedom we surrender buys us ever-smaller degrees of protection, in pursuit of Absolute Zero Threat [Privacy International, 2006].

For more than two decades, governments and companies have used technologies to collect process and disseminate a vast spectrum of personal information. Since the late 1980s, when computer and telecommunications systems began to converge, this process has accelerated. The result is that personal privacy is endangered as never before [Bocozk, K.; Buster, C. J. e.d., 2005]. Nowadays we often hear how everything has changed because of terrorism, international organised crime and other important threats in our society. As a reaction to all these threats we risk to jeopardise our principles of an open society.

Consequently, in the name of safety, governments justify the implementation of the increasing security related technologies, such as biometric passports and surveillance cameras.

As we can witness, big events such as September 11th have had repercussions on the social world. It shows that greater awareness becomes apparent; a sort of 'wake-up' call. It has

created a potential increase of surveillance in several countries. One can see a dramatic increase of the centralisation of surveillance in western countries. Furthermore there is a tendency to rely on technological enhancements to surveillance systems, whether they work or not.

One can see that in the U.S.A. and several other countries laws have been passed; intended to tighten security, that give police and intelligence services greater powers and to permit faster political responses to 'terrorist' attacks. Moreover it has become easier to find or arrest people suspected of terrorism, since there are limitations on wiretaps, which has also been extended to the interception of email, Internet click stream monitoring and phone calls. In Canada profiling methods are used to track racial and national origins as well as travel movements and financial transactions. Furthermore some countries have proposed a new national identification card system, some involving biometric devices or RFID chips.

In response to September 11, technical companies have multiplied. High-tech companies saw September 11 providing just the platform they required to launch their products. Various technical surveillance tools mushroomed, including the iris scan, such as at Schiphol airport in Amsterdam, which is now being implemented in other places in Europe and North America. CCTV cameras in public spaces enhance if possible facial recognition. DNA banks store genetic information, in order to identify known 'terrorists.' In spite of all these new technologies, they may be tried, but not tested. It is not clear that they work with the kind of precision that is required. Moreover such technologies enhance social division and exclusion in countries where they are implemented.

We can also see a shift in solutions against terrorism; the technologies that are sought are iris scans, face recognition, smart cards, biometrics, DNA. All these technologies rely on searchable databases, with the aim of preventing acts of 'terrorism' by isolating in advance potential perpetrators. In America one can see that after September 11 possibilities of 'racial' profiling have increased especially 'Arab' lines. FBI collects information about Middle Eastern students from 200 campuses. With these technologies, persons and groups are constantly risk-profiled, but at the same time consumer categories are formed.

Surveillance has become the abstracting of bodies from places. The flow of personal and group data percolate through systems that were less vulnerable, more discrete and watertight. Thus after September 11, this surveillance data from various and numerous sources like supermarkets, hotels, traffic control points, credit cards transactions records etc. were used to trace activities of the 'terrorists' in the days and hours before the attacks. As mentioned above these searchable databases also make it possible to use commercial records, and so police and intelligent services can draw conclusions from these databases.

Such measures, which are based on everyday communications and transactions data; phone calls, e-mail, internet behaviour, could implicitly discourage these media tools for

democratic debate. In current individualistic societies this kind of surveillance methods are often seen as a potential threat to privacy, an intrusion on an intimate life, an invasion on the home sphere, and jeopardising anonymity. However it is never seen as a form of 'social sorting'. The general line of reasoning in public debate is: 'if you have nothing to hide, you have nothing to fear', an argument without any substance. Under the present circumstances, people are willing to collaborate with surveillance techniques and put up with many more intrusions, interceptions, questions than before September 11. This process has only been increased by media. Media polarise the choice between 'liberty' and 'security' [Lyon, D., Private Lecture Series, 2001].

These mechanisms of social sorting only reinforce social, economic and cultural divisions. Categorical suspicion does have implications for the new anti-terror measures passed after September 11. It is clear that 'Arab' and 'Muslim' minorities are disproportionately and unfairly targeted by these measures.

Surveillance has become more intrusive and technically-driven, so that it has become more preventive than investigative. Especially high-tech surveillance-device companies confirm that these technologies are required to prevent future 'terrorist' occurrences. The attraction of new technologies and the notion of pre-emptive measurements are strongly accepted among policy makers.

However, searchable databases and international communications interceptions were operational before September 11, but without benefit. The only result is that surveillance of citizens by the state will increase and 'terrorists' will anyway be seized by other means. Commercial surveillance; phone calls, supermarket visits and Internet surfing seems soft and not worth to see as 'surveillance', but one should have a critical stance towards these technological promises, since September 11, the bombings in London haven't prevented terrorist acts, but they do have an impact on citizens.

2.2 Dutch Landscape after 9/11

After the September 11, Madrid attacks, and the assassination on Theo van Gogh in Amsterdam, the European police collaboration has increased rapidly. Now that it has become clear that also the Netherlands could be a possible target for terrorist attacks, both in social responses as well as in government policies, various measures are taken. The war on terrorism has become one of the main focus themes in present politics. The September 11 event has had global effect. Even in the Netherlands one can see a change in the legislation. It seems that the Dutch government is especially trying to follow the U.S. policies, by acting firmer than before. This is especially problematic, because it does not prove that the police and the Dutch legal system comply with the current legislations [Amersfoort, R., Buuren v. J., e.d., Buro Jansen & Janssen, 2006]. Internationally the situation has already escalated to a stage, where people on an UN-or EU terrorist list, do not have any possibility to be judged by an independent judge about the correctness of the accusations.

In the name of terrorism certain values and norms of the democratic society are being undermined, including civil rights. Politicians easily approve of these new laws, without having the accurate knowledge which is required. We can see that civil rights are under pressure because hasty anti-terror laws are taken. Authorities do not seem to make an impression that it is a problem. Rather it seems that they try to seize the opportunity in order to take extreme measures which gives the state a bigger control over its citizens. In this context privacy is seen as a right one will have to give up in order to effectively fight terrorism. Politicians are ready to minimalise its citizens' privacy with decisions which don't even guarantee an effective contribution to society's safety, such as the obligatory ID card, data retention, and passing on citizens' information to the U.S. Moreover, one can say that citizens are also ready to easily renounce from their civil rights, by justifying it: 'if you have nothing to hide, you do not need privacy'. Apparently, those who fear are ready to give up their rights; additionally the right to freedom and the right to a fair trial are in jeopardy in the war against terrorism.

Previously one could only be tracked and traced if one would be a suspect of a certain crime; one is innocent unless proven otherwise. However the situation has changed since new law bills have passed as measurements against terrorism. For instance, it is sufficient to follow someone with special tracing methods based on some simple indications [Prakken, T., Buro Jansen & Janssen, 2005]. Secondly, infiltrators can be used in terrorist crime investigations. Thirdly, officials of a foreign state have the right to make use of the same local authorities. These facilities undermine objectivity; moreover it gives police the same power as the AIVD [the Dutch Intelligence]. It means that with little suspicion, the police can act upon the indication, even though it is not related to terrorist activities. In this case various databases can be linked when an investigation in terrorist crimes is being carried out. A problem with this form of investigation is that there is a chance that it is based on physical traits and ideologies rather than an objective outlook on the case.

Also the media play an important role; they enhance an insecure feeling by carelessly mixing information and facts. We can see that increased friend–foe thinking is going on especially towards the Muslim community.

2.3 Legal Framework

Until now biometric technologies have not been taken up by the law.
Article 10 of the Constitution is one of the fundamental rights. This article stands for the right to respect and protect the personal living environment [Artz, S.M., Blarkom, RE, v. G.W., p.1-10, 2002]. This Article has been taken as a result from Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Registration of Persons Act
Article 10 of the Constitution has the task to protect the personal living environment concerning the personal data. This has led to the Personal Data protection Act in 2001.

European Guideline 95/46/EG
On the European level article 8, the European Convention for the Protection of Human Rights and Fundamental Freedoms has led to adopt the 'Guideline 95/46/EG concerning the protection of people in combination with the processing of personal data and concerning the free flow of that data.

Personal Data protection Act
From the 1st of September 2001 the Registration of Persons Act has been replaced by the Personal Data protection Act, in which the Netherlands has to need up to the demands of the Guideline 95/46/EG and convert this in to national legislation. The Personal Data protection Act is a Framework Act in which general rules are introduced with regard to the protection of the personal living environment.

Other legislation
Next to the Personal Data protection Act there are several other laws in which specific rules are introduced with regard to the protection of the personal living environment. Examples of this are the Dutch Medical Treatment Act, Municipal Database Personal Records Act and the Telecommunication Act.

Article 13 Personal Data protection Act
The one responsible should implement appropriate technical and organisational measures to protect personal data against loss or against only form of unlawful processing. These measurements guarantee an effective safety level looking at the risks which come along when data is being processed and the nature of the data that needs to be protected, taking technique and costs into account. These measures are made in order to prevent unnecessary collection and further processing of personal data.

The principles of personal data protection
If there would not be personal data, there is no need to protect it, since there are no threats to the personal living environment. Nowadays we cannot imagine a system without personal data. Everybody has a computer system, which contains heaps of personal data. When a system is designed for processing personal data, the one in charge has to take in account which data is indispensable for processing. In short, personal data can only be processed when it is collected or processed for appropriate objective and not more than excessive.

Moreover the less people that have access to personal data, the better. Within the framework in which it is necessary to justify the usage of data; a strict authorisation structure is essential. It is obvious that this authorisation is only effective after a waterproof

process of identification and authentication. Authentication is necessary for as well as the user of an information system to get access to process personal data, as well as for the people concerned so that the identity can be ascertained when one wants to make use on ones right to inspection or improve ones personal data.

Biometrics

In order to ensure the authentication of a person, one can think of using biometrics. Biometrics is a technique which can be implemented only within the framework of the Personal Data protection Act. It is an efficient solution to secure personal data. The Dutch Data Protection Authority is much in favour of this technical measurement. The reason here for is that it is efficient: it is difficult to elude from the effect.

2.4 Legislation on Biometrics

In order to introduce a biometric identity card and passport the current legislation needs to be changed drastically. Most important here is that according to the constitutions' article nr. 11, the body cannot be exposed to humiliating situations; since the body's sovereignty and integrity is at stake.

The whole discussion came about in relation to identity theft and look-a-like fraud. Here identity theft means that someone intentionally uses another person's identity, which does not belong to him or her by using a false identity document. Biometrics seems to be the solution to this problem. Here biometrics could play a significant role. In the Netherlands there is no specific legislation yet for biometrics. But one has to look at the proportionality, necessity and the usage of biometrics. One has to question whether biometrics as an identification tool weighs up in relation to the problem.

Until now the laws regarding biometrics are similar to the other technological applications, such as the privacy laws and laws regarding identification data.

In the media one can especially see the discussion on the biometric passports and the question of central data storage. Most probably the central data storage system will not be implemented, since the privacy of Dutch citizens is at stake.

2.5 Landscape of Suppliers

Authentication is a critical function in many consumer and industrial applications. The shift to biometrics almost seems a natural solution for governments and industrial sectors seeking for better identification methods for security and fraud prevention [Langenderfer, J., Linnhoff, S., p. 314-315, 2005]. Since the September 11 attacks and the rise in worldwide terrorist activity, governments focus in the development of foolproof identification and tracking systems turning to biometrics as part of the solution. Prior to the September 11th events, biometric technologies were still just work in progress. But it is clear that there was pressure to develop and install face-recognition CCTV systems from the US Defence department, major companies and think-tanks such as Rand Organisation [Lyon, D., p.670, 2003]. Immediately after the attacks, the stock price of five major biometric vendors increased between 20% and 100% [Fleming, S.T, p. 134, 2003]. Billions of euros are involved

in this booming business. Facial scanning systems were established at some airports, proposals were made for fingerprinting foreign nationals entering the US. Everybody believed in the reliability and usefulness of the wide variety of biometric systems.

Within days and weeks of the aftermath a huge industry was eager to manufacture and sell the technology of surveillance: video cameras, facial recognition systems, fingerprint scanners, email and web monitoring, smartcards, location tracking etcetera. Moreover many people are eager to argue if you don't have anything to hide; you shouldn't mind revealing everything [Zureik, E, p.6, 2004].

Biometrics is quickly becoming a standard part of modern life. Commercial and governmental entities are rapidly embracing the technology that promises enhanced security and improved identification. It is seen as the magical formula to all security problems. Biometric payment systems using fingerprint scanning technology are widely in use by various companies. In 2003 point-of-sale biometrics existed out 2% of the total biometrics market, generating over €10 million and are expected to raise over €181 million by 2008. Biometrics is quickly becoming a source of income for the world of commerce. The revenues are driven by large-scale government programs and dynamic private-sector initiatives [International Biometric Group, January 2006]. Asia and North America are expected to be the largest global markets for biometric products and services.
The industry trends appears to be towards packaged systems that make use of two or more biometrics, comprising roughly 5% of the total biometrics market, making combinations such as fingerprint recognition and face scan. Such systems will probably be more dominant as customers recognise that a single biometric do not provide total accuracy.

On the other hand it almost seems to be a must to purchase and invest in biometric systems. There is a tremendous commercial pressure to purchase new surveillance equipment [Lyon, D., p. 675, 2003]. It is seen as a new business opportunity by some who have seen the share prices rise several times since September 11th. American security companies in particular are urging industries and governments around the world to make use of biometrics, taking advantage of the political climate of anti-terrorist activity.

It is rather noticeable that there is no pressure from governments to invest in these security measures but they are proclaimed by industry and private companies as the solution for our safety. Industry and private corporations especially seek customers from banks, motor vehicle officials and others as customers. They have been successful in persuading these private companies to invest in biometrics [Lyon, D., p. 670, 2003]. One can see that their pressure increasingly bears fruit, as many biometric systems are implemented in the public sphere [discos, swimming pools] as well as in the private sphere [monitoring employees, staff].
Peculiar of this scene of biometrics is that it is completely a non-political issue. There is hardly any debate on privacy in public, whereas we are affected by it in our daily lives. Citizens are not aware of the possible effects of biometric technologies. However as with all

these security systems, they are not invulnerable to attacks. Moreover we see that national legislation is lagging behind the technology, adjusting to the technological development, pressured by American authorities all under the name of: 'war against terror'.

3 Biometric Technologies

3.1 What is Biometrics?

Biometrics is defined as: "the statistical study of biological phenomena". 'The term is commonly used to refer to the identification or recognition of biological individuals by statistical means [Simpson, I., p. 1-3, 2006]. In practice this means that biometrics is the use of physical features of the body of an individual as a password to give one access to a bank, office, passport and one's information. Your body is used as an identifier for who you are in society.

Some features are harder to decipher by machines, for example the complexity of identifying an individual by their face. It is difficult to read a frown instead of a smile, which could lead to an incorrect identification. In contrast with the general notion; the majority of humans would find facial distinction straightforward, regardless of the facial expression.

3.2 Techniques and Applications

There are many biometric identification techniques currently in development and in use. Some of these technologies are likely to come in use widely in society due to political and security reasons. Biometrics is pushed by industries as a solution to combat identity theft, terrorism and for criminal identification. Biometrics can also be used in more day-to-day applications.

There are two types of biometrics: invasive and non-invasive. Invasive biometric technologies require the individual in question to perform an action in order to be identified [Simpson, I., p. 1-3, 2006]. Usually used for authentication. Techniques belonging to this category are for example: iris recognition and fingerprint recognition.
Non-invasive biometric identification does not require an individual's action. He or she doesn't even need to be aware that they are being identified; some of these techniques can even be applied at a later date. Such technologies are for example: ear recognition, gait recognition [identifying an individual by the way they walk], face recognition, voice recognition, and odour recognition.

In order to increase safety and reliability of biometric systems, some researchers encourage the use of two or more biometrics in a multi-model system. Various biometric technologies can be combined to create a multi-model biometric system [Langenderfer, J., Linnhoff, S., p.316, 2005]. Multi-model systems are technically more complicated and expensive; also they require more sensors, data and interpretations, therefore they are slower in processing. However the increased accuracy offered is gaining favour and is pushed ahead by governments.

3.3 Security Procedures

Biometrics is usually used as a security procedure. This can be classified into enrolment and authentication [Fleming, S.T., p.120, 2003].

Enrolment

During the enrolment phase, biometrics is obtained and linked to an identity of an individual. The identity is encoded and can now be stored, retrieved and matched. Some biometric devices store the data locally within the device itself. Individuals must enrol and authenticate with the same device. Other biometric systems allow the enrolled biometric data to be stored in a database that can be accessed from multiple locations. For example there are various controlled entry points, and there are many devices distributed over a wide area and many potential users. In this case the device allows retrieving the biometric data from a database and then performs comparisons. Data can be retrieved by a sensory device for example a fingerprint scanner, and the distinctive biometric characteristic can be identified.

Authentication

Authentication is the process of an individual claiming to have a certain identity. New information is compared to the stored data. Authentication can take place in two different ways: identification and verification.

Identification

Identification is when an individual's biological features are searched within a data set. This is a one-to-many search. For example if fingerprints are found at a crime scene, they are compared to fingerprints of all known delinquents stored in databases. The system returns all the closest matches to the individual. Identification is usually performed in a non-invasive context.

Verification

Verification occurs when someone claims to have a particular identity, for example to gain access to a high-security area. The biometric system compares the newly scanned data to a previously stored version. Thus the user's identity is then validated biometrically. This is a one-to-one search process. A direct comparison between the user's features and the data are matched. With a certain error margin it allows for minor temporal factors or sensor discrepancies.

As a general rule verification systems are considerably more accurate than identification systems, primarily because one-to-one comparisons are technically simpler than one-to-many.

In the following chapters I will describe the biometric technologies related to my case studies in more detail.

3.4 Fingerprint Authentication

"Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics, used to identify an individual and verify their identity [Wikipedia, May 2007]."

Fingerprinting is the most commonly seen form of biometrics used for authentication. It is especially known, because it has been in use for 100 hundred years, such as stamping palm and footprints on paper with ink to identify individuals. Justice and police used it in order to solve crimes [Haaster van, F., p. 11-12, 2003]. Therefore the fingerprint scanner has been well developed and is relatively cheap.

In 1998 the most sold biometric technology was the fingerprint recognition devices. This was a total of 78% of all the biometric sales [Smith, A.D., p.3, 2005]. It probably means that fingerprint recognition is considered most reliable by consumers, companies and/or government agencies than other recognition systems. Fingerprint recognition products are sold in such great quantities for probably two reasons: for tracking and identification purposes. Globally the fingerprint is used as one of the main methods in order to identify a potential criminal. The Federal Bureau of Investigation [the FBI] uses this technology to locate and track criminals internationally. Especially with an increase in security measurements, because of terrorism and other criminal activities, huge volumes of fingerprinting are streamlined and managed through computer information systems.

Moreover fingerprints are also used at crime scenes; if found at such a place, they are matched against database records. Prints that match to a certain level are taken as hard evidence, meaning that a suspect visited the crime scene. The fingerprints are often enough to assure a conviction [Anderson, p. 266-267, 2001].

A number of automated systems have been developed in order to cut the costs of manual fingerprint matching. Again others use fingerprint reading devices to authenticate people in real time for various applications, such as building entry control and benefit payment. In countries, such as India and Saudi Arabia, in which large proportions of the population have not benefited from formal education, the use of [ink] fingerprints is common. In the U.S. and Europe this system has not been implemented, because of the connotation with crime. However a few banks in the U.S. do ask non-customers for fingerprints when cashing checks. Surprisingly customer resistance is less than expected, especially if scanners are used instead of ink and paper.

Moreover it makes a whole difference, whether a fingerprint is matched against a whole FBI database [which is much larger and harder] or a common crime scene, which has [only]

hundred suspects. There are several initiatives to ban the use of fingerprints in the U.S. banking system because of privacy violations.

In the Netherlands finger- and hand geometry is applied in the Rotterdam harbour in order to admit truck drivers with load.

3.5 History of Fingerprint Identification

The use of fingerprinting for identification purposes has been discovered several times independently. In the seventh century fingerprints were used as a legal code as an alternative to a seal or a signature. In Japan the fingerprint was being used in the eight century if an illiterate man wished to divorce his wife. In the seventeenth century they were mentioned in Italian work by Malpighi. In 1691, Ireland fingerprints were used by 225 citizens to sign a petition asking for reparations [Anderson, p. 266, 2001].

During the mid-nineteenth century, the first modern systematic application of fingerprinting appears in India. William Herschel, a colonial official, used fingerprints to stop impersonation of pensioners who had died and to prevent rich criminals paying poor people to serve their jail sentences for them.
In the 1870s Henry Faulds, a medical missionary in Japan, discovered the fingerprinting system independently. He brought this system to the attention to Darwin, who consequently stimulated Galton to make a scheme and classify fingerprint patterns. Galton classified fingerprints in loops, whorls, arches and tents, which are still in use today.

Fingerprints are now being used worldwide by police. In the US, it is mainly used for identification. The FBI uses their files to check out arrested suspects or to determine whether there are people wanted by other law enforcement agencies. Fingerprints are also used to screen job applicants. Anybody who wants to have a U.S. Government clearance at Secret Services or other agencies must have a FBI fingerprint check. Fingerprints are also used in forensic crime investigations.

3.6 Fingerprinting Technology

Fingerprints are considered unique. The skin on the inside of a finger is covered with patterns of ridges and valleys. Therefore fingerprints are considered suitable for verification of the identity. Some fingerprint recognition systems do the comparison based on actual recognition of the pattern; however most of these systems only use specific characteristics in the pattern [Putte van der, T and Keuning, J., p. 5, 2000]. These characteristics are a consequence from the fact that the ridges in the fingerprint pattern are not continuous lines, but end in split forks, or form an island. These points are called minutiae. A normal finger consists of 100 such points or minutiae. A fingerprint that is scanned usually contains approximately 30 to 40 minutiae. When a fingerprint scan is

made, one makes use of the thickness and the width of the lines, the endpoints, branches, knots, loops and notches in the print.

A scanner is used to see the differences in light reflected by the ridges and valleys that make up the fingerprint. It makes very few flaws in reading the individuals' identities. This system has proven to be most effective and least costly of all forms of biometric systems.

The reliability of the fingerprint can be influenced negatively by wrongly placing the finger on the scanner [Wikipedia, May 2007]. Other factors could also play a role, such as dirt, cold, wet or wrinkled or cut fingers; they could have influence on the result of the measurement. The quality of the fingerprint also depends on gender, profession, and age. Some people are not recognised by the sensor, because the thickness of the line is not sufficient. Other problems with this system are that it may carry germs and other harmful organisms, since there is a continuous physical contact with the scanner interface [Smith, A.D., p.5, 2005].

Fingerprint Scanner
A fingerprint sensor is an electronic device that captures digital images of fingerprint patterns. The captured image is called a live scan. The results of the scan are represented in grey scales, which are converted to a black-white scale for better readability. The scan is digitally processed in order to create a biometric template which is stored and used for matching. A template is a reduced piece of information of someone's biometrical data.

3.7 Face Scan

A facial recognition system is a computer-driven application for automatically identifying a person from a digital image. It does that by comparing selected facial features in the live image and a facial database [Wikipedia, May 2007].
It is mostly used for security purposes. This system can be compared to other biometric technologies such as fingerprint or iris scans.
One can see an increasing trend of facial recognition systems being applied in situations where identification of people is necessary, but where the identification process has to be automated in order to save manpower and time. Several pilot studies with cameras have been set up to monitor shops and city centres, where one searches automatically for well-known offenders. Also Schiphol uses the facial recognition system at the customs. Since 2005 the Dutch government has been involved in a pilot study called 2 be or not to be; experiments are conducted with passports in which biometrical characteristics are registered, including facial characteristics.
The high unreliability of existing systems makes it clear that these systems have hardly found any real acceptance in monitoring 'really important' installations. Moreover the facial recognition system is usually not used as the only technique for surveillance. Therefore the Dutch biometric passports have been adapted in advance; the passport photo must be taken from the front and not any other angle. The personal registration process digitises the

passport photos for future use. In this manner these surveillance cameras could monitor, recognise and follow 'potential terrorists' and other individuals.

3.8 History of Facial Recognition System

The first computer to recognise human faces was developed during 1964 and 1965. The pioneers of this automated facial recognition system were Woofy Bledsoe, Helen Chan Wolf and Charles Bisson. An intelligence agency funded this work, but did not allow much publicity.
The technology works as follows; a large database of images and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The difficulty with this system was the recognition problem, because of the "great variability in head rotation and tilt, lighting intensity, angle, facial expression and aging etcetera. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation [or pattern matching] of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations" [Wikipedia, May 2007].

3.9 Efficacy and Reliability

Facial recognition is not the most reliable and efficient technique among the different biometric technologies. Its advantage is that is does not require any aid from the user. If a system is designed properly it could detect the presence of criminals among crowds. Other biometric techniques such as fingerprints, iris scans and speech recognition cannot perform this form of mass scanning. However it is not considered as a very reliable technique and questions have been raised about the effectiveness of facial recognition software in cases of railway and airport security.

3.10 Secure Access Road B.V.

Company
Secure Access Road BV [SAR BV] was founded in 2001 and has an office nearby Rotterdam, in Puttershoek. SAR BV has implemented various biometric bases access systems in several companies in different branches of industry.
SAR BV is the provider of biometric based access systems. In combination with biometric technologies they develop several applications which allow the customer to see time and attendance, customer loyalty and electronic payment. The main links between these applications are stored on a smart card.
SAR BV has several partners such as Alcazar Pleasure Village and B+P Computersystems. In 2000 these two parties aimed to develop a biometric access control system for the catering industry in order to keep out troublemakers.

The biometric engine of their systems are built and maintained by BioWise, one of the leaders in the field of biometric technology. SAR BV's hardware is developed and maintained by B&P, an Authorized Compaq Reseller and ISO 9002 Certified company.

SARFunGuard Totem

SAR BV presents the SarFunGuard Totem [SAR totem] as a total solution for a secured entrance. The SAR totem allows people to register and verify themselves. During the registration and verification processes the totem assists people audio-visually. The totem gives instructions, supported by voice-overs in four languages: Dutch, English, German and French.

As soon as the user inserts a smart card into the totem a registration or verification starts. If the totem is out of use, the system gives information, such as advertisements and toilet directions.

The totem supports the following [biometric] techniques for access control:

- Electronic fingerprint recognition
- Electronic facial recognition

These techniques can be used in combination or separate from each other. While registering, one has the possibility to make one or more fingerprint scans with the electronic fingerprint recognition system. When verifying ones identity the system can randomly ask to put for one or more fingers on the scan. This increases the reliability of the system.

Another possibility is to make use of the electronic fingerprint recognition in combination with the visitor's four digital photos. The biometric fingerprint identity is checked by the system and not that of the face. The visitor's photo appears on the screen; a guard usually determines whether the person on the photo is the visitor, he or she claims to be.

SarFunGuard Software

Here I will describe the main and essential modules which the administration software package contains. The SAR administration package consists of various modules, which can be linked with each other independently.

Personal Data Module

SarFunGuard [SFG] 'personal data' module consists of an essential part of the administration package. This module links the personal data with the person's biometric data. This module also gives an overview of the visitor's visiting pattern. Moreover it is possible to make changes manually.

Search Module

Another essential module 'search' makes it possible to effectively search and find one or more people, by filling in one or a combination of data; such as first name, last name, gender, zip code, place, mobile number, visiting group. The results can be produced given

per visitor, if there are several search results one can go through a 'photo album', so that the person in question can be found. Moreover there exists an advanced search engine. For example, when one is searching for a person, without knowing any of their personal data, but one does know that the visitor came in around 10.00 p.m. In such a case one can fill in the time and look for all the women who came in between 9.45 and 10.15 p.m. All results will be given in a photo album.

Blacklist Module

If one is confronted with people who are misbehaving or troublemakers, then one can put these people on a so-called blacklist. The blacklist is a list with visitors, who are banned to enter a location for a certain period of time [or forever]. One has total control over the blacklist and one can determine which troublemakers you want to keep out of the door. The blacklist module works closely together with the search module, so that one can quickly find a person and put the visitor on the blacklist. As soon as someone is on the blacklist, the visitor cannot enter the location of concern. The system automatically blocks the possibility to create a new card. In this way the system tries to create a safe environment by keep 'nuisance' out of the door.

Statistics Module

By making use of this system, one can read trends and statistics. One can see the visitors' age, demographic and gender compositions etcetera. Everything is shown in various diagrams and statistics.

Various Modules

There are several other modules included in the administration software package, such as sticker, smart card administration, the sms module, credits module etcetera.

Sticker Module - In order to take care of the mailing, one can directly print addresses; this is possible by region or zip code. Everybody receives an invitation or flyer with for example the agenda, people on the blacklist will be automatically disregarded. There is a special birthday invitation.
Smart card Module - With the smart card module one can read, copy, erase and write smart cards.
SMS Module - The SMS module makes it possible to send a SMS at any time to people who are included in this module, depending on age, gender and or target group.
Credits Module - It is also possible to earn credits. For instance VIP members can earn 50 credits, while 'normal' visitors can only earn 10 credits per visit. Moreover one can stimulate visitors to come earlier, by rewarding them with more credits. By stimulating visitors to come earlier, one can generate more income. It is also possible to make an action stunt by asking members 100 earned credits for a free entree. In this case 100 earned credits are deducted from the total. This makes it for the visitors that every visit becomes worth money.

Linking to the Internet

People registered in the administration package can have access to the website with a login. Some areas might only be accessible for members such as: the guestbook, forum, photo album and the chat box. It is also possible for the user to buy tickets and other merchandise from the web-shop. It can stimulate and attract smart card members to the website. One can even link the earned credits with the web-shop and get discounts on products and tickets. It also gives the end-user the possibility to control his/ her date and time of visit, history, earned credits and more.

3.11 Smart Card

A smart card is a plastic card with a microprocessor chip. It consists of a memory, the CPU and some contact points. Smart cards are contact cards with a chip, comparable with a bank card. It is also called chip card and can be defined as a pocket-sized card with embedded integrated circuits, which can process information [Wikipedia, May 2007, SAR, May 2007 and Fleming, S.T, 2003].
. This means that the smart card can receive input which is processes and delivered as output. It is being used by banks and the purchasing costs are relatively low.

The oldest card has a memory of 8K, now we can see cards with 512K. This increasing memory capacity is necessary in order to enhance security. The largest producer of chip cards is Gemplus. Gemplus produced more than 5 billion chip cards in 2004. In 2006 Gemplus and Axalto fused in to Gemalto. There are over 200 types of chips.

3.12 History of Smart Card

The chip card was invented in 1968 by a German scientist Helmut Gröttup and his colleague Jürgen Dethloff. The chip is actually a mini computer. In 1982 the technology was patented. Modern chips are increasingly being produced with a bigger memory.

It was firstly used as a payment in French pay phones, starting in 1983. From the mid 90s throughout Europe smart card based 'electronic purse' systems, [in which value is stored on the card chip and not in an externally recorded account, so that the machine accepting the card don't need any network connectivity], were tried out, in the Netherlands known as the Chipknip and Chipper.

A major boom came in the 90s, when the smart card based SIM used in GSM mobile phone equipment was introduced in Europe. Since the mobile phone is widespread in Europe, smart cards have become very common.

Also smart cards are broadly used as payment cards by big international payment brands such as MasterCard, Visa and Europay.

Smart cards are also introduced as personal identification cards at regional, national and international levels, such as in citizen cards, drivers' licenses, patient cards. It is also becoming more common that contactless smart cards are integrated in International Civil Aviation Organisation [ICAO], biometric passports to enhance security for international travel.

3.13 Smart Card

A smart card is a chip card; it can be compared with a magnetic stripe card, in which information is stored on memory chip card. The card can be secured. The cards without security are for example phone cards. The smart card is not just composed of a memory, but also of a microprocessor, which makes it possible to communicate and make calculations.

Secure Access Road BV [SAR BV] also uses the smart card for its solutions. The card is being used to speed up the verification processes and ensure reliability. Moreover the cards can be used as a facility card, parking card and more. The smart card has the chip on the card. The card needs to be inserted into the reader. Moreover it can save the information in code.

The smart card technology is usually used to provide further privacy assurance to the individual. Their public/ private key pair could be embedded on the smart card along with the encrypted copy if the biometric template. This means that the biometric data has been reduced to a template and not an original copy of the biometrical data. When one enrols into a biometric system, the key pair is generated and the enrolled biometric template encrypted with the public key. On entering, the enrolled biometric is decrypted by the smart card using the private key and is then uploaded to the biometric device and compared and matched.

There are still vulnerabilities involved with this system. In order to break the security of the system, an attacker must substitute an encrypted version of the biometric template both within the database and within the smart card [Fleming, S.T., p. 131, 2003]. The private key must also be obtained in order to decrypt the template or break the public-key cryptography. In order to fool the system, the attacker would have to steal the smart card and present cloned or copied biometric data to the scanner. However the risks of these attacks are lower, because the raw biometric data has never been exposed, it is always encrypted. Moreover as soon as the loss or theft of a smart card has been discovered, the encrypted biometrics can be erased.

3.14 Radio Frequency Identification

The Radio Frequency Identification [RFID] is a small chip, which can be read from short distances. These information systems consisting of RFID chips exchange data with an RFID-reader at radio frequencies. RFIDs mostly used in logistics in order to identify cargo, is

currently entering into the public domain on a massive scale to recognise people. We see this technology in employee ID cards/tokens, clubs and football stadiums, the pubic transportation cards [OV-chip card], the biometric passport, all sorts of local pay and access systems and tracking systems in amusement parks.
RFID has been in use since the Second World War. Since then the market has only been growing. According to IDTEchEX 2.5 billion chips have been sold since the past sixty years, of which 600 million chips have been sold in 2005. One expects a sale of 1.3 billion chips in 2006. Main applications of RFID tags are tags in freight and smart cards. RFID is also called the 'Internet of things', using radio waves to automatically identify and track individual items.

RFIDs are the next generation of the barcode. It creates a variety of interfaces that can directly connect computers to individual physical items and even to people [ITU, p.6-7, 2005]. An example of one of the largest RFID networks in the world is the JOINT Asset Visibility [JTAV] network built by the US military to track military supplies globally, using RFID tags and GPS locators.
RFID tags have the capability to contain almost anything from item location and pricing information to washing instructions, banking details and medical records. RFID is also being implemented under the human skin [my case study] for the purpose of authentication, location and transaction and under the consideration as a mechanism for tracking bank notes and passports.

Nowadays we can see that the RFID has become a part of ordinary life: a person going to work by public transport, taking a car to shopping. The RFID displays an identity of this person to gain access to services. In return the maintainer of the RFID environment receives valuable information on this person. On access the first question is usually asked: is this person allowed here? Once the systems are implemented and the databases start running, they provide much interesting information, sometimes even more than anticipated. Profiles start to emerge on movements, spending, productivity, preferences, habits and so forth ['t Hof, p.1, 2007].

3.15 History of RFID

Radio Frequency Identification [RFID] has been in use for many years already. It is the technology used in cats and dogs [identification chips] and electronic door keys for offices and cars. However a few years ago RFID became a hype, especially in the supply chain [Plaggenborg, p. 9, 2006]. It first emerged during the Second World War. It is a combination of radio technology and radar. The 'identification of friend or foe' [IFF] program saw the first type of identification tags in military aircrafts and tanks used by the British, reading units could query whether to attack or not [ITU, p.6, 2005, Jechlitschek, p. 2, 2006]. These systems and related ones send coded identification signals by radio. Thus an aircraft that sends the right signal is a friend and the rest are foe. Accordingly the radio frequency identification was born [Garfinkel, Holtzman, p. 15, 2005]. Harry Stockman was maybe the

first person to explore RFID in his work 'Communication by Means of Reflected Power' in 1948. He realised that it was possible to power a mobile transmitter completely from the strength of a received radio signal, introducing hereby the passive RFID system. In the 1950s RFID techniques were further explored, due to the development of radio and radar. In the late 60s, nuclear and other hazardous materials were started to be identified and monitored by radio frequency. The first commercial RFID application was the 'Electronic Article Surveillance' [EAS], developed in the 70s as a theft prevention system. It was based on tags that could store 1 bit. This could be read when customers would leave the store; the alarm would go off then, if the bit was not unset. In the end 70s RFID tags were used for animal tagging. The first patent on RFID originates from 1973 for a passive transponder with memory. Since then and the 80s work on RFID began to grow, when developers, inventors, companies, universities, governments actively developed RFID applications in laboratories.
In this period RFID technology aimed at reducing its costs and size. It also tried to enhance its power requirements and communication range. This all led to a mass market for RFID. At the end 90s millions of RFID tags were implemented into applications such as toll roads, entry access cards and container tracking. Since then all sorts of RFID applications have emerged together with new applications such as RFID in athletics; it has become widespread and has become a part of our daily life.

3.16 RFID Technology

Here I will describe how the RFID technology works and what parts it consists of. It shows a few important values.

To explain RFID technology in simple words: it is a way to identify a person or an object using electromagnetic radiation. RFID enables the automated collection of product, time, place and transaction information. Frequencies used are usually 125 kHz [low frequency], 13.56 MHz [high frequency] 0r 800-960 MHz [ultra high frequency]. RFID tags in general consist of four basic elements: the tags, the RFID readers, the antennas and the option of radio characteristics and a computer network [if used] to connect the readers [Garfinkel, Holtzman, p. 16, 2005].

Tags

A tag is one of the basic components of RFID. Each tag consists of an antenna and a microchip that contains a radio receiver, a radio modulator that sends a response back to the reader, some amount of memory, control logic and a power system. The power system can be activated by an incoming radio frequency signal, also known as passive tag. On the other hand the tag's power system could contain a battery; in this case the tag is active [Jechlitschek, p.4 2006, Garfinkel, Holtzman, p.17, 2005]. Most tags are only activated when they are in a particular zone of the reader. When outside that area the tags are dormant. The information on the tag can be received and read by readers. This can also be attached to

a computer containing the relevant database. Accordingly this database can be connected to the company's Intranet or even to the Internet.

Passive Tags

The passive tag is much smaller and cheaper than the active tag, because they don't have any batteries integrated. This tag relies on the power generated by the reader. It means that the reader has to be active until the transaction is completed. Its reading range is very limited; it ranges between 2mm and a few meters. Another benefit is that the passive tag can be produced by printing. Furthermore these tags have a longer life; an active tag [with battery] lasts only for a few years, but a passive tag can still be read many decades after the chip's production.

Semi-passive Tags

In between the passive and active tags, one can also distinguish the semi-passive tag. This kind of tag has an internal power source [a battery] that keeps the microchip powered at all times, like the active tags, but it does need a reader's power in order to transmit a message back to the RFID reader. Since the chip is always powered it can respond faster to requests. This is especially useful when a large number of tags need to be queried per second. This means that this tag has the reading reliability of an active tag and the reading range of a passive tag. They also have a longer life than a fully active tag. Additionally its reading range is wider than the passive tag.

Active Tags

The active tag contains an internal power source, powering the microchip and generating a signal on the antenna. This type of tag on the other hand has two main advantages compared to the passive tag; its broader reading range and its reliability. With a proper antenna on the reader and the tag, a 915MHz [ultra high frequency] tag can be read from a distance of about 30.5 meter or even more. This is ideal to locate objects and it can also serve as landmark points. Moreover these tags are more reliable, because they don't need a constant radio signal to activate their electronics. The lifetime is approximately up to 5 years.

Tag Characteristics

Tags come in all sorts of shapes and sizes. Most tags are not bigger than grain of sand [less than 0.3mm] and are typically embedded inside a glass or plastic element [ITU, p.5, 2005]. One of the smallest chips ever produced is the Hitachi mu-chip, which is smaller than 0.4mm on each side [Garfinkel, Holtzman, p.17, 2005]. This type of tag is used for a piece of paper and tracking documents, which can easily be printed in an office environment. This type of chip can only be read at a distance of a few centimetres. The mu-chip is a passive tag. Another small tag is the implantable tag, the size of a rice grain, manufactured by VeriChip. These tags are passive tags with a very limited reading range. The idea behind this application is to give machine-readable serial numbers to people. Later in this part I will go further into this type of RFID chip. RFID tags can be promiscuous, meaning to say,

that they will communicate with any reader. Tags can also be secure; this means that the reader has to provide a password or another form of authentication before the tag responds [Garfinkel, Holtzman, p.18, 2005]. However majority of the tags that are in use are promiscuous, since they are cheaper. Moreover the systems are also easier to manage. Tags that use passwords or encryption codes have a difficult management problem, because the codes need to be distributed in advance and properly controlled.

Readers

The RFID reader reads transmitted data with either a handheld device or one embedded on the wall. The reader is a read-only or a read/write device. The reader scans tags and then forwards the information to the backend [Garfinkel, Holtzman, p. 20, 2005, Jechlitschek, p.5, 2006]. The backend is usually a database. This database can then also be connected to a company's Intranet or the Internet. The response sent back contains the tag's serial number and generally other information as well. This system behaves in the same way as a barcode reader; if the reader scans the barcode [at for example the checkout point in the supermarket] the application uses the derived identifier to lookup the current price. In addition the backend provides the discount information; it also decreases the amount of products available and notifies the manager if the number falls below a certain limit.

Implantable RFID Tags

VeriChip is a company specialised in implantable RFID microchips. VeriChip is the first company in the world to offer such a chip for the purpose of automatic identification. The FDA has approved the implantable radiofrequency transponder system for patient identification and health information.

The microchip measures 12 mm long and 2.1 mm in diameter, roughly the size of a grain of rice. The device is usually implanted above the triceps in the arm or sometimes in the hand. It is inserted just under the skin and contains a unique 16-digit identifier. The insertion procedure is performed under local anaesthetics. An accomplished doctor can complete the procedure in less than 20 seconds. It is invisible to the eye. The chip doesn't contain any other data than the unique electronic ID, nor does it contain any Global Positioning System [GPS] tracking capabilities. The idea is that with this identification method one cannot lose, misplace or get one's ID stolen; one 'carries' is always with you. The estimated lifetime of a VeriChip is over 20 years.

Once it is inserted under the skin with a syringe, via a quick outpatient procedure, the VeriChip can be scanned with a handheld or wall-mounted chip reader. The microchip is passive; this means that the chip will only be activated when a reader with the proper frequency responds to the dormant chip, which then emits a radio frequency signal, transmitting the individuals' unique verification number. This number can be used to access personal medical information in a password-protected database or assess whether someone has authority to enter into for example high-security areas.

At first 68 hospitals in the US had signed up to adopt the technology in their emergency rooms, but many have already abandoned the trials because of lack of acceptance and privacy concerns. VeriChip estimates that around 2000 people currently have a VeriChip

worldwide. A surveillance company in Cincinnati became the first American business to use the VeriChip for access to its data-center.

3.17 VeriChip

While VeriChip argues that the RFID tag can play and important role in the healthcare sector, it also makes potential users more vulnerable to privacy loss. The company says that the chips can be used to authenticate people in high-security environments. 'The advantage' of this system unlike the password, is that the implanted chips cannot be easily shared [Garfinkel, Holtzman, p.17, 2005].

3.18 VeriChip Usage

Healthcare Sector

The VeriChip is especially useful for hospitals where the staff occasionally mixes up patients and gives them wrong treatments. VeriChip primarily functions as a tool for managing patient information. The chip allows healthcare professionals to quickly and accurately retrieve critical patient information. The device, containing a unique serial number, is linked to the patient's database maintained by a hospital. Typically the database information would contain information as the person's name, address, current medications, known allergies and critical medical history. People who could benefit from a VeriChip include anyone with impaired speech, memory loss, or chronic loss of consciousness. These conditions barrier the communication, leading to delayed treatment or result in medical errors. In this way the VeriChip fills a possible information gap in the healthcare sector and could be considered as a preventive tactic.
VeriChip also claims that the implanted chip can be useful for identifying wandering Alzheimer patients who go out without any identification, not knowing their location or destination.

Financial Security

Moreover the VeriChip could increase a person's financial security. Almost fifty percent of all debit-card fraud happened when a card is stolen by someone who knows the PIN of the victim. With a VeriChip linked to a credit or debit card, card readers equipped with a scanner would authorise transactions if the matching VeriChip is in range. Thus without having the correct VeriChip one cannot make use of a stolen debit card.

High Security Areas

The VeriChip is also used for security purposes for high-value areas. The Mexican government is using the VeriChip to control access to offices storing sensitive information. Only high-level officials with a VeriChip implant will be able to enter these high-security areas. Until now 18 government officials have been implanted with a VeriChip.

Disasters

Another recent application of the VeriChip is in the field of the mortuary science. In order to obtain the remains of your loved one's quickly and bring closure, the RFID chip could help morticians match and identify victims faster and get their remains back to the family. This is especially an interesting application with environmental disasters occur, such as Katarina. The VeriChip can be used to keep track of human remains, speed up the morgue management and reduce morticians' errors.

3.19 Company

VeriChip provides security solutions for organisations/ companies. Their applications make them predominant in RFID solutions provider in the healthcare industry. These technologies identify and locate people by infant protection, wander prevention, asset tracking and patient identification applications. VeriChip systems have been installed in over 4000 locations worldwide in various sectors, such as in healthcare, security, industrial and government market. They are the first in the world making RFID for people.
As VeriChip states, "their roots trace back to the events of September 11 2001, when New York firemen were writing their badge ID numbers on their chests in case they were found injured or unconscious. It was evident that there was a desperate need for personal information in emergency situations and that an injectable RFID microchip could help patients [VeriChip Corporation, May 2007]".
In December 2001 VeriChip was created to produce and market the implantable device [also known as VeriChip]. In December 2004, the company received approval from the United States Food and Drugs Administration [FDA] for the device in medical applications [FDA, 2004]. Two medical centres Beth Israel Deaconess and Hackensack University have agreed to use the technology in their emergency departments.
VeriChip fulfils its leadership position as the world's first RFID company for people offering a wide range of RFID solutions: implantable, wearable and attachable. They produce human-implantable RFID microchips to active RFID tag with skin sensing capabilities. In April 2004 the wearable RFID innovation had been developed especially for infant protection, wander prevention and asset tracking. It is a non-implantable RFID technology. In June 2005 a vibration monitoring system for regulated vibration control had been acquired.

VeriChip is majority-owned by Applied Digital Solutions of Delray Beach, Florida. It trades on the NASDAQ under the symbol "CHIP".
According to an article the United Sated currently has 50 people with a VeriChip implant. This is very low; however worldwide there are hundreds of people chipped. The VeriChip corporation ships more and more to hospitals and businesses, the number of VeriChip implants will continue to grow.

3.20 Vulnerabilities of Biometric Technologies

False Acceptance and False Rejection

Imagine a situation in which different individuals are granted access to some area and some are not. In order to gain access to that particular area one needs biometric data from an individual, which is compared with biometric data from a previously enrolled individual and next a decision is made whether or not to grant access [Simpson, I., p.4-5, 2006, Langenderfer, J., Linnhoff, S., p.326, 2005, Fleming, S.T., p.121-124, 2003] . If a biometric has been registered for that individual and the feature matches with sample presented, then access should be granted, otherwise not.

The most optimal biometric technology would be one which always correctly identifies an individual. However to come close to the best performing systems one should consider speed and accuracy. Moreover this process does not always go as smooth as it should.

When using a biometric technology, there are two types of errors involved:

1. False rejection: this is when a person is wrongly denied access
2. False acceptance: this means when an impostor is accepted by the biometric technology

False Rejection

A false rejection [or false negative] is a situation where an individual presents their biometric data and the device does not match correctly with the enrolled data. This could occur if there is a major change in the form of the biometric since enrolment, imprecise measurement by the device or a major difference in the environment during the enrolment and acquisition process. This false rejection is particularly inconvenient for the individual concerned. Usually one would need to repeat the presentation of the biometric, multiple times, before the correct match is obtained or in more extreme situations one would have to repeat the enrolment process to have their data restored in the system.

False Acceptance

A more serious situation is that of a false acceptance [or false positive]. In such a situation a person is granted access, where he or she should not be allowed. This leads to a system failure, breach of the security system and a situation one wants to avoid. For example with a fingerprint scanner comparing a greater number of minutiae would tend to have a more accurate match, comparing fewer minutiae would result in a less precise match. It is of great importance that the false acceptance rate should be reduced, so that the potential for breaches of security are reduced. This is usually done at the expense of the individual's convenience. The end-users may have to present biometric data multiple times for authentication or repeatedly enrol biometric data. The level of inconvenience could impact the usability of the system in terms of user satisfaction.

Comparison of Techniques

Here is an overview of all biometric technologies compared with one another, looking at various aspects:

Uniqueness: How well does a biometric separate one individual from another?

Permanence: How well does a biometric resists aging?

Collectability: How easy is it to acquire a biometric measurement?

Performance: How accurate, fast and robust is the system in capturing biometric?

Acceptability: How high is the approval, acceptability of a technology by the public in everyday life?

Circumvention: How easy is it to fool the authentication system?

Biometrics	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	Low	Medium	High	Low	High	Low
Fingerprint	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	High	Medium	Medium	Medium
Keystroke Dynamics	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	Medium	High	Low	High
Retina	High	Medium	Low	High	Low	High
Signature	Low	Low	High	Low	High	Low
Voice	Low	Low	Medium	Low	High	Low
Facial Thermogram	High	Low	High	Medium	High	High
DNA	High	High	Low	High	Low	Low

Table 1: Comparison of Biometric Technologies

Higher scores mean a better performance for all criteria except circumvention. Each technology has its strengths and weaknesses. The fingerprint recognition is both fast and unique, although the majority of the systems can be outwitted. On the other hand a technology such as face recognition is hard to by-pass, but has a lower performance. Thus it is important to choose a particular biometric technique carefully, taking all relevant factors into account.

3.21 Is Biometrics Foolproof?

Biometric technologies can be fooled. There are different ways to outsmart biometric technologies, called: digital spoofing and physical spoofing.

Digital Spoofing

Digital spoofing involves presenting an image of a legitimate user to a biometric sensor. For example if a biometric identification chip contains information related to a subject's finger, then the perpetrator could create a model of the relief for his hand and impersonate the

subject, pretending to be the person in question. It is widely publicised that there have been many successful efforts to fool fingerprint scanners by presenting fake fingers, using melted gummy bears and silicone fingers with a mould of the original fingerprint pattern embedded. Voice recognition could be easily fooled with a playback device. While with human intervention one could ensure that no playback device is used to fool a voiceprint sensor.

Physical Spoofing

Biometric technologies can also act as an 'informant'. This means that any biometric data on a real document can be modified to match that of the impostor. The false biometric data verifies the impostor's identity and he or she can pass through the various security systems without any problems.

3.22 Other Disadvantages

Cost

Biometric systems are quite expensive; the cost of implementing a large scale system is much larger than simply using an individual password. However the cost of these systems has been dropping in the past few years, as the industry has grown drastically. The prices are fairly stable now.

Disadvantages related to VeriChip

Problems which could occur with VeriChip are when companies use these databases to track consumers or build extensive profiles about them. This information is not only attractive for identity thieves, but also for companies, wanting to analyse consumers. People should be aware of the risks involved with the VeriChip, which is the possible reduction in personal privacy [Laczniak, S., p.14, 2006].

4 Methodology

4.1 Qualitative Research

Qualitative research is an investigative methodology. It involves an in-depth, comprehensive understanding of human behaviour and the reasons that govern human behaviour. It tries to investigate the why and how of decision making and tries to understand people's interpretations [Key, J.P., Oklahoma State University, 1997]. Therefore when conducting qualitative research a smaller and focused samples are required. Detailed data is gathered usually through open-ended questions that provide direct quotations. The human is the primary collection instrument. The interviewer is an integral part of the research. Research is usually conducted in the natural environment under natural conditions. Data derived from these case studies are then categorised into patterns, a way to organise and report results. When conducting a qualitative research, one seeks a wide understanding of the entire situation. During the research different theories evolve. The idea behind qualitative research is to gain 'real', 'rich', and 'deep' data. Data gathered from qualitative research are perceptions of the people in a certain setting.

4.2 Case Studies

Case studies are detailed investigations of individuals, groups, institutions or other social units. When a researcher decided to analyse a case study, one focuses on an individual case and not the whole population of cases. The focus doesn't lie on generalisation, but on understanding the particulars of the case. A case study focuses within a certain frame, usually under natural conditions, so that the system can be understood in its own circumstances.

4.3 Empirical Research

When I started with my research, I firstly decided my cases studies. I had read several articles about recent developments regarding biometric technologies in public spaces. Biometrics are implemented in various places, but mostly one encounters these technologies in private companies. These case studies are particularly interesting, since they are the first public spaces in the Netherlands, where biometric technologies have been set up for security reasons. All three case studies have been heavily represented and publicised in the media. In total I chose three case studies.

My case studies concern three different settings:

1. A disco in Puttershoek, where a finger scan and face scan are taken
2. A swimming pool in Ridderkerk, where they also use the same biometric technology at the entrance
3. A disco in Rotterdam, where VIP – members can implant a RFID -tag in their bodies

Another reason for me to take these three case studies is because information is extracted in various ways from the end-users. In the first two cases, the body becomes data. In the third case data is inserted into your body, by injecting an implantable RFID-tag. This is an interesting contrast, which makes it especially provocative to look into future developments and implications of these technologies.

4.4 Time Period

I have conducted the interviews over a time span of 8 months, first starting in May 2006 until July 2006. The next set of interviews was conducted from September 2006 until November 2006. I conducted one last interview in February 2007. The time span of my research has taken up a long period, since it was difficult to find respondents for the case study in the Baja Beach Club.

4.5 Data Collection

The next step was to look at the approach of these case studies. I was particularly interested to look at the effects of these technologies on end-users and conduct a field study. I decided to look at the three case studies from three viewpoints. I looked on three levels at the industry chain of biometrics. Therefore I first interviewed people from the production and supply end [the producers and suppliers of biometric technologies]. Next I interviewed their clients. At last I interviewed the end-users of the technologies of each case study. This in order to answer my main question: Which functions do biometric technologies take in society and how do end-users eventually internalise these technologies?

For this research I did a qualitative research. My three case studies are a disco in Puttershoek; here they have implemented a biometric entrance system. The device scans the face and fingerprint.
My second case study uses the same system at the entrance; it is a swimming pool, De Fakkel in Ridderkerk.
In my last case study implanted chips are used for VIP customers to enter the well-known Baja Beach Club based in Rotterdam. Beers are paid via the implanted chip.

At the first level I interviewed LogicaCMG, Dartagnan and Secure Access Road B.V.
On the clients' level I interviewed Secure Access Road B.V., the managing director of de Fakkel – the swimming pool in Ridderkerk and Conrad Chase, one of the directors of the Baja Beach Club.
At last my intention was to interview ten end-users of each case study. At the end I interviewed ten young people at the disco in Puttershoek and one guard. Next I interviewed seven adults in the swimming pool, six women and one man. I also interviewed nine young people at the swimming pool, because they belong to the target group regarding the biometric device at the entrance. For my last case study – the Baja

Beach Club, I was able to interview only five chipped people; three of the respondents were working for the Baja, the other two were VIP members. I tried to interview more people, but the Baja Beach Club was reluctant to ask her members for my research. They didn't find any respondent who were willing to cooperate with my research. I went a few times to the Baja Beach Club itself to find chipped members, but every time I was there, there was only one chipped member present. Moreover they were about to stop the whole chip implant VIP-membership program.
For all my case studies I went to interview the end-users at the location of concern.

I conducted the interviews in an informal way. The idea was to conduct a semi-structured, open-ended interview. I had a list of questions as a guideline. The respondents on the suppliers and client level were able to tell a lot around the questions, I hardly needed my interview guideline. However upon interviewing the end-users, they were restricted in their answers. This could be due to several reasons:

- Most of the respondents were young people.
- Most of the respondents wanted to swim or dance and not 'waste' a lot of time in an interview.
- Most of the respondents didn't have many opinions about the entrance system, so discussion around the topic was out of question.

During the interviews I made rough notes of the respondents' replies, answers, remarks, comments, explanations and observations. I used these notes to transcribe the most meaningful important and outstanding [according to my own interpretation] responses.

4.6 Limitations

The problem with case studies is that it is probable that one cannot generalise it to complete populations. It is solely representative for the three case studies itself. However certain patterns can be read from the respondents' answers, which one could also imagine to be applied on similar settings. Moreover the researcher's interpretation could also play a role in objectivity. The researcher could give a different meaning to a certain answer than another researcher, when conducting the same research, which could lead to different conclusions of the whole study. Therefore the subjectivity of the study could lead to difficulties in establishing the reliability and validity of the approaches and information. It is also difficult to detect the researcher's bias.

5 The Case Studies

For this research I did a qualitative research. In total I have three case studies. I looked on three levels at the industry chain of biometrics. At first I interviewed producers and suppliers of biometric technologies. Next I interviewed their clients. At last I interviewed the end-users of the technologies.
This in order to answer my main question: *Which functions do biometric technologies have in society and how do end-users eventually internalise these technologies?*

My three case studies are a disco in Puttershoek; here they have implemented a biometric entrance system. The device scans the face and fingerprint.
My second case study uses the same system at the entrance; it is a swimming pool, De Fakkel in Ridderkerk.
In my last case study implanted chips are used for VIP customers to enter the well-known Baja Beach Club based in Rotterdam. Beers are paid via the implanted chip.

At the first level I interviewed LogicaCMG, Dartagnan and Secure Access Road B.V.
On the clients' level I interviewed Secure Access Road B.V., the managing director of de Fakkel – the swimming pool in Ridderkerk and Conrad Chase, one of the directors of the Baja Beach Club.
At last my intention was to interview ten end-users of each case study. At the end I interviewed ten young people at the disco in Puttershoek and one guard. Next I interviewed seven adults in the swimming pool, six women and one man. I also interviewed nine young people at the swimming pool, because they belong to the target group regarding the biometric device at the entrance. For my last case study – the Baja Beach Club, I was able to interview only five chipped people; three of the respondents were working for the Baja, the other two were VIP members. I tried to interview more people, but the Baja Beach Club was reluctant to ask her members for my research. They didn't find any respondent who were willing to cooperate with my research. I went a few times to the Baja Beach Club itself to find chipped members, but every time I was there, there was only one chipped member present. Moreover they were about to stop the whole chip implant VIP-membership program.
For all my case studies I went to interview the end-users at the location of concern.

I conducted the interviews in an informal way. I had a list of questions as a guideline. The respondents on the suppliers and client level were able to tell a lot around the questions, I hardly needed my interview guideline. However upon interviewing the end-users, they were restricted in their answers. This could be due to several reasons:

- Most of the respondents were young people.
- Most of the respondents wanted to swim or dance and not 'waste' a lot of time in an interview.

- Most of the respondents didn't have many opinions about the entrance system, so discussion around the topic was out of question.

During the interviews I made rough notes of the respondents' replies, answers, remarks, comments, explanations and observations. I used these notes to transcribe the most meaningful important and outstanding [according to my own interpretation] responses.

5.1 Alcazar

Puttershoek

Puttershoek is a village close to Dordrecht in the Hoeksche Waard. It belongs to the Binnenmaas municipality. Binnenmaas consists of six villages. Binnenmaas has a total population of 19636 [from CBS statline, 2006]. There are in total 454 non-Western immigrants, which is 2.3% of the total population. The majority of the non-Western immigrants are from Surinam [0.6%].

People of the villages mostly live in Binnenmaas, they go shopping, go to school, they participate in clubs, and they sport and entertain. Not many people work in the villages, only at the outskirts or at business locations. The majority of the people work outside the municipality or even outside the Hoeksche Waard [Binnenmaas, April 2007].

The population Puttershoek is 6400 people, the second largest village of all six. It has an outspoken identity in a positive sense. The shopping facilities, the disco, the port and the new living quarters all contribute to the pleasant atmosphere of the village. About 2% of the population of Puttershoek is a non-Western immigrant [Binnenmaas, Gemeente op maat, 2002].

Alcazar

Alcazar is the local mega disco in Puttershoek, a village close to Dordrecht in the Hoeksche Waard. It has a capacity of 5000 people in one night. Every Saturday the place is packed with young people coming from different places. About 10% of the village is member of Alcazar. Alcazar exists 25 years now. It slowly grew from a capacity for 600 people to 2000 people; after the third rebuilding it now has a capacity for 5000 people. Alcazar has mainly visitors coming from de Hoeksche Waard and Rotterdam. Every Saturday 300 new people come to visit Alcazar, sometimes even from Belgium and Germany. Moreover Alcazar is located is easy accessible from different directions. There is a big parking area for free for visitors.

Alcazar is also an all-round party center [Alcazar, April 2007], where several events can take place at the same time. Their core activity is the total organisation of events for 50 to 3500 people. There are many different halls with different themes. There are conference rooms, theatre halls and a disco. In total there are ten rooms with various themes and one

disco, ranging from a Spanish Bar - Don Quijote to an African hut – the Tonga, an Après-Ski bar to a French station hall.

The main entrance gives you access to four halls [Music Dance Hall, the Don Quijote bar, the Havana Club and the Snack Corner]. The Music Dance Hall, also called the Urban Dance Hall, is the largest hall of them all, with two floors, four bars and two dance floors. It has a capacity for 2500 visitors.
Alcazar has introduced the Pleasure Card [a smartcard] system. Through this card system Alcazar knows at any time who is in or isn't in at the club. One has to give your fingerprint, which is stored on this smartcard and a face scan is made too. The main entrance is a big hall with on one side the biometric system; the other side has a pay desk. It is not compulsory to become a member in order to access, even though it is made attractive with many forms of discounts [saving points for the Web shop, on CD's, at McDonalds] and free entrance on special occasions etcetera [birthdays, parties].

Supplier/ Client
Gerben Bazuin [about 27 years old], de initiator of Secure Access Road B.V. started his company in 2002. Gerben and his friend worked behind the bar in Alcazar in weekends. They studied informatics.

"The whole idea to use biometric technologies for the disco in Puttershoek started a few years ago, when there used to be 15-20 incidents on a standard Saturday night. There used to be many clashes between various groups of people, since we have visitors coming here from surrounding villages, farmers and people from cities such as Rotterdam etcetera. There used to be especially fights between Moroccans and the villagers. The owner of Alcazar had to employee thirty bouncers for one evening. Another reason for them [Alcazar] was that civil servants used to come and check whether minors were being served alcohol. If so, then Alcazar was fined for that. Therefore the owner asked my friend and me to look into the possibility of biometrics as a solution to their problem. In 2002 we held our first pilot study. It was successful. The owner of Alcazar was interested to market the product, because he was sure that other discos and catering industries would be interested in this product. So they started their company end of 2002, beginning of 2003. Alcazar has a network of about 10 discos all over the Netherlands, where they have implemented this system.

Now we facilitate:
- 10 disco's
- 1 swimming pool
- 3 coffeeshops

We are negotiating with banks and with some companies in Belgium and Turkey as well. Also a new project together with InterPay is being developed."

Secure Access Road B.V. usually implements the SarFunGuard Totem, in which two biometric systems are integrated. It is a combination of face recognition and a finger scan. Gerben admits that none of the technologies are watertight and that the iris scan is the most reliable biometric characteristic.

"The disadvantage of this technique in comparison to the SarFunGuard is the long registration time. With this system it only takes 15 seconds to get one self registered. First of all a picture is taken with the camera built in the totem. Sixteen pictures are saved and four are used for comparison. Next the visitor has to put his/ her finger on the finger scan. The user is asked to put his/ her finger four times on the scanner and all four scans are saved in the system.
In the beginning stage the finger scan wasn't working at all; people had to dry and clean their fingers; the optical sensors were dirty in no time. It wasn't user-friendly for the customers. People don't want to take a lot of time and hassle while entering a disco. The problem has been solved. Now about 30.000 people have registered themselves with Alcazar."

The power of the system lies in three functionalities:

- Registration
- Identification process
- Verification process

"In this system, the SarFunGuard, the fingerprint recognition is used for identification. It is a one-to-many process, meaning that if a person stands in front of the totem [see Figure 1], you have to put your finger on the scan; it tries to identify your fingerprint from the list on the blacklist. This method is used, because the system isn't flawless yet. When a fingerprint is scanned and it is compared with 30.000 fingerprints, the chances that the system makes mistakes are big. Therefore the system compares the fingerprint scans with the blacklist, which has 165 people on it, and the chances for mistakes are immediately much smaller. Verification occurs when you stand in front of the totem [see Figure1]. The photo of the visitor appears on the screen; third parties [guards etcetera] verify whether the visitor is the person which he/she claims to be. It verifies whether the face scan matches the one in their system.

Figure 1

If you are recognised as a person on the blacklist, the totem starts beeping, prohibiting you to enter the club. When you are kicked out the club, because you were drunk or misbehaved is one or another way you will be blacklisted as well. However it is possible that you can be removed from the blacklist if you apologise at the club during a weekday, depending on the offence. Dealing in drugs, consuming drugs, possessing arms and fighting are absolutely prohibited. These people remain on the blacklist.

What one can see, is that the amount of incidents on an evening have decreased tremendously. There is 70-75% less incidents on a Saturday night then before. Since the biometric system has been implemented at the entrance there are fewer incidents at Alcazar, because people are taken out of anonymity and behave more calmly. Moreover the technology is not discriminating; every person gets a fair chance to enter the disco. Only if you misbehave you will be blacklisted. Moreover the SarFunGuard has proven to be cost-effective. Since there are fewer confrontations, the personnel costs have reduced. Before there were thirty bouncers and now it has been cut down to eighteen people.

We work together with the Belgian company BioWise. The demand of biometric technologies is an interplay between the catering industry and companies which are into biometrics. We usually find our clients on fairs. One totem costs €10.000. If a client decides to take a network system, it will be cheaper.

In order to use the totem one needs to insert a smartcard, this costs €3.50. The end-user pays €5.00 for the smartcard. Thus the costs can easily be covered. We also rather have 10 serious clients than 30 fools who just keep the totem in a corner of their bar; this would be bad for the name of our product. We especially focus on SME's [small medium-sized enterprises], whereas other big companies in the Netherlands, such as Nedap, LogicaCMG and so on do projects for the government. Last year we managed to make a small profit. The total turnover last year on the biometric market was 330%.

In Alcazar people don't make complaints on principal grounds [e.g. privacy reasons]; rather they call up to say that they are fed up of with the sms's and emails from Alcazar. People can make their own profile on Alcazar's website. We are not allowed to share the data from our database with other discos; at least that is the case in 'disco land'."

End-users
I interviewed 10 young people. Only one girl was willing to participate with my research. The age ranged from 15 years to 22 years old, with an average of 17 years old.

When I asked the respondents **what they think about the new system with finger- and face scan**. Almost all of them are positive towards the system, they don't see any harm. They all know it is for safety purposes, but they don't actually feel it. All of my respondents have the Alcazar Pleasure Card – the smartcard on which the finger- and face scan are stored, except one 15- year old girl. One can only obtain the card from the age of 16.
It is not compulsory to become a member of Alcazar; the only 'setback' is that you have to pay €10, - instead of €7, -. So all of them become members, it is easier, faster and cheaper with an Alcazar Pleasure Card.

None of the respondents saw any disadvantage of the system, except one mentioned some disadvantages: *"your photo is being registered; no privacy and germs can spread via the finger*

scan". Another boy also said: *"it is a disadvantage, they want to know everything, but they never check"*. *"Sometimes I forget my card that is a disadvantage; I have to pay €10, - instead of €7, -."* Some of them liked the Pleasure Card: *"an extra card in my wallet"*.

When I asked the respondents **whether they feel a real member of Alcazar**, three of them answered positive: *"I don't feel a real member now, because I have to see, whether they allow me to enter, but if I will have the Pleasure Card, I think I will feel a real member."* Two other boys really do feel a member of the Alcazar.

On the question **have you ever been witness of any incident in Alcazar or been involved in one yourself?** Almost all of the boys have witnessed or have been in some kind of fight, quarrel.

Respondent 2: "Once someone threw an ashtray to my head, I slapped him. The other was sent away. He didn't have to hand in his card. Moreover you can easily enter again, if you pay another 10 euros. "

Respondent 3: "Yes I have witnessed many fights. Nothing discriminating, but it are often Turks and Moroccans who are annoying with fighting and all. They stand against the wall at the end of the hall, bumping and poking around. It is a pity, they get a bad name. The system didn't make it safer; one can easily enter again via the other entrance, where you have to pay 10 euros."

Respondent 4: "Every Saturday people fight. Every week there is something, but then you have to get lost. Sometimes it is so bad, that you have to tell everything [give all your personal data] and you cannot enter for a few years."

Respondent 6: "Last week I have been kicked out twice; my ex-girlfriend, we were together for 2 years, started kissing in front of my nose, they kind of provoked me and started laughing at me and pushing. But I was able to persuade him [the bouncer] and I could enter again. I just said sorry to a friend of mine in front of the guard. There are maximal once a month fights over here."

Respondent 7: "Last week there was a fight. Two boys were kicked out. They were being 'smart' and provoking the guards, they kept coming back and then they were hit. Now the boys can never enter, or at least for a very long time."

Respondent 8: "I have seen a fight, but I don't know anything else."

Respondent 10: "I have witnessed a verbal dispute, but no fights. People have been warned."

Are there discounts attached to the Alcazar Pleasure Card?
"The entrance costs 7 euros instead of 10 euros and for some events one is invited for free.

It is anyway free if you come before 11.00 p.m."

My last question was a scenario, to see what young people thought if their personal data would be linked to other discos.
The scenario is: **Imagine that your personal data is known here at Alcazar, now you have been in some kind of dispute and you cannot enter this disco anymore. But Alcazar has this data about you and passes this information on to other discos, so that you cannot enter those either. What do you think about this?**

Respondent 1: "I think it is good, and then at least it makes sense."

Respondent 2: "I don't like it at all. It doesn't matter to me, because I am not annoying. Sometimes I have problems with Ajax supporters and other car sprayers."

Respondent 3: "Very good; at least you can leave the nasty people out. The system should be something like: once nasty – one month no entry, twice nasty – two months no entry etcetera. Actually they should scan everybody's fingerprint at the entrance. It is costless, so why not. So they should oblige everyone on fingerprint scanning upon entry."

Respondent 4: "Good, you go out to have fun and not to fuck around."

Respondent 5: "Everybody deserves a few chances, but if your chances are over, then you should not let someone enter anymore."

Respondent 6: "Stupid, but clever, everybody can have a fight and you can forgive someone three or four times, but after three times you have crossed your limit then it is over. "

Respondent 7: "Actually I don't think that is possible, if you feel shitty or crappy one evening then your whole evening can be a complete disaster, but it doesn't mean that it has to be like that the next time."

Respondent 8: "Is gloomy, not good."

Respondent 9: "Strange, doesn't make sense at all, you can enter any place you want."

Most of the respondents think that everybody deserves several chances and that the measurement is too drastic. As seen from the question about being witness or involved in incidents yourself, almost all respondents had experience with some or another fight or dispute.

5.2 De Fakkel

Swimming Culture

The Netherlands is known for its swimming culture. People go to the swimming pool for fun and for sports. In the Netherlands children learn swimming at an early age. There are about 700 public swimming pools in the Netherlands. The Ministry of Housing, Spatial Planning and Environment has laws regarding hygiene and safety in swimming pools. The rules regarding hygiene are usually related to quality of the water, showers and toilets in the pool. Safety is concerned with supervision by bath superintendents, but also for example about the floor texture [VROM, April, 2007].

There are special rules in the Netherlands regarding supervision at swimming pools. During opening times at least one person has to have a constant watch over the pool. The supervisor has to have a good overview on the pool [Senter Novem, April, 2007]. The superintendent has to assess how many pool supervisors are required based on experience and expectation patterns, such as which visitors come at what timings and what activity is going on at the swimming pool. With type of visitor is meant: age, physical condition, mental capacities, skills, social level and familiarity with the situation. Accordingly one decides how many superintendents should supervise at the pool or maybe limit the amount of pool visitors if there aren't enough supervisors available. If there are just a few swimmers, supervision can be exercised in intervals.

Supervision has to meet certain qualitative and quantitative requirements. For example extra observation can be required when there are:

- Big crowds.
- Young visitors between 6-18 years old [e.g. at birthday parties].
- Noisy, reckless or disobedient visitors present.
- Visitors with medical problems, like eye- and ear disabilities, epilepsy, people using heavy medicines, mentally challenged and invalid people.
- Visitors who don't have adequate knowledge of the spoken and/or written Dutch language [e.g. asylum seekers and immigrants].
- Visitors who are not familiar with the swimming pool.
- Extra deep pools, pool waves, diving boards, slides and rapids etcetera in use.
- Glare which causes the water surface to sparkle.
- Fixed and floating objects for fun.

Ridderkerk

Ridderkerk is a municipality in Zuid-Holland [province in the south of the Netherlands], close to Rotterdam. It has 44757 inhabitants [from CBS statline, 2006]. There are in total 2698 non-Western immigrants, which is 6% of the total population. 1.3% of the population is from Turkish decent, 1.1% is from Surinam, 0.6% is from Morocco and 0.5% is from the Dutch Antilles. The remaining 2.5% is from other non-western countries.

RADAR [the Rotterdam Anti Discrimination Counsel] conducted research on discrimination in schools in the region of Rotterdam [consisting of six other municipalities, including Ridderkerk] in 2005 [RADAR, 2005]. They have taken 400 surveys from youngsters between 12-18 years old. From this research they concluded that approximately one third has been discriminated at school. Mostly students are discriminated because of their origin.

During the municipal council elections of 2006, an extreme right party [Nieuw Rechts] won 800 votes [3.7%], represented with one seat in the city council of Ridderkerk [Monitor Racisme, 2006].

One could conclude from this data, that there are racial tensions in Ridderkerk.

De Fakkel

Swimming pool de Fakkel is divided in two pools. On one side there is a lap pool and on the other side there is a subtropical recreational pool. At the entrance in front of the recreational pool one can find the SarFunGuard Totem, the biometric system with an integrated face- and finger scan. In summers one can find a big outdoor pool as well. The recreational pool has various facilities, such as a 60 meter long waterslide, whirlpools, waterfalls, rapids, a Caribbean bar and special arrangements for children parties.

De Fakkel introduced the Fakkelcard [the same smartcard system as in Alcazar] in the year 2005. The card has been introduced for safety reasons just as in Alcazar. Visitors who don't obey the set of rules can be refused at the entrance through this card system, since they have been registered on the blacklist. This system allows De Fakkel to know at any time who does or doesn't belong in the swimming pool. Visitors have to fill up a registration form with their personal data in order to receive a Fakkelcard. Next four photos and a fingerprint are made, which are stored on this smartcard. A saving system has been connected to every card; swimming for the 11th time means free entrance.

For Wednesdays [1.00 pm-5.00pm], Fridays [7.00 pm-22.00 pm] and Sunday afternoons [1.00 pm-5.00 pm] the Fakkelcard has been set compulsory for the recreational pool from 12 years old. The other days the card is not obligatory. However registration will take place afterwards in case of a calamity. Moreover during holidays it is compulsory [each day] to have a Fakkelcard from the age of twelve. The costs of the Fakkelcard are €3.50 including entrance.
Most pool visitors come from Ridderkerk and surrounding municipalities. Also there are many visitors coming from Rotterdam, especially during holidays.

Supplier

Secure Access B.V. is also the supplier of the SarFunGuard Totem [see Figure 1] for the swimming pool – De Fakkel in Ridderkerk. According to Gerben Bazuin the swimming

pool in Ridderkerk a small town close to Rotterdam has also introduced the SarFunGuard Totem.

"Here [at De Fakkel swimming pool] they especially have problems with Moroccans. 3% of the visitors raised objections against the biometric entrance system. Most of them were elderly people. They made a connection with the Second World War, especially because they didn't find themselves to be dangerous people: "so why should we have these cards". People are easily swayed, when you explain that it diminishes nuisance and trouble. There were about 15 people who were against the new technology at the entrance. We spoke to all of them and explained about situations such as a 55-year old paedophile and other harassing people and that it would make the swimming pool a safer place. But it was easy to convince this group of people to include them in the system; since there are advantages connected to the membership. If you swim 10 times, the 11th time you can swim for free. Most people were easily persuaded by these discounts. The swimming pool has 10.000 registered people. In this swimming pool case it is an agreement with three parties; the police, the judicial power and the swimming pool of the municipality. Here the SarFunGuard Totem fulfils a public function. In practice it means that once you have been sent out of the swimming pool, you immediately get charged, since it is legally grounded.

As with the case of Alcazar, here too the SarFunGuard Totem has proven to be cost-effective. At first there were six pool attendants and now there are three.
Moreover in swimming pools it is possible to share data with one another, because it is legal. Therefore if one is not allowed to enter one swimming pool, that person would not be able to enter any other swimming pool within that municipality."

Client
I interviewed Patrick Vermeulen, the manager of De Fakkel. The biometric system at the entrance of the swimming pool started off in August 2005. The system is used for the recreation pool that is on Wednesdays from 1.00 - 5.00 p.m., on Fridays from 7.00-10.00 p.m. and Sunday afternoons from 1.00-5.00 p.m.

"We deliberately chose these special days to make use of this system, because we have the biggest mix on these days between young and old visitors. The largest group of young people is present on these particular days and times."

When asked **what reasons De Fakkel had to set up this system**, Patrick answered:
"It works preventive and it is a way of marketing. Youth who used to be annoying before, are now taken out of anonymity. Before they could fake their personal data, but now with a finger scan one cannot forge one's identity. You can block the De Fakkel – card and the police always comes."

What advantages does the system offer?
"The aggressive behaviour towards employees has reduced and there is a decrease of people being thrown out of the swimming pool. Heavy assaults, aggressive behaviour and feeling up have become less. Employees experience it positively; it is much more relaxed in the swimming pool. Normally the pressure is high when there are annoying guests, but now it is relatively quiet. Another advantage is that most visitors have a positive stance towards the system. A small number of people are opponent and also some older people, who had to work with fingerprints during the Second World War. One can also see that highly educated people have a more critical outlook regarding the privacy law. These people think that they have knowledge about privacy. One couple was very much against the biometric system, because of religious reasons. They were Christian and believe that biometrics will on the long run lead to a form of dictatorship, also called 'the mark of the beast'."

What kind of problems occur here at the pool?
"Youth hardly ever comes; they usually come on Tuesday evenings. If they are thrown out of the swimming pool, and they are not registered yet, they are compelled to register themselves so they come on the blacklist. At first the police was interested to cooperate with the system, but then we told them: "But it will be favourable for you too; maybe the same people are also on your 'list'." The police corps is decentralised, so they pass it on to the district agent. At Alcazar a district agent is also at work, we want to set up a similar system over here.
If people show aggressive behaviour or touch up girls, in such cases the police always come."

Are there other swimming pools in the Netherlands where this system is in use?
"Tilburg wants to implement this system and maybe later De Meerkamp in Amstelveen. De Meerkamp will come here, to see how the system works. Other municipalities have been here. The KNVB has also been here in relation to hooligans for football stadiums. We are one of the first to use the SAR-system. It is not with the intent to be unique, but we got attention from all wind directions, SBS6, RTL4 and RTL7."

Did any of your visitors have problem with the system?
"About 1 percent of our visitors had problems with the system. We were able to change the negative attitude of ½ percent of our visitors, without them giving us their finger print. It was especially easy to persuade grannies, because they could save, "I am here for the 11th time and I can swim for free". The other ½ percent we were not able to convince, these visitors absolutely did not want De Fakkel-card: "You don't need my personal data, in order to swim". Another older woman didn't want a card, but then she doesn't belong to our target group.
In total we went into a discussion with thirty fundamental objectors. According to me they are all still here. We have about 10.000 cards a year and especially for prevention, at the same time it functions as a discount card."

Is the card also used for marketing purposes?
"In future we want to use it as a marketing tool, for example you can load the card with 10 euros and next you put the card in the machine and your credit is deducted from the card automatically."

What other advantages does the De Fakkel-card have?
"It is also useful to eventually have your medical data in the system. If one has an epileptic attack or a heart attack, then we can take these matters into account. If someone has a heart attack in the swimming pool, you know where the person lives, if you take his or her card and you can inform the family member within a minute. Such a card adds a lot of value, also for children [from the age of 12 years, children are also compelled to have a card]. If a boy breaks his leg, you can directly inform his parents."

Is there a difference in the acceptance of the system between young people and older people?
"Young people have no problems at all and are ready to give their personal data at any time. They are grown up with it. It is totally cool and hip and don't have any problems with it. 45-plus people are much more concerned. Also in discos the acceptation of such technologies is much higher, because it is normal to be frisked in those settings, also at football stadiums there are guards everywhere."

What do you think of a central database?
"If you have a central database of all the swimming pools and all the people on the blacklist in it who committed sexual offences, such people never have to swim again. Every time people speak of the privacy law, it is because of the media, image-forming. This system is much softer instead of having security guards at your pool."

Did you have many incidents this year?
"This year we had eight incidents, three boys from the Antilles wanted to keep the play-materials in the pool en then they pushed three bath superintendents in the pool. Now they are not allowed to enter the pool for a whole month. We have about four to five expelled cases per year. Expelling means that the police are involved. What we see is if young people are bored or have problems at school, you can see that back here at the pool. Something is looming between two groups."

End-users
In this case I interviewed 16 people in total, seven adults and nine youngsters. The second time I went to the pool I only interviewed young people, since they are the target group regarding the SarFunGuard Totem. First I will discuss the adults' responses, followed by those of youngsters.

Most of the respondents were positive towards the biometric system at the entrance. It is again very apparent that most visitors I spoke are not critical towards the new system.

All seven adult respondents have a positive attitude towards the biometric system / Fakkel–card. From the seven adults I spoke, five people have the Fakkel–card.

One of the more critical visitors, *respondent 1* answered: "I don't think that one is anonymous anymore. One is known everywhere. This system is useful and fast. The idea is that one is anonymous, but that word does not exist. Everything is linked. This is one of the last links which still have to be made. When the zip code was invented, I was very much against it. For years I didn't fill up my zip code on forms, but one has to finally give in. Now even more with one Europe, one should really have to have it, it is not that I like it. In 20 years one has to adjust one's ideas. One has little privacy. One thinks that one lives in a democracy, but it has its shortcomings, it is a luxurious prison. Nothing is wrong, as long as one is an honest, righteous citizen and one takes part in the system."

Respondent 5: "According to me the system is very nice, but for children it is much harder."

Respondent 6: "It is a good system, a safe system, but I don't have a feeling that it is really required over here."

Respondent 7 from Ridderkerk: "It is a very good system; I don't have the Fakkel-card. Excellent, it can't be enough safe, now one can at least find out, such strange things happen in swimming pools. Ridderkerk started with this system."

Respondent 8: "Is a good system, if there are troubles, then one can throw someone out."

On the question **whether the adults felt a member**, the answers were mixed.
Respondent 2: "Yes, I feel like a member and that also due to the card. I feel obliged to come here more often."

Respondent 4: "Now I feel a real member with the Fakkel-card, before I didn't."

Respondent 5: "Yes, I feel a real member, now after the Fakkel-card."

Respondent 6: "No, I don't feel a member. I have done this, because I was obliged to, but I absolutely don't feel like a member."

What are the advantages of this system?
Respondent 2: "It is useful, because one can see which boys are misbehaving; they get three warnings and then they are not allowed to come in anymore, especially with girls etcetera, I think it is good. "

Respondent 4: "I don't have any objections, I think it is nice. If something happens, then they immediately know who you are, who, what and they have your address."

Respondent 5: "I don't have any objections, it is just safe, moreover troublemakers can be expelled faster and that is an advantage, is better."
Respondent 6: "If people misbehave, then they can be thrown out and that gives a nice feeling."

Respondent 7: "Registration is very important, if something happens it can be traced, but if something happens, it is already too late, but with harassment in dressing rooms or rape, such a person can at least never enter again.

Respondent 8: "For me it doesn't have any advantages, but if someone misbehaves, it is useful for that purpose."

Are there any disadvantages according to you about the system?
Respondent 1: "I think there is one disadvantage to the system, because once a thief, always a thief. One can never make a mistake. One is registered; it has to become more and more 'ideal', but this harms happiness."

Respondent 2: "No, one cannot enter without card, further then that I don't know."

Respondent 4: "There are no disadvantages."

Respondent 5: "There are no disadvantages."

Respondent 6: "If you forget or loose your card, there are so many cards these days."

Respondent 7: "No, there are no disadvantages; one has to fill the form and just another extra card in your wallet."

Respondent 8: "No disadvantages, if you have nothing to hide, it doesn't matter, but if one misbehaves one does."

Do you know what happens with your personal data?
None of the respondents knew what happens with their data.
Respondent 4: "I actually don't know, I didn't ask. But it will be all right."

Respondent 5: "I assume that they are handled confidentially."

Respondent 6: "I don't know what they will do with it."

Respondent 8: "I assume that it will be stored in some database and used for some mailing list, but I am not making use of that."

Do you feel any change after the implementation of the system?
Respondent 5: "There are fewer problems then before the introduction of the system. But for me the atmosphere hasn't changed."

Respondent 6: "It is possible that some of those annoying boys have left, but I don't know."

Do you know whether there are any discounts attached to the Fakkel-card?
Respondent 4: "What I heard, if you buy a 10-track card, then the 11th or 12th time will be for free."

Respondent 5: "After 10 times, it is free for one time. It always goes very fast for me."

Respondent 6: "I don't know whether there is any discount, it has not been mentioned."

Respondent 8: "According to me not, if you come 10 times, then the 11th time is free."

My last question was again a scenario, to know about their view on privacy.
What do you think about the privacy discussion, what if you personal data is passed on to other authorities or organisations? What do you think about this?
Respondent 2: "Discussion about privacy is good. I am only not aware about the discussion. I want that my personal data remains here and is not shared with others. Moreover it isn't good, because otherwise you cannot enter anywhere. It is also possible that someone else misbehaves and that you are caught, and that is not the intent. "

Respondent 4: "Then one should not misbehave. It is more for the youth, because adults won't misbehave quickly."
Respondent 6: "I think it is logical, I don't think you are just sent away like that. The idea of the system is that it observes. It is possible that the problem just shifts, if they cannot enter here, then they will go to another swimming pool."

Respondent 7: "If you have nothing to hide, then they can have all my personal data they want, except my PIN-number. No, I think it is fine, or they will go from pool to pool and we don't want that to happen."

Respondent 8: "I think it is exaggerated. There is too much protection, in the name of privacy it is not possible and well, if you have nothing to hide, then what is the problem…"

Almost all of the youngsters have a Fakkel-card. Most of them have a positive attitude towards the biometric entrance. They are hardly critical about privacy issues.

What do you think about the biometric system?
Respondent 9 and 10: "Unnecessary, but on the other hand, the fighters don't come anymore. It is fine, I never fight anyway."

Respondent 11: "No, I don't have any objections, the system is good."

Respondent 12 and 13: "It doesn't matter, I don't have any troubles, and it is for safety."

Do you know what happens with your personal data?
Respondent 9 and 10: "I don't know what happens with my personal data, I don't mind giving my data, depends what is behind it."

Respondent 11: "I don't know what happens with my data."

Respondent 12 and 13: "According to us, nothing."

What is the advantage of this system?
Respondent 9 ands 10: "When there are fights or someone feels you up, you can immediately point out the person."

Respondent 11: "It is better, they can recognise you."

Respondent 12 and 13: "It was immediately ok; there is quite some sexual harassment here in the pool by Turks and Moroccans, so it is good.

What is a disadvantage of this system?
Respondent 9 and 10: "You have to stand long in the queue, it takes time."

Respondent 11: "Nothing, no disadvantages."

Respondent 12 and 13: "Not really, if you forget your card, then they can be a bit tough. I know the bath superintendents in the pool quite well, so they aren't difficult."

Respondent 14, 15 and 16: "For very small children it is safe, but it is also annoying if you forget your card, then you cannot enter."

Do you get any kind of discount with your Fakkel-card?
Respondent 11: "If you have a Fakkel-card the fee is €3.15 otherwise it costs €3.40. "

Respondent 12 and 13: "You have to fill in a form, you get your card, and you have to put your right fingerprint thrice. On the 11th time you can swim for free."

Do you sense any difference in how it was before the introduction of the biometric system and now?
Respondent 9 and 10: "Boys, who used to come here before to fight, don't come here anymore. Now there is a nice quite atmosphere, one doesn't need to be afraid; before there used to come more Moroccans here. They would say: "Come with me", but they are not here anymore."

Respondent 12 and 13: "It is Ramadan now, but usually it is full with Turks and Moroccans, and they are over there [pointing at the back of the pool] looking for a fight."

Respondent 14, 15 and 16: "I notice a difference, new slide, a camera; prices have gone up, €0.20 or something. There are fewer people, more white people. De brown people go to Ambacht; here they are strictly watched and sent away. "

Do you feel a member of De Fakkel?
Respondent 9 and 10: "We don't feel a real member; we don't come here very often."

Respondent 12 and 13: "Yes, everybody knows me, my name, everything."

The last question is regarding their outlook on privacy. It is a short scenario: **Imagine that you have been misbehaving at the swimming pool and you are not allowed to come in anymore, but your personal data is passed on to other pools and you cannot go for a swim in those pools either. What do you think about this?**
Respondent 9 and 10: "That you are not allowed to come in for a month, but after that you can, one should learn from your mistakes."

Respondent 11: "It is better, but only for really very bad things."

Respondent 12 and 13: "That doesn't make sense, that other swimming pool has nothing to do with it, what we do here in this pool is our problem."

Respondent 14, 15 and 16: "If your whole class can come in and you are not allowed to enter, that is not nice, but if you do really bad things it could be useful. It is annoying if you can't swim here, maybe in future you cannot swim any place. If you have been misbehaving only once and behave well somewhere else, then you are not allowed to swim anywhere, not very nice!

5.3 Baja Beach Club

Rotterdam
Rotterdam is the second largest city of the Netherlands. The city has the largest harbour of Europe. Rotterdam has a population of 58.8500. Rotterdam consists of 11 sub

municipalities, with about 85.000 inhabitants. About 55% of the population earns a low income [Rotterdam, April 2007].
The Erasmus University has a strong focus on research and education in management and economics. The University is surrounded by numerous multinational firms, such as Deloitte, PricewaterhouseCoopers, American International group [AIG], KPMG, CMG, Procter & Gamble, Coca Cola Company, Cap Gemini, Ernst & Young etcetera. In the center of the city one can find Unilever offices, Robeco, Fortis, ABN-AMRO, ING and Rotterdam WTC.

Baja Beach Club
The Baja Beach Club opened her doors in 1994 in Rotterdam, the Netherlands. In 1995 the Baja Beach Club moved to a new location at the Karel Doormanstraat, Rotterdam, five minutes walking from the central station. The club has millions of national and international visitors. The Baja Beach Club tries to invest and expand in many new markets.

The Baja Beach Club provides entertainment in a tropical setting. The entrance is a 3.5 meter purple beach ball. Music is played from a speedboat. Every first Tuesday of the month an 'After Work Party' is organised, where people come straight from work to the Baja beach Club for a buffet and live performances. Also other events are organised, such as 'Champagne Night', 'Party Night' and 'Ladies Night' etcetera. Moreover the Baja Beach Club organises all kinds of events, celebrate reunions, and prepares lunches or dinners for companies. They organise parties, congresses or meetings.

The setting is surrounded with life-size palm trees, a mini cruise ship, a 26 feet speedboat, paintings symbolising the Baja lifestyle and beach souvenirs from famous beaches from all around the world.

In the past 20 years the Baja Beach Club has been involved in the design and construction of more than 50 clubs worldwide. The Baja Beach Club is always looking for innovations. They believe in new technologies in order to improve their position.

They try to attain this by:
- Constantly renewing their computer hard- and software systems.
- They try to ensure their guests' safety with 'state-of-the-art' security system.
- A loyalty program for their guests; resulting in a steadfast core of guests.
- Inventory systems.

In 2004 the Baja Beach Club introduced the VeriChip. They received worldwide press attention, because of its unique way of payment, not only in Rotterdam, but also in the Baja Beach Club – Barcelona, the first in the world. A special zone, a VIP-deck with a jacuzzi on the left back side of the club, was designed for only VIP visitors, where this integrated chip system was initiated in order to pay. It allows VIP-members to identify themselves or pay their drinks without showing any identification. End 2006/ beginning of 2007 the Baja Beach

Club stopped with implanting chips, because they wanted to keep the chip exclusive. Moreover now the VIP-deck is accessible for everyone.

Supplier/ Client

The Baja Beach Club is well-known club in Rotterdam; they have a branch in Barcelona – Spain. Here I interviewed Conrad Chase, one of the managing directors of the Baja Beach Club.

"Three years ago in February 2004, we started the program. We were open for 7 years. We built a VIP area, for that we needed VIP cards, for our customers; a customer loyalty system. We thought we need technology. I was looking into smartcards etcetera. Then I found out about RFID on the Internet. It exists already 20 years.

Then I encountered the VeriChip – which has an official American Food and Drug Administration [FDA] approval. It is an idea, it is unique and not everybody is going to accept it. Nowadays everybody has silicones, tattoos, piercings, so it is not so strange. Let's give it a try. We like to take advantage of technology.

We want to have a better service for our VIP customers. We have handhold device for ordering, laser systems, and fresh mixing systems etcetera.

The VipChip – We were the first to have the VIP-card, there is another in Galicia, as a method of payment."

Is it possible to deduct money directly from your account?

"It will be possible in the future to do this, but there are many doom scenarios, where the truth is twisted. Nobody creates a story, which is true. But no, we don't store any personal information on the chip, just an ID-number, name and a picture.

Katherine Albright founder of Caspian, she is against the VIP. She is putting false information on the Internet. She has written a book, a spy-book. She does this to sell her book, since it is very controversial. She is against the VeriChip. According to her, the chip can track you and can trace your spending habits, and therefore loose your civil liberties. She is against RFID-tags, but is simply not possible. According to her one can be tracked through databases, but it is not connected to any database. Unfortunately people believe her; it is very unfortunate that she is sending bad information out in the world.

Also CNN and the BBC have been here. The BBC journalist had put a chip in his arm. Also Liberation was here, a French newspaper, they were very informed."

Where do customers get chipped?

"We do it here; a registered, certified nurse gives the injection. We don't do it on the spot, but in a controlled, clean environment to avoid risks and complications."

How many people have the chip implant?
"In Barcelona we have 94 customers. There are many benefits:

- You don't have to carry money with you
- No credit card
- No VIP-card
- You can't loose it
- Can't be stolen
- Can't forget it
- Free entrance
- Access to VIP – area

We only use it for VIP-people. We have a lot of interests, but it is only for exclusive clients. On the VIP-deck we only have exclusive clients and those who want to make use of the bottle service, because there we only offer bottle service. It is a higher range. One can order; champagne, whiskey, vodka etcetera."

What kind of people get chipped?
"Normal people: boys, girls, fashionable, young and old, everything."

Did people have any problems?
"We never had any medical complication. When the first customers got it done, they liked it. In the beginning it was to test it. People enjoyed playing with it and we were quite pleasantly surprised that it was received so well. More people want the chip.

In Rotterdam we have 72 people with a chip. I am from America near Florida, then I lived in Rotterdam for 6 years and now I have been living in Barcelona for a while [Conrad tells me this in fluent Dutch]."

[The rest of the interview is conducted in Dutch.]

Do friends get themselves chipped together?
"Once a father and a son came together to get themselves a chip implant. Sometimes friends do come together, but usually people come separately.

In the Netherlands we ask a different price for the chip implant than in Barcelona. Here we ask €125, - and they get a credit of €100, - on their chip. So the customers have only spent €25, -.
In the Netherlands we ask €1000, - and they get a credit of €1500, - on their chip. It is a big advantage for them."

Are the clients different in the Netherlands from the clients here in Barcelona?
"In the Netherlands it is more exclusive; people with more money make use of this facility. We started this system first in Spain, we didn't know whether it would be accepted, but it did. In the Netherlands we decided to make the chip more expensive, we dared to ask them this amount of money. Actually we want do the same in Spain.
In the Netherlands there are more people with money. Here it is slightly more normal; there are people with more money, but not like in the Netherlands.

In the Netherlands we exist 11 years and in Spain 9½ years. In summers we mostly have tourists coming here. We have a capacity of 1600 people, but we have 2000 people coming here. Friday and Saturday are the busiest days. From the end of July until August we are open for 7 days and nights. The rest of the year we are open from Wednesdays until Sundays."

Who supplies you these chips?
"VeriChip is produced in Boca Raton in between Miami and West Palm Beach. They don't sell it to just anyone. It is very correct company. Each time 50 chips are ordered for the Netherlands and Spain. I am one of their distributors. The name of the company is Metro Risk Management in Miami; they are also based in South America."

Could you tell me something about the chip?
"The chip is as big as a rice grain. It is a 'passive' RFID chip; it means it doesn't have a battery. It only activates if there is a reader close-by. The chip can be read from 2 cm. distance. If the chip is activated, a small transmitter sends the identification code to the radar."

What is according to you the reason that people get themselves chipped?
"To be a VIP, it is a nice piece of conversation. It is something unique.

We have a release waver; we did this deliberately, that the Baja isn't held responsible, if the chip is removed. The BBC journalist wanted to get it removed after a single day, but we advised him to get it only removed after the healing process.

I have also played in Big Brother here in Spain in 2004. I had just got myself chipped a day before and in September I went into the house. I was the first with a chip."

Why did you get yourself chipped?
"I did it to be an example to others.

I also want to tell you, if you type my name on the Internet, you will be taken to my website, but the second link – www.prisonplanet.com, does a doomsday prophecy."

Client

Clarissa Slingerland does the PR for the Baja Beach Club. She was asked to give information about the VeriChip on a conference, conducted by Emerce. Emerce is a magazine about business, media/ marketing and technology. The conference was about Barcoding and RFID.

Baja Beach Club - VeriChip

"We wanted something to bind our customers to the Baja Beach Club, moreover we were interested to get media attention, for our VIP-deck we wanted something outrages.

So we found VeriChip. It costs 1500 euros in total to be chipped; 500 euros for the chip and 1000 euros expenditure money. Privacy is completely guaranteed.

The idea is that only VIP-members can be chipped; you are always recognised and have access to the VIP-deck, you get special invitations, and we also have a branch of our club in Barcelona. Advantages are that you don't need to bring your wallet with you.

We introduced the VeriChip 2 years ago at the Baja Beach Club and it has had a lot of positive publicity. BBC, CNN, Dutch TV, all have come to interview us. It is still very original and very advantageous for the users.

We have 70 happy customers. It is just for VIP members and we want to keep it available for just for VIPs. These members have certain privileges and the more customers we have with a chip, less exclusive it will be.

We are just keeping the usability of the chip the way we have it now, we are not thinking of changing anything at the moment. The catering industry is not all ready for this step, but several clubs have approached us and have shown interest in this system. Moreover the RFID acceptance is high with our customers."

When I went to visit the Baja Beach Club to see how the system works, I also spoke with Clarissa Slingerland, who does the PR and marketing for the Baja Beach Club.

What type of people gets themselves chipped?

"You cannot say what type. Most of the VIP-members are men with money, younger people aren't very pro. Especially older men get themselves chipped. According to me, it has nothing to do with not having money in your wallet, because nobody leaves their home without money. All these people really have a Baja feeling and get themselves chipped to really be a part of the Baja and belong.

In the weekend we have a lot of visitors from Brabant. At this point we have some 100 people on the waiting list who want to be chipped.

The Baja Beach Club never had to deal with the law for personal data and privacy issues."

End-users
At the conference Sari, the first customer at the Baja Beach Club to be chipped also told us about his experience.

"It is all beautiful. We have a lot of space at the VIP-deck, on Saturdays for example it is very crowded, and so you have space there. It only has advantages, everything is better, you cannot feel the chip. It will just stay in my body. Well actually the chip is not scanned at all, because they know me there, I get a drink and once in a while I deposit 100 or 200 euros on the chip at the counter."

What data is attached to the chip?
"The name, RFID-number, birthday, we know what they drink, what there custom drink is, the amount of money on the chip, and once in a while you bring your wallet to deposit money."

Next I went three times to the Baja Beach Club to see if I could speak to more chipped people.
I met Marlies and Irving. Marlies also does the PR for the Baja Beach Club. Irving has been working for 2½/ 3 years for the Baja Beach Club; he is a bartender on the VIP-deck. He has been coming here already for about 10 years.

"There are about 70 people who are chipped. We have just put a stop to chipping, because it has to remain exclusive. The scanner scans the chip, which is implanted in the left upper arm. When you scan the arm one can see the photo of the person and his/ her number and how much money you have on the chip. With a password one can load and withdraw money, you pay directly at the bar and hand the money to Irving. The chip is made of glass and cannot break. If you get chipped, you get papers for your health, but I don't have any health complaints.
You can feel a small lump in the upper arm. Everybody gets the chip in his/ her upper-left arm, so you can't ask for it in your leg.

Most people who have been chipped live in or around Rotterdam. We have had a lot of publicity even from China, Hong Kong. Most of the people who are chipped are regular customers; so they aren't per se friends."

Irving got himself chipped to be an example for other customers. In total there are 3 employees who got themselves chipped. People who are chipped can come on the VIP-deck and those who buy a bottle of drink for maximum 3 persons.

"We are open from Thursdays until Sundays. We have very varied public. On Tuesdays people come after there work from various companies such as Fortis, Telemobile and other big companies, they come in their suit, but we also have very different visitors.

The Baja exists 11 years. There are several 'fake' Baja's, they try to imitate our atmosphere, but they usually all come down. Our club is especially famous because of its name, you just call it and everybody has heard of the Baja; [geholpen herinnering]. There are even organized bus tours from Brabant [province in the south of the Netherlands].

During the first 'session' approximately 30 people were chipped, since then one-by-one over a period of two years. Mostly those who get themselves chipped are individuals, because most people are still quite reluctant to get a 'foreign' thing in their body.

The whole system came from the idea that we wanted to offer something exclusive and special to our customers. All the co-owners/ managers came together and held a brainstorm session; consequently the chip was commonly agreed upon as a new way of paying and entering.

Once you become a member all your personal data is written down. As a VIP-member you always have free entree to the Baja, moreover you can take one guest. Not only do you have a free entree on regular days, also you are invited for free on special occasions, on all holidays and special actions, on these days you cannot bring a guest along. Invitations are usually done by email."

Is it possible to remove the chip?
"If you want you can get the chip removed in the hospital, the chip is placed under your second skin, but so far nobody wants to have the chip removed.

The entrance fee is €7.50 from Tuesdays till Sundays, except on Saturdays it costs €8.50. On special occasions it costs €9.50 such as on Easter, Pentecost etcetera. At the entrance chipped members are also scanned, there you cannot see the amount of money they have on their chip, but you can see this here on the deck. However it is still not very convenient, because you have to put your arm in an unnatural position to get it scanned, so we are thinking to make the scanner stronger, to catch the signal from a bigger distance. On the deck VIP-members immediately get their favourite drink. The chip is a stunt to have loyal customers and bind them to our club.

We have had a lot of publicity from the whole world: Japan, the biggest TV channel from China, Dutch TV, National Geographic, CNN, Discovery, we are the first in the world with a wallet under the skin."

Next I interviewed three end-users,

Ismael Sari, one of the first to be chipped at the Baja Beach Club, Arno Gerbscheid, he is the manager of the Baja Beach Club and Ryoni, who got himself chipped in 2005.

Why did you get yourself chipped?
Sari: "There was an action; the first 25 people could get the chip for free. It is my second home here; it only has advantages, no disadvantages. I know everybody here, the owner, and my friends."
Arno: "I got myself chipped to show other people that it is not harmful, from a commercial point of view."

Ryoni: "Because of laziness. The main reason was that you are a VIP. Moreover you can just walk into the club without paying etcetera."

Did your friends get themselves chipped?
Sari: "From my own group of friends, nobody got chipped, not many of my friends come here anyway, I am the only one, who comes here a lot. But I have met many other VIP-members."

Ryoni: "I don't know anybody with a chip."

Do you have a feeling that you belong to the Baja?
Sari: "Yes, you really have the feeling that you want to belong to the Baja and yes, you really do belong!"

Ryoni: "I know the owner, but I don't feel a member of the Baja Beach Club. I don't really feel connected."

What advantages and the disadvantages of the chip according to you?
Sari: "When entering you immediately get your favorite drink, mine is red bull and it is deducted from my balance. There are no disadvantages. The only difference is I don't to want to show-off. Here it is quiet, down there it is crowded, and that is the only difference."

Arno: "No disadvantages and no advantages; not directly with the chip, but indirectly the advantage is the tremendous media attention."

Ryoni: "It is very convenient. I can take one person for free with me; I can just walk on, the staff knows me and I don't need to pay cash anymore. I haven't had any disadvantages so far."

How many people got themselves chipped? What kind of people and for what reasons do you think?
Arno: "Around 40 to 45 people have a chip. It varies what kind of people, but most of them got chipped out of ease of the chip. If it is crowded in the Baja, you can go to the deck and you are taken care of, you get personal attention."

Ryoni: "According to me it is especially for lazy people; with the chip everything goes faster."

What age are the people who get themselves chipped?
Arno: "Between 20 and 55 years old, usually people have their own company, they want easy and comfortable. They are common people; it could be anyone who wants to be chipped. Condition is that these people don't mind having a strange object in their bodies which is not their own."

Could you explain what the procedure is, when chipped?
Ryoni: "The Baja Beach Club makes a doctor's appointment; checks your medical condition; then the chip is injected. All-in-all it just takes half an hour. National Geographic asked my permission, whether they could film the chip implant for a documentary, I agreed."

Would it be convenient if the chip could be used at other clubs?
Ryoni: "Yes, but I would not get another chip in my arm, only if this one chip can be used at other clubs it would be really convenient."

Do you worry that your personal data may be misused?
Ryoni: "I don't worry about this at all; if people want to do wrong they will find ways, Anyway, anyhow, so this chip doesn't make a difference, it is for my convenience."

6 Theoretical Framework

Life is increasingly concerned with communicating and travelling. People go multiple directions and dimensions, move simultaneously, and wait in various queues in different situations; movement happens at innumerable speeds. We always need more and faster, more highways, more airports, more servers, more nodes on the global network. We are now in a society in which movement is a commodity. It has effects on urban planning, city life, concept of citizenship and on life itself. This complex system of movement has become streamlined, we seem to travel seamlessly in and out at these various entry points. We are continuously checked. What is your credit limit? Where do you buy your goods? Who are you really [Zournazi, M., p. 229, 2002]?

6.1 Introduction

In this chapter I will be describing various theories regarding surveillance. Biometric companies, media, governments argue that travelling has become risky; main concerns are terrorist attacks. Bodies are electronically scanned and names are matched automatically in databases containing image archives, credit card purchases, social security information and travel itineraries. The body has become the data mass of modern life.

Especially after 11 September 2001, governments and companies have pushed these developments. Consequently, the biometrics industry is booming since then. In order to have control on the mass, various surveillance systems have been implemented. But how do these technologies work and what effect do they have on the individual or on society? How does the body move in the networks? What kind of relations come to existence? How does power operate through these new relations of bodies? In this chapter I will try to give answer to these questions from various viewpoints.

6.2 Big Brother Society

"Your worst enemy, he reflected, was your nervous system. At any moment the tension inside you was liable to translate itself into some visible symptom", [Orwell, G., p. 64, 1949].

George Orwell's, Nineteen Eighty four [published in 1949] has become a rich source of examples when discussing privacy, state-security issues and surveillance. The term 'Orwellian' is to describe actions or organisations of a totalitarian society [Wikipedia, May 2007]. Orwellian is also used to describe oppressive political power of the state over the individual.

Some of the meanings the term Orwellian has, can be directly referred to our society:

1. Invasion of personal privacy by the state, whether physically or by means of surveillance.

2. The exercise of total state control in the daily life of citizens, as in a 'Big Brother' society.

The phrase 'Big Brother is watching you' has the meaning of any act of surveillance that is perceived as invasive. The Big Brother state is often used to describe negatively a situation in which a Big Brother is constantly monitoring the population in order to identify betrayal or improper behaviour or thoughts. In Nineteen Eighty Four the 'Thought Police' uses telescreens in every household and public area, as well as hidden microphones and informers in order to catch potential 'thought' criminals, who can endanger the security of the 'Party'.

Today's situation differs from Orwell's work: "In Nineteen Eighty Four the state exerts power over the individual", whereas now we can see other agencies than the state making use of these surveillance methods. Moreover now one makes use of electronic technologies.

Orwell points out a few important issues, one of them being "the value of human dignity in a world dominated by rational bureaucratic control [Lyon, D., p. 174, 175, 2001]". Orwell's vision is less relevant for our current situation, since he didn't foresee the present computerisation of bureaucratic surveillance and the systematic processing and collection of personal data in people's day-to-day lives, such as public streets, homes, schools, sport centers, airports etcetera.

6.3 Surveillance

"We are all subject to many kinds of surveillance, from categorical suspicion to categorical seduction [Lyon, D., p. 174, 2001]." Surveillance has become a routine in our information society. Many different parties are interested in people's personal data. Mostly they make use of searchable databases in order to classify and catalogue such data to prepare the data for specific uses, including marketing and security [Lyon, D., p. 171, 2001]. Personal data has become very valuable from an economic and an administrative viewpoint.
Moreover with the increasing desensitisation, consumer profiling has almost become standard. We are surrounded by panoptical cameras, which are marketed as highly desirable, moreover people enjoy being on television [Barber, G., p.1, 2001]. The range of surveillance technologies (dataveillance) has expanded to genetic, biometric, global positioning and video surveillance systems. These technologies are implemented in unfamiliar contexts to 'improve' security [Lyon, D., p. 672, 2003]. Biometrics seems to be a novelty, but it has been in use in several contexts, such as retinal scans at bank machines to digital records of fingerprints in police databases. These surveillance systems have one thing in common; they all make use of databases. This means that all technologies have algorithms, mathematical codes for computers to make 'decisions' whether a person fits a certain category, depending on behaviour, signal, word or image. It means that everything is automated.

Surveillance is practiced on the pretext of enhancing efficiency, productivity, participation, welfare, health and safety. Today's surveillance is computer-assisted. Computerisation has introduced different ways of monitoring everyday life for social administrative, commercial and employment by making use of databases. Now we can see that surveillance is applied by far and at large at the workplace, to check the behaviour of employees.

The rapid increase of surveillance in the twentieth century administration and commerce may be due to rising rates of mobility. On the one hand we can see an increased mobility on the other hand we do not need to be physically present to interact with others, buy goods, engage in exchanges, or to communicate. Therefore some tokens of identity, authenticity and eligibility are required [Lyon, D., p. 171, 2001]. New types of technology have evolved for travelling and communicating. Fewer, transactions and interactions are based on face-to-face relationships. Consequently, new forms of identifying have come in place, substituting 'the person' with PINs, barcodes, signatures, photo IDs and biometrics. People are thus identified by abstract data instead of human characteristics.

Biometrics is used as a form of surveillance, but it is rather a scanning technology than a visual technology, therefore probably more suitable for control than for discipline [Fuller, G., p.2, 2003]. In the world of biometrics, your body becomes your password, leaving you free from remembering a pin-code or password, active cards or keys; it means that you are 'free' to move as long you are authorised to move. Control doesn't just imply moulding a subject; rather it signifies a continual process of modulation: like a self-transmuting, moulding, continually changing from one moment to the next.

Many are afraid that this electronic form of surveillance becomes too widely spread, like in Foucault's treatment of Bentham's Panopticon prison; a system of ubiquitous power based on continuous observation. This theory assumes that monitoring populations comes ostensibly from above. Next I will go into Michel Foucault's panoptical prison theory.

6.4 Panopticon Observation

The Panopticon is a type of prison, designed by the English philosopher, Jeremy Bentham in the late eighteenth century. The design was to maximise the visibility of inmates who were to be isolated in individual cells such that they were unaware moment-to-moment whether they were being observed by guards from a central point. Thus the idea behind the design is that the observer can monitor all prisoners without the prisoners knowing whether they are being observed or not. Michel Foucault [1977] based his theory on this panoptical prison [Wikipedia, May 2007]. He used it as a metaphor in 'Discipline and Punish' for modern disciplinary societies and its invasive inclination to observe and normalize. Foucault situates surveillance in the context of a distinctive theory of power. According Foucault all hierarchical structures, such as schools, the army, the hospital, the factory etcetera resemble Bentham's Panopticon.

Bentham's and Foucault's want to point out here, that the panopticon is powerful, because its surveillance is subtle, hidden [Lyon, D., 175, 2001]. The power lies in the 'invisible gaze' of the prison inspector; who is shielded from the prisoners' views by venetian blinds. One of the characteristics of panoptical surveillance is that the minority watches the majority. Another important characteristic is that surveillance isn't masked; the observed is aware that he is being watched. This is crucial, otherwise the observed won't feel the pressure to obey the rules. The fear is derived from the uncertainty instead from the watchful Big Brother. Consequently the prisoners learn to discipline themselves. However in both cases fear is the main method in order to obtain control.

Foucault in contrast to George Orwell's Big Brother, which served to repress, induce and maintain obedience and social order, "understood modern surveillance as something which had been made increasingly unnecessary, due to the 'normalizing gaze' of the disciplines and the constitution of self-regulating subjects" [Hier, S.P., p.401, 2003]. Foucault's ultimate question was to know how the modern society had developed. He believed that surveillance played an important role in that process. Repressing, panoptic observation makes one reflect on one's behaviour; generates disciplinary practices and one exercises power over oneself. With subtly and ongoing efforts, people can transform their selves [Haggerty, K.D. and Ericson, R.V., p. 607, 2000]. Thus by monitoring, and what Foucault calls biopower, prisoners are normalised.

6.5 Biopower

Foucault emphasises the following: "discipline was 'a type of power, a modality for its exercise comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is 'physics' or an 'anatomy' [structure] of power, a technology' [Walters, W., p.190, 2006]."

Discipline is an 'anti-nomadic technique'. It fixes arrests or regulates movements, and it clears up confusion. This disciplinary control is mostly found in the school, the prison, the hospital, and the factory. Discipline operates a regime of confinement, segmentation and utilisation. These institutions make it possible to organise human diversity by totalising and individualising it, in order to maximise and extract its capacities.
For Foucault it is clear that discipline is a 'technology' of power and not power in itself.

6.6 Contemporary Surveillance Systems

Surveillant Assemblage

According to Kevin Haggerty and Richard Ericson, Foucault and Orwell fail to engage contemporary developments in surveillance technology. Foucault focuses mainly on transformations in eighteenth and nineteenth century. Foucault's insight should be reconsidered in relation to the panoptic metaphor.

A successor to Foucault's panopticon is a post-panopticon theory; Haggerty and Ericson's 'surveillant assemblage'. Haggerty and Ericson try to fit the technological particularities of contemporary surveillance. “These assemblages are said to be composed of 'discrete data flows of an essentially limitless range of other phenomena such as people, signs, chemicals, knowledge and institutions” [Haggerty and Ericson, p. 608, 2000]. “They operate by abstracting human bodies from their territorial settings and separating them into series of discrete flows. These flows are then reassembled in different locations as discrete and virtual 'data doubles' [Haggerty and Ericson, p. 605, 2000]”. “...Groups which were previously exempt from routine surveillance are now increasingly being monitored” [Haggerty K.D., and Ericson, R.V., p. 606, 2000]. When simulating data, it is not simply a representation, but it involves an advanced form of pragmatics having to do with instrumental efficacy in making discriminations among various populations.

Surveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole. This leads to the term surveillance as assemblage, operating across state and extra-state institutions. Police and other authorities are constantly looking for ways to integrate their different computer systems and databases, linking for example databases for fingerprints and DNA. A regional police computer system would receive combinations of information such as: phone conversations, reports, tip-offs, hunches, consumer and social security databases, crime data, phone bugging, audio, video and pictures and data communications are all visible in a GIS [geographic information system], allowing to read relations, which are used in investigation and monitoring. All this information will be corporated into a database and one can know everything about a given person and associated relevant links, such as vehicle, other individuals etcetera. This information combines knowledge and derives risk profiles from these various surveillance systems.

The surveillant assemblage can be understood as a mechanism of 'visualisation', creating a merger between flesh and technology, consisting of pure information which is then redirected back towards the body for a multitude of reasons [Hier, S.P, p. 402, 2003].

One could say that bodies and identities are reconstructed in 'data doubles'; a mirroring of their activities and qualities down in the finest detail. Haggerty and Ericson argue that in late modern period, information and data gathering techniques are increasing at a rapid rate, which break the human body into a number of discrete signifying data flows. This data is again reassembled as functional data, formulating categorical images or risk data profiles [Hier, S.P., p. 400, 2003].

Remarks

We can see that the new measures are taken in order to create rather than detect conditions of fraud. It reveals that surveillance functions as a cause as well as an effect of intensified forms of social monitoring and information gathering. What remains are prejudicial

evaluations, populist reinforcement while certain groups of people are confronted with ever increasing intrusions into their personal lives.

Lyon suggests that the political system not merely works top-down, but has been transformed into a flexible assemblage.

Contemporary surveillance practices, [Hier, S.P., p. 410, 2003] characterised of assemblage may be best understood as a categorical seduction in which participatory forms of surveillance where the consumer has to give more and more personal information and is seduced by consumer convenience and rewards.

The assemblage model categorises ‘suspects’. It entails profiling of any number of socially perceived dangerous groups.

'**Informaticised Body**'

Professor Kevin Warwick of Reading University is the 'first cyborg'; he has a silicon chip transponder implanted in his forearm. This technology with the opportunity for surveillance has been rapidly embraced to monitor pets. The microchip can be read with a scanner which connects the unique identifying number on the microchip, revealing details of the pet's history, ownership and medical records. Warwick proposed already in 1998, that the implanted microchips could be used to scrutinise the movement of employees and monitor money transfers, medical records and passport details. For example, if someone would like to enter a building where he of she is not allowed to enter, the central computer would warn people inside with an alarm system or prevent him access.

Biometrics is the ultimate tool in connecting our bodies to the computer world. By measuring and statistically analysing the body as data, biometrics creates a match with borders based on the uniqueness of the body. With the increased mobility, biometrics is becoming a way to compare our body against the networks in which our 'multiple self' reside. In the world of biometric, the individual is not seen as a whole body, but seen in fragments.

Just like Haggerty and Ericson, Van der Ploeg reformulates Foucault's paradigm. Her emphasis is on 'biometrics and the body'. She reconfigures the panopticon because of the ongoing developments in surveillance and dataveillance technologies and practices. She focuses on biometrics, technologies of corporeal tracking and control. “The observation that many spheres of activity, the generation, collection and processing of body data is increasing.”

She tries to make existing theoretical frameworks up-to-date by arguing that merely collecting yet another type of personal information are not the main concern. However, one has to reconsider how the various aspects of the physical existence are translated into digital code and 'information', how the new uses of bodies are subsequently allowed, how

it effects one's framework of relationships , instead of just being a representation [Van der Ploeg, p. 69, 2003].

Van der Ploeg's study of biometrics and the body describes the new and surveillant regime resulting not in bodily discipline, but undermining the boundaries of the corporeal itself. Like Haggerty and Ericson's data double, she also emphasises the 'informaticised' body, resulting from its effective, biometric reproduction.

In these theories of data double and assemblage, the object is of main interest. Surveillance and control is explained through an emphasis on functions, practices and structures that are impersonal and ultimately institutionalised. The surveillant assemblage relies on machines to make and record observations.
In this sense whatever step we take, we always leave a trace which is related to us by its origin and often by internal signs of various sorts [Friesen, N., p. 11, 2006]. This means that we continuously leave our steps behind; traces have become aspects of our being through which we become objects in the world. This means that our identity is identified now with the assemblage of traces rather than the actual presence of ourselves. Van der Ploeg calls this "the inability to distinguish between the 'body itself' and 'body information'"[Van der Ploeg, p. 69, 2003]. Similarly, Haggerty and Ericson state: "the surveillance assemblage standardises the capture of flesh/information flows of the human body. It is not immediately concerned with the direct physical relocation of the human body, but with transforming the body into pure information, such that it can be rendered more mobile and comparable." [Haggerty, K.D., and Ericson, R.V., p.613, 2000].

Remarks
The problem with this system is that if we are the data double could be based on incorrect data; we could unfairly be denied access on every level. This means that scanning the body with biometrics will directly affect the protocols of authentication. Thus movement is logged at every threshold.

Moreover, if biometric controls access, life becomes a pattern match. Identity is not just concerned with categories like race, gender, sexuality etcetera, but categorisation has gone cellular and biological; race can now be refined into other areas. This leads to a distinction among races, a hierarchy of races; some races are described as good and others are described as inferior. This is a way of fragmenting the field of the biological that power controls [Fuller, G., p. 3, 2003]. It is a way of separating groups that exist within a population.
It is clear that a eugenic dimension is created through the use of these technologies. These databases operate to read the 'identity'. Any form of identity is necessarily regulatory on one level; some attributes are recognised and privileged, whereas others are excluded.

Race and representations are codified; the 'terror' of seeing men bent in prayer, the outrage at women in purdah are like signs; these 'codes' have become a heuristic for explaining a

complex world. Categories of race, gender, religion, sexuality are now 'patrolled territory'. In this perspective, biometrics just allows one to investigate deeper into the database and divide race with spatial and temporal coordinates. In other words, in a multicultural world, biometrics can revive race-discrimination.

What biometrics does is to control access to buildings, websites and countries. It is a way of controlling the 'chaos' of movement, but also to streamline the flow for those with the right password. These new control technologies make new relations visible that give insight into the issues of power in a networked world.

Rhizome

The rhizome functions as a metaphor in order to explain contemporary surveillance. Rhizomes are plants usually underground, horizontal stem of a plant that often sends out roots and shoots from its nodes in different locations; the root structure is inconsequential. In surveillance theory it means that no centralised structure exists, which coordinates 'the branches' of surveillance, but that surveillant technologies operate by variation, discontinuity, intensification and horizontally fragmented expansion [Deleuze, G., Guattari F., p. 21, 1987].

Haggerty and Eriscon have borrowed Gilles Deleuze and Félix Guattari's theory; they maintain that the rhizomatic expansion of surveillance has penetrated all sectors of society; "...cumulatively highlight a fractured rhizomatic criss-crossing of 'the gaze' such that no major population groups stand irrefutably above or outside the surveillant assemblage"[Haggerty, K.D., and Ericson, R. V., p. 618, 2000]. The expansion of surveillance has been supported by subtle variations and intensifications in technological capabilities and connections with other monitoring and computing devices, trying to seek new target groups that require a greater degree of monitoring, such as: young people, caregivers, commuters, employees, elderly, international travellers, parolees, privileged and the weak [Haggerty, K.D., and Ericson, R. V., p. 615, 2000]. Much of this expansion is driven by financial imperative to find new markets for surveillance technologies which were originally designed for military purposes.

On the other hand the population is increasingly seen as a consumer and seduced into the market economy. While surveillance is used to construct and monitor consumption patterns it is more concerned with attempts to limit access to places and information or to allow for creating consumer profiles through reconstructions of a person's behaviour, habits and actions. In this way, surveillance plays a vital role in positive population management strategies [Haggerty, K.D., and Ericson, R. V., p. 615-618, 2000]. One can see a growing trade in the sale of such information. Governments are keen to profit from the sale of information stored in various databases. But also marketing firms have developed consumer profiling techniques that contain precise information on a person's age, gender, political inclinations, religious preferences, reading habits, ethnicity, family size, income

and so on. Money is being made through the sale of data from license bureaus, personal income data and employment records.

It is recognised that surveillance monitoring is different in various applications, in which bottom-up forms of observation are also at work now. Surveillance techniques are slowly developing through advances in information and communication technologies across state and beyond, through for example extra-state agencies. These technologies enable the many to scrutinise the few like never before. The incorporation of surveillance in society is deep, but so far the lives of the white mainstream are still comparatively untouched by it. Moreover if one differs in financial practices, education and/or lifestyle than the usual and comes into contact with different institutions, one will automatically be a unique and be subjected to surveillance. Thus people are categorised in various profile groups; the poor will be in regular contact with surveillance systems associated with social assistance or criminal justice, whereas the middle and upper classes will be subjected to another form of observation and analysis, such as: consumption habits, health profile, occupational performance, financial transactions, communication patterns, Internet use, credit history, transportation patterns and physical access controls.

According to David Lyon it is important to realise that these new patterns or 'shoots' are not random. They involve 'leaky containers', meaning to say that unconnected public and private informational infrastructures are increasingly come into contact with each other. These surveillance systems with the desire to coordinate and control populations make that visible, evading direct perception.

Thomas Mathiesen misses the role of the mass media in Foucault's panoptical surveillance society. Under the panoptical surveillance the few were able to see the many, now the many have increasingly become accustomed to see and consider the actions of the few with the rise and expansion of mass media, communication systems and in particular television [Mathiesen, T., p. 215-234, 1997]. If footage on terrorism, abductions etcetera is revealed to a worldwide audience, the obvious solution seems more surveillance and tighter security.

Thus instead of a panoptical gaze, removed from the open view, the synoptic [a common viewpoint] embraces the visual in the most emphatic manner. In the terrorist attack on the World Trade Center of 11 September 2001 and the visual representation of the collapsing Twin Towers, which invited a global audience to 'consume' this image, led to panoptical aspirations, through intensification of information gathering, data sharing and risk management techniques.

Post-traditional Societies

Information has become more than ever a way to reflect on the causes and consequences of our actions. We have the means to maintain and revise a set of biographical narratives, social roles and lifestyles, the story of, who we are, how we came to be and where we are now. “We are increasingly free to choose what we want to do and who we want to be, even

though that wealth gives access to more options" [Giddens, A., p. 54, 1991]. On the one hand choice can be liberating and on the other troubling. It is liberating, because it gives the opportunity to increase one's self-fulfilment, whereas it can be troubling, causing an increased emotional stress and one needs time to analyse the choices and minimise risk. Whereas in traditional societies one is provided with a social role in post-traditional society one is usually forced to create one themselves.
Furthermore in pre-modern societies the elderly possessed the knowledge, however in modern societies we rely on 'expert systems'. They are not physically there, but we must trust them. Even though one trusts them one knows that something can go wrong. Also the technologies one uses hold risks. As Giddens puts it: "modernity is said to be like an unsteerable juggernaut travelling through space" [Giddens, A., p.151-154, 1991].

Remarks
Increasingly we see that in western society documents are constructed, based on data about ourselves. They serve as a badge, which we have to show everywhere to gain admission and receive normal treatment as a person.

6.7 Social Sorting

Many agencies have an interest in personal data. A wide spectrum of them uses searchable databases to classify and catalogue such data. Various parties; governments, the internet, e-commerce companies are all interested in valuable personal data for economic and administrative purposes [David Lyon, p. 171-181, 2001 and Burrows, R., Gane, N., p. 793-812, 2006].
In first instance, it may not be clear that loyalty cards, used in supermarkets are a way to analyse our spending patterns and bind client by giving discounts.

However everyone who lives in a high technology society is aware that data is abstracted from our daily activities. Various authorities, companies, governments collect, store, check, exchange and use these data to determine some eligibility or access to persons, placed, experiences or events. All modern societies are now heavily dependent on information infrastructures, which have important implications. Many techniques are used for processing personal data that allow profiles to be constructed from different and dispersed sources or by datamining that delves into existing sources for further details. Biometric, genetic and video data may be processed and cross-checked against each other by the state and commercial agencies.

But why have the interest in these personal details? Surveillance is a way to sort, classify and categorise populations and persons for risk assessment and management. Social sorting is an ancient practise; categorising is a necessity of life…how would we otherwise know which bathroom to use or which immigration line to choose at the airport? However categorising is becoming more and more central to a sociological understanding of contemporary societies.

In many cases these constructed profiles are sold to companies for marketing strategies, leading to spam messages of products which have been selected on the basis of their profiles. Governments too collect this type of information and create profiles based on the data. Aim is to track potential dangerous criminals or terrorists, before they commit any crime, so that they can be monitored by secret agencies.

Social sorting today attempts to minimise risk by 'discovering' [preferably in advance], who is likely to break the law, buy a particular product or seek a certain service. Networked computer databases facilitate in social sorting for whatever purpose. These systems thus create categories of suspicion and try to foresee undesirable behaviours. They accentuate difference and reinforce existing inequalities.
By categorising and systematically collecting and arranging data affects how one perceives society. Insurance companies increasingly determine what sort of properties or people need to be protected, making communication more central to policing. Risks are classified. Would-be immigrants, youth or ethnic minority groups are categorised; determining their life-chances. Police also contributes to the construction of identities in which differences are accentuated. These technologies and systems have less and less to do with individual suspicion, they rather relate to risk assessment and the 'probability that an individual may be an offender' [Lyon, D., p. 173, 2001]. Data becomes a way to judge a person or groups of people. Digital data which circulates within risk assessment is distanced from the person from whom the data was initially obtained. Purchased goods or participating in a sport event or being in a particular city at a certain time, becomes a clue for an identity of a person. 'The system watches what you do; it fits you in a pattern; the cycle begins again' [Lessig, L., p. 154, 1999]. These systems make people up. It is a way to exclude people from participation in certain activities.

By classifying, one trains to predict consumption patterns and lifestyle variables derived from various data. It also leads to the greatest level of discrimination when predicting these differences. Classifications have always been a major feature of commercial and public sector activities. They especially seem to be effective tools for marketing activities; direct mailing, store location, political campaigning etcetera. Another serious effect of profiling is the danger that innocent people can be monitored, because they have 'wrong' set of data. People usually don't know that their profile has been constructed and that they are being observed by for example the Algemene Inlichtingen- en Veiligheidsdient [AIVD, the Dutch secret agency].

Software Sorting
By classifying the 'information rich' versus the 'information poor', by 'software sorting', Stephen Graham means to say that certain functionalities and services are offered to those who seem attractive whilst the less attractive users and communities can be pushed away electronically [Graham, S., p. 325, 2004]. Graham argues that software sorting happens with

technologies such as: internet prioritisation, call center queuing, electronic road pricing, biometrics and algorithmic surveillance techniques.
According to Graham two forms of software sorting exist:

1. The physical presence of software code which is mediated by human conduct.
2. New technologies of surveillance that capture personal data triggered by human bodies.

In the second situation by abstracting data, people are placed in new social classes of income, attributes, preferences or offences so that they can be influenced, managed or controlled. In such situations identity and data are linked with each other, thus identities are created through acts of consumption, classifying you into certain categories or even communities.

Panoptic Sort
According to Oscar Gandy surveillance conducted by computers through searchable databases create systems of discrimination. He is mostly concerned with database marketing, although his theory can also be applied for other systems. He uses the concept 'panoptic sort'; a discriminatory technology that assigns people to groups of 'winners and losers' based on numerous bits of personal information that have been collected, stored, processed and shared through an intelligent network [Lyon, D., p.177, 2001]. The real concern here is that there is no loss of privacy, but the political and economic consequences of loss of control over personal information. Since the 'panoptic sort' is justified with practical explanations such as efficiency, broadening consumer choice, reducing costs etcetera.

Remarks
Dataveillance potentials have expanded as never before, not only the internet is such technology, but it has extended to genetic, biometric, global positioning and video surveillance.

6.8 Society of Control

Disciplinary versus Control
Whereas Foucault understands power in terms of multiple tactics and functioning's, Gilles Deleuze sees that disciplinary societies are gradually turning into control societies. He claims that a new power is coming to define the social and political life of states and citizens. Deleuze does not see the rise of control as a benign phenomenon, but it is also not a situation of perfected domination. He theorises control by comparing its logic, topology, assumptions and its mechanisms to those of the 'disciplinary society' that it challenges and threatens to displace [Walters, W., p. 189, 190, 2006]. As Foucault studied the disciplinary society, Deleuze argues that the disciplinary mechanisms are breaking down and are slowly changing into control societies. In panoptical surveillance societies; simple machines for

monitoring are used, opposed to control societies, which make use of advanced computer technologies. Observation in such societies does not take place in confined spaces, but is a continuous process by making use of computer networks. Another difference with Foucault's panoptical surveillance is that in a disciplinary society the aim is to mould the citizen in such a way that he acquires the desired norms and behaves in the desired manner. It is clear that in Foucault's theory, the person is central in relation to Deleuze's control society. "These are the societies of control, which are in the process of replacing disciplinary societies [Deleuze, G., p.3. 1992]." Discipline involves power that is concentrated in if not contained by sites of confinement.
Control societies operate in fluctuating networks of production and consumption. Power is now solely related to social orders such as 'consumer societies', 'information societies' or 'risk societies' [Walters, W., p.190, 2006]. Moreover the way we move has turned to a digital order where the borders between inside and outside have become blurred, a social order in which power is inseparable from mechanisms and circuits of desire, which are updated by systems of advertising, marketing and self-actualisation. "In a society of control, the corporation has replaced the factory [Deleuze, G., p.4, 1992]. The corporation constantly presents the most aggressive rivalry as a healthy form of working; moreover it tries to motivate individuals to oppose one another. Marketing is the main 'soul' of the corporation. Corporations tell us that they have a soul, "which is the most terrifying news in the world" [Deleuze, G., p. 6, 1992]. Market operations have now become an instrument of social control. Additionally in control societies, the signature or the name aren't important, but the code. The code becomes the password.

He argues that various aspects make the difference between the disciplinary society and control society. Money for example in the disciplinary society are bundles of money that locks gold as numerical standard, whereas in a control society money relates to floating rates of exchange, established by a set of standard currencies.

Dividuals
According to Deleuze discipline creates a tension between masses and individuals, whereas with control individuals have become 'dividuals'. Their context has changed from society to that of profiles, samples, databanks, markets or 'banks' [Walters, W., p.191, 2006, Deleuze, G., 5, 1992]. An individual is something that cannot be divided, however various technologies try to proliferate in multiple fields, attempting to 'know' and control the individual by measuring it.
Walter explains Deleuze's notion of the dividual: a partial, fragmented and incomplete in comparison to the individual signifying a complete, whole person.

Whereas in Foucault's disciplinary society has the ambition to reform, moralise, remake and integrate the individual, in Deleuze's control society the dream of a normalised society has been abandoned. Since Deleuze's control society surveillance occurs with computer technologies, people change into numbers, such social security or air mile numbers. Observation happens through algorithms; it is not bothered with the reform of the young

offender, but rather wants to secure the home or the shopping mall against their presence [Walters, W., p.191-192, 2006]. With this type of observing, the observer is not interested in you as the person, rather the observer is interested in a certain segment of you, the dividual. Thus a telephone company is not interested in the person behind a certain telephone number, but just wants to know the services the user uses and in which way. In such a control society, surveillance is 'designed in' to the flows of everyday existence. Deleuze illustrates this by referring to the technology as the password. The password is a self-explanatory tool for the control society; the credit card, the passport, the reward card, the identity card, the electronic ankle tag. Even the body can operate as a password, as with biometric technologies.

Felix Guattari imagined a city controlled by mechanism, in an open environment. Everyone owns an electronic card, that gives access or barriers one to areas; one's apartment, one's street, one's neighbourhood. The computer tracks each person's position, 'licit' or 'illicit' and draws conclusions.

Control societies resemble networks of privatised consumption and information; circuits of desire and lifestyle, linked to databases deriving conclusions and sorting risk profiles, giving access and status. It creates privileged populations, who are able to enjoy the rewards of credit, mobility and information, filtering out the risky and excluding the remainder [Walters, W., p. 192, 2006].

Thus the dividual leads to social division. The 'underside' of society is either abandoned or forcibly placed outside the circuits of consumption and lifestyle, denied the assurance of tolerability and having a purely negative value [Walters, W., p.192, 2006]. These populations are excluded, but at the same included in the control society. They are included for certain 'scandals' and images such as 'welfare cheat' or 'undocumented and non-citizen labourers', the 'outsider', and 'they' are particularly interesting for security, risk management and societal protection.

Diagram

Deleuze sees control rather as a 'diagram' than a form of society. According to him diagrams are necessary to abstract and are meant to express "something at work in many different institutions and situations, spread out in several countries, working in a manner not given in the map of social policies and prescriptions, planned as such by no one" [Walters, W., p. 193, 2006].

The difference in a disciplinary society and a control society in the prison can be seen in the form of penalising subjects substituted with electronic collars that force the convicted person to stay at home during certain hours [Deleuze, G., p. 7, 1992].

7 Biometrics and the Effects on Consumers

As stated in previous chapters, the use of biometric technologies is quickly becoming widespread and becoming a standard part of modern life especially commercial and governmental entities embrace the technology as the solution for security, fraud and improved identification. Particularly after September 11 2001, governments are increasingly focused on the development of foolproof identification and tracking systems turning to biometric technologies as one of the key solutions to fight terrorism. Commercial use of biometrics has simultaneously been encouraged in order to fight fraud and related crimes. Shortly it is said to have many advantages, however biometrics could have serious negative consequences. Here I will give some arguments in order to answer my main question: *Which functions do biometric technologies have in society and how do end-users eventually internalise these technologies?*

7.1 Organisation's Perspective

From an organisational perspective biometric identifiers are attractive, because they generally do not change over the lifetime of an individual; they cannot be shared and they cannot be acquired through computer hacking or secretly observing. In reality this means that employees cannot punch each other in on a time clock, criminals can be identified regardless of what identification cards they have stolen or forged, terrorists can be denied from boarding aircrafts and healthcare providers can be relatively certain that the patient they are treating does indeed match the name on the insurance card and medical history file and moreover the patient will receive the correct treatment [in case of the VeriChip, the implanted chip].

7.2 Consumer's Perspective

From a consumer perspective, biometric authentication also offers advantages. Once you have enrolled in a biometric system, consumers are likely to be free from worries about the fraudulent use of their credit cards. One is able to make payments without carrying any cash or other identifiers, just your fingerprint will suffice. A stolen car will only be useful to a few smart thieves, because access is biometrically controlled, reducing the interest to steal. Furthermore one would not need to remember passwords anymore.

7.3 Dangers of Biometrics

The biometric industry has hyped biometric technology as the end solution for all sorts of security problems. However there is limited discussion about the potential harm that biometric identifiers could bring. Consumers could face real threats, but unfortunately the inadequate discussion that occurs is mostly focused on biometric efficacy with some discussion of privacy implications. Perhaps one of the most important characteristic of

biometric data is their irrevocability. If a password or security code is exposed or a key is stolen, then the individual can still select a new password or change locks, but if a biometric is exposed, there is real serious problem; the individual cannot change the physical characteristic on which biometric is based. One cannot grow new fingers or change one's iris pattern.

Consumer Implications

The rapid growth of biometrics has especially created a great concern regarding privacy and the effectiveness of the system among special interest groups and some consumers. The biometric industry is not going to announce the disadvantages of biometrics and the marketplace is not likely to provide sufficient incentive for industry to correct system deficiencies. Primarily because buyers of biometric systems are not willing to bear the many costs; these costs will rather be borne by the consumers.

Privacy

One of the main concerns of biometric technology is the storage and maintenance of data files. Storage issues are especially important from a consumer perspective, unlike other identification methods, such as identity cards and passwords, biometric data cannot be erased and replaced. If someone's fingerprint is exposed by data theft or an alteration is made, there are hardly any possibilities to correct or undo the damage. Many members of the population are becoming increasingly worried about the use of biometrics; afraid that the system will not function properly and make life more complicated. There is a certain resistance to change everything in society, especially among the more senior members [Simpson, I., p.6, 2006]. People already feel that they are violated if their credit cards are used without authorisation, how will they feel when their fingerprints are used in a similar way?

Security means that people do not need to be frightened or to be harmed in their public and private environment by criminals or terrorists.
Privacy in contrast to security does not have a clear unanimous meaning. It is therefore seen as a weak right in comparison to the term security, which is considered as a much stronger right.
Many definitions and concepts exist of the term privacy, but none of them can be applied on each and every situation. Nevertheless there are some general rights which can be extracted from the privacy concept.

At first privacy means; *the right to be left alone.* This means that other people do not have the right to disturb someone who is in a secluded area, like in the premises of its own house. Therefore if people are in a private area, they have the right to seclude themselves from others. Others ought to leave them at peace [Agre, P., p. 744, 2003].

Secondly privacy also means *the right to have access to your own personal data.* This means that everyone has the right to know which organisations, government authorities have gathered information. Moreover one has the right to claim and look into that data. This has been incorporated in the *Personal Data Protection Act* [CPB] and is therefore legally grounded. This also means that people want to have a say and autonomy on one's data, because people are concerned of what will happen with their data and how it will be used [Agre, P., p.744, 2003].

The last form of privacy is *the right to abstain certain data from public knowledge* [Darren, C., p. 247, 2002]. This generally means that religious and sexual preferences, but also financial information should remain private. Furthermore some people prefer to keep their political preferences for themselves.

Another classification of privacy has been developed in a study 'security' versus 'privacy' [ICTWeb, 2005]. Two future scenarios have been laid down in which various forms of privacy have been distinguished:
Spatial privacy is concerned with the private environment. The emphasis lies in the form of privacy; one should be able to be completely oneself, without any reservations in its own house.

Physical privacy gives an individual the right to do whatever one wants with its body. This means that a person wants to have autonomy over one's body.

Relational privacy gives one the freedom to start and maintain relationships. One component of this form of privacy means that one is able to communicate in public by means of mobile phones or by using electronic media, such as the internet.

Another alternative term to privacy is data protection. Data protection is similar to the concept 'information privacy', the classic definition is: the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others [Lyon, D., p. 176, 2001].

As described in Deleuze's control society, surveillance is not longer carried out in an analogue, but a digital manner. People are no longer recognised in these systems by their names, but are linked to a code, or number, such as the social security number, membership number. This numerical 'language' [existing of codes] either grants access or denies people from information. In this way, one can claim that one's privacy is not jeopardised, since it is not the individual itself being observed [the person remains anonymous], but the code related to the individual. In such a case not the individual but the dividual is observed.

Basically dataveillance does not necessarily have to intrude into a citizen's privacy. An example is registering all telephone conversations; phone numbers, the location and the

duration of the phone call. In the Netherlands all mobile conversations are kept in databases. This data is only released the moment someone is suspected.
The privacy is only violated if the police or judiciary system claim data of a suspect and at a later point it appears that this person in question is innocent. In such a case the data is linked to an individual and is no longer anonymous.

However the widespread use of biometric data collection does pose a privacy concern, because it threatens the anonymity that many individuals carefully guard. Even though internet tracking is 'anonymous', it is a disturbing idea that one's movements and everyday behaviour is tracked by commercial or governmental entities. “Genuine freedom means not only the freedom to choose, but also the freedom to be left alone, unburdened by the scrutiny of watchful machines or people. When individuals can no longer behave anonymously, real freedom is threatened [Langenderfer, J., Linnhoff, S., p. 332, 2005].”

What one can see here is that biometric technologies are now driven by consumer culture dictated by commercial and financial pressures rather than privacy concerns. Therefore no privacy principles have emerged yet to govern biometric data collection, storage, exchange, security and accuracy. If no regulatory system comes up soon, it could lead to real consumer harm, as each commercial or governmental entity approaches these issues in its own way with its own set of priorities.

In relation to biometric data I consider this form of privacy the most significant: Privacy is the ability for an individual to control the use of their own personal data, wherever it might be recorded [Fleming, S.T., p. 131-132, 2005]. Biometric data is personal data private to an individual and therefore required to be protected from abuse. Privacy of biometric data is only assured if it is never stored as raw data.

It is important to be aware of the use and implications of biometric systems: aware that biometric systems are used; aware of the purpose of the data collection and aware of future implications and usage of that data. Especially indirect forms of biometrics can be risky for privacy, since there is no enrolment process required and scans can be taken from a distance without the individual knowing that he or she is being monitored by iris scans or facial scans.

Thirdly consent is very important for the user. It gives the user some control over the enrolment and attainment of the biometric data. It is a mutual agreement between the administrators of the systems and the users to agree on the purpose of the system and that it is not imposed as a necessity. The individual is aware that biometric data is being collected, but also knows that it can only be used with their consent and cooperation.

Errors in Biometric Devices

Error rates in biometric systems are also a cause for concern, because they determine how well a system actually works on a day-to-day basis. From a consumer perspective, it is really important, or the toll could be relatively high. Errors can either result from device malfunction or attempts to fool the security measure. It is widely publicised that fingerprint scanners can easily be fooled with melted gummy bears and silicone fingers.

Another error that could lead to serious problems is when for example face recognition systems are placed at airports to improve security by 'flagging' potential terrorists, and the fails to detect a match and allows a terrorist to travel. This could have fatal consequences. In a reversed situation a system that wrongly flags a non-terrorist as criminal, it would threaten the civil liberties. This is of great concern, if one considers that even a system with 99.99% accuracy rating would wrongly flag more than 100 individuals per month for detention if more than 14 million passengers would be screened. Another problem here is that people assume that biometric data are 100% error free, but virtually all data sets of a given size contain errors. Biometrics is often seen to be immune of such problems.

Another difficulty with biometric authentication is that for any biometric system, there will always be some people in society who will not be able to enrol, due to missing fingers, limbs, cataracts etcetera. Therefore all systems must also be equipped with some process for exceptions, introducing a human element into the system, which could lead to traditional errors involved in human decision-making processes.

Database Attacks

Other complications to be considered are cases in which authorisation is granted to individuals based on the comparison of enrolled biometric data, with data acquired from an individual at the point of authorisation [Fleming, S.T., p. 125, 2003]. For example if a malicious individual attacks the database where all enrolled biometric data is stored, the attacker could substitute their own biometric data for that of an authorised individual. They then show their biometric data; the system matches it with the substituted data and the malicious individual becomes authorised and can enter. The original individual is locked out and must repeat the enrolment process.

In a second case the biometric data of an individual is captured by a malicious attacker and makes a copy of it. This does not need to be a perfect copy. It just needs to be good enough for the biometric scan. The malicious attacker then shows this copied data to the biometric scanner and gains access, by pretending to be an authorised individual. Especially fingerprint and voice recognition systems are vulnerable for such attacks.

Exchange of Data

Another major concern of biometrics is the exchange of data. For example insurance companies share data with each other for claims and security purposes. Financial; institutions share data with 'affiliated companies' for marketing purposes. Naturally many

ordinary merchants and nonprofits sell customer lists including personally identifiable information. Although all this data sharing potentially provides a consumer benefit in the form of additional choice and lower prices, there is also a cost in terms of decreased privacy. This is of course especially uncomfortable in the case of biometric data, because it is worrying to what extent personal information is collected ad shared by governmental and private entities. Imagine if fingerprints records from commercial applications such as grocery are matched with criminal files, some criminals would certainly be caught who would have otherwise evaded detection. However there is a price to be paid by citizens, to live in a society where nobody ever gets away with anything. Nowadays parking violators are ignored by law enforcement except in most extreme cases. With biometrics they might be vulnerable to instant detection and arrest in a society where fingerprint matching and law enforcement records are routinely shared. This leads to an intrusive society in which the government knows perhaps too much.

Intrusive Society

Even though the goal seems to stop crime, the question raises whether such a society is desirable to live in. If there is no legislative or voluntary limit on the exchange of biometric data, government[s] and private users could share databases; it might be possible for some organisations to track virtually every movement of every individual as they pass through various biometric checkpoints. For example a consortium of private companies could share data for the purpose of tracking the spending habits of consumers and delivering advertisements and coupons. Internet surf tracking and online ad serving is already common. This data could then be commercially exploited.

One can especially see when potential harm in society is expressed; courts are faced with a law enforcement petition for data access. Courts hardly resist when vague concerns about broad social implications are competing with an immediate genuine harmful threats, especially if it is related to terrorism or other national security matters. The threat of terrorism has already been successfully used to justify a wide scale of privacy intrusion, unknown before the September 11th attacks, such as the USA Patriot Act 2001. Political arguments are usually much stronger: 'Whose side are you on, ours or the terrorists?' Moreover once data is used for one law enforcement it is easy to expand the use to all law enforcements under the guise 'to make society a safer place'.

Moreover consumers are willing to accept some loss of privacy in exchange for enhanced security. As seen from my research, some of the end-users gave arguments that they did not mind giving away their data, since they had nothing to hide anyway. However the problem with biometric data is that the choice to share data is not left to the consumer, but is made for her. Additionally security enhancement is usually a benefit for the organisation, but the privacy cost is paid by the consumer. Privacy loss is dangerous and unfortunately consumers are often unaware under what kind of scrutiny they are until it is brought to their attention. Only then do they become perceptive of any invasion.

Biometric identification can only be effective in capturing repeat offenders, who have already been caught before and enrolled in the system. Even though the goal of a more secured society may be important, the existence of such a database is somewhat disturbing. Even more so when ordinary citizens who have not done anything wrong, are being scrutinised and watched, it poses a privacy threat to all; it could open doors to potential abuse.

7.4 Critical Outlook on the VeriChip

Critics of the VeriChip claim that the VeriChip databases may become linked to other private and public databases. The interlocking of databases makes complete profiles on any consumer available. The problem is that these extensive databases are a tempting target for criminals. Also, companies who gain access to the information could use it secretly to make employment decisions. Introducing the VeriChip creates the potential for a person's medical history to be included in these cumulative databases. In the end, consumers have little reassurance that VeriChip databases will remain private and separated from other databases and data brokers. Consumers who are considering implanting the VeriChip should be weary as their personal information could be exposed.

Privacy

Katherine Albrecht, founder of CASPIAN [Consumers Against Supermarket Privacy Invasion and Numbering] recognised as one of the world's leading experts on consumer privacy believes that a MedicalAlert bracelet or health card is a viable alternative to the VeriChip. However proponents of the RFID technology state that the VeriChip cannot be lost, stolen or misplaced, reasons why a bracelet or a health-card no solution, since they are usually missing at the critical point. As a result VeriChip Corporation stands firm in its opinion that this technology is the only solution to retrieve critical patient information.

A VeriChip system, stores identifying information in databases, which could be stolen by identity thieves, or merged with other databases or simply used unethically. The most critical part of the VeriChip is the personal information linked to the VeriChip's serial number. Opponents of the VeriChip claim that the databases may be linked to other private or public databases. The linking and merging of various databases has become a very lucrative business. These interlocking databases create complete profiles on consumers. Such biographical sketches might include name, address, social security number, credit reports and—with the addition of VeriChip databases—even medical records. Third parties could link other information such as the books that one purchased or some other relevant financial information. Companies, such as the data broker ChoicePoint, will start maintaining databases of RFID numbers and their associated parties [Laczniak, S., p.3, 5, 11 2006]. Moreover unauthorised parties could even monitor the movements and transactions made by individuals. In February, ChoicePoint accidentally sold confidential information on 145,000 people to identity thieves posing as legitimate businessmen. These extensive databases are especially tempting for criminals. But what if employers also get access to

these databases and help make promotion and hiring decisions based on that information. In the end it is difficult to reassure whether VeriChip databases will remain private and separated from other databases and data brokers.

Health Risks

While VeriChip Corporation claims that the device is completely safe, critics warn consumers of several health risks related to the chip. The VeriChip is subjected to a number of additional safety standards related to tissue compatibility, magnetic resonance imaging [MRI] compatibility and overall performance. The potential risks related to the device are: negative tissue reaction, migration of the implanted chip, failure of the implanted chip, failure of inserter, failure of electronic scanner, electromagnetic interference, electrical hazards, MRI incompatibility and needle stick.
There is especially potential risk involved with MRI, it is a common imaging technique used to diagnose all sorts of diseases and the procedure can be life-saving.

Security Risks

VeriChip claims that its device is completely secure; however experts hold a contrary position. As with almost any technology, the VeriChip is still 'hackable'. According to Bruce Schneier, a security expert, various parties could track VeriChip users [Laczniak, S., p.11, 2006].

The VeriChip is vulnerable to spoofing attack. This means that an attacker scans a VeriChip, or eavesdrops while it is scanned. Thus an attacker can easily spoof a reader into accepting the simulating device as the target VeriChip. In principle an attacker can simulate a VeriChip on the basis of its serial number alone [Halamka, J., Juels, A., e.d., 602, 2006]. Normally RFID tags can be uniquely identified by their 'collision avoidance signal' a special identification number. This signal allows RFID scanners to work when there are multiple RFID tags within range of the scanner. When there are many tags in range of the scanner, each tag behaves uniquely based on its collision avoidance signal. Thus the scanner knows which chip is which. However a high-tech criminal could steal or mimic a person's VeriChip, by reading and replicating the device's transmission data and collision avoidance signal.

8 Discussion

One can see the long history of intercepting communications. It is one of the oldest methods of surveillance.

The biggest surveillance system ever established is ECHELON, a global spy system created by the U.S. national Security [NSA]. It is an international electronic eavesdropping network run by intelligence organisations of the U.S., U.K., Canada, Australia and New Zealand. It is said that the first ECHELON network was built in 1971. The existence of ECHELON was first publicized late 80s. Since 1990 the development of the network has continued on an ever-increasing basis [Campbell, D., p. 149, 2000].

ECHELON is used to capture and analyse virtually every email, fax, telex, telephone communications carried over the world's telecommunications networks. It is said that it can intercept almost any electronic communication. Some estimate that it has capabilities to sort through up to 90% of all internet traffic. ECHELON, designed during the Cold War, was primarily used for non-military targets, such as governments, organizations, businesses and individuals in every country. The focus changed from espionage to surveillance of terrorists, orgainsed crime, domestic political groups, considered to be a threat, diplomatic negotiations [Hager, N., Mediafilter.org, 1998, Q&A,BBC News, 2001].

This systems works by intercepting large quantities of communications; it uses computers to identify and extract messages of interest. These computers automatically search through the millions of messages, containing pre-programmed keywords. Keywords could include all the names, phrases, words, locations, subjects or anything the intelligence service regard 'suspicious'. This helps the intelligence agencies to create a picture of the communication between various networks of people which require watching. Flagged documents are forwarded to the respective intelligence agency [Poole, P.S., 1999].

After September 11th these internet surveillance systems, a large system of international monitoring of all communications, fax, telephone, telex and email became grew to a much larger extent. Since then companies are willing to cooperate in the 'war against terror', by complying to requests for data even before the warrant has been issued, suggesting that the continuous 'state of emergency' has been accepted [Lyon, D., p.669-672, 674-675, 2003, Lyon, D., p. 172, 180, 2001, Fleming, p.125, 136, 2003, Langenderfer, J., Linnhoff, S., p. 325, 330, 332-334, Migani, C., p.4, 2005].
Search engines check messages for key words and contexts in quest of suspicious or risky communications. However these are used not only for military or terrorist threats. They are also used by police departments trying to prepare for protests such as those by anti-globalisation groups, but also as a means for commercial intelligence.
The problem here is that our day-to-day transactions and conversations are under scrutiny and they may not even catch terrorists, but they do complicate life for everyone, especially

since we are monitored, classified, categorised and evaluated continuously. Above that, biometric technologies have been introduced into our daily life.

As seen from the previous chapters, there are still many questions to be answered regarding the complex biometric technological scene.

Due to the fewer transactions and interactions based on face-to-face relationships, new 'tokens of trust' have come in place. Hence the PIN, barcodes, signatures, photo IDs are replaced by biometrics. Human beings are abstracted and have become data in various flows and networks of surveillance systems.
These high technology societies relate data to our daily activities by collecting, storing, checking, exchanging and using in order to determine some eligibility or access to persons, places, experiences or events.
As Lessig states: 'The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again' [Lessig, L., 154, 1999]. The point is that searchable databases 'make people up'; it reinvents each person as a unique individual in the system by capturing personal details within a set structure.

To finally come back to my main question: *'Which functions do biometric technologies have in society and how do end-users eventually internalise these technologies?'*

Biometrics is seen as the solution against terrorist attacks and other threats, but at the same time creates a danger for a democratic society. These technological solutions, as explained in foregoing chapters, are dangerous because of some key trends:

A. The centralisation of state power and social control over society
While there seems to be a very great 'care' motive for implementing biometrics; it appears that it is in favour of an increased 'control'. This trend is inevitable, but a trend which could become a serious threat for society.

B. The increased capacity to discriminate between different classes of persons, using biometrical surveillance
This biometrical system deepens the process of social sorting, categorisation. It is a way of including and excluding, accepting and rejecting people of worthiness and unworthiness. Personal data is abstracted into information and assessed into risk or non-risk groups, giving privileges to some and disadvantaging others. Furthermore these biometric technologies intend to classify and discriminate between different groups of people. They are intended to check for illegal immigrants or other persons in transit who have inadequate documentation. There is even evidence that after September 11th that especially Arab and Muslim people are singled out for negative treatment, including lengthy detention without charge or trial.

C. The relative lack of accountability of these systems

These new ID cards and new methods of identification are introduced; however it is still possible to fool these technologies. If central databases are used, they are very vulnerable to attack. Then there is still the biggest difficulty, suicide bombers do not strike twice. How can one pick terrorists out of crowds? Does the biometric match anyone in the crowd? So even though a whole surveillance network is set up, the criminal or terrorist has to be known in the database. Terrorists do not pose for photos and are likely to use evasive techniques and disguises, because human beings are more flexible and imaginative than technologies. Eventually any technology can be outwitted given time and ingenuity. Thus it is unlikely that the terrorists will ever find their way onto suspect lists.

D. The willingness of populations to accept these technologies as the 'price of security'

According to Henk Attema, director of Secure Access Road [SAR] biometric entrance system are still not fully accepted in the Netherlands [Security, July 2007]. Here we are lagging behind in the acceptance of biometric technologies; however one can see an increasing interest among private companies taking these technologies up as a security solution. However the majority is ready to accept these technologies, for they prefer to give up their privacy for a more 'secure' life.

To come back to the case studies I used for my research one can conclude that they follow a similar trend as mentioned above.

As stated in **point A**; all three case studies motivate the implementation of biometric technologies in their public space for security purposes. In the Baja Beach Club they state that the customer is safe, because one will not need to carry one's wallet, so one cannot be robbed. In the other two cases, they want to keep troublemakers out of their club. Therefore they claim that for a safer and better environment it is important to apply these security systems in order to have a more pleasant situation than before, because of their 'care' for the customer. But it is quite evident that their motivations are quite different than they claim; they are especially interested to bind their customers to their club. Finally the customers' data is mostly used for marketing strategies. In the case of the Baja Beach Club it seems that it was a big media stunt, since they received worldwide media attention.

Point B states that there is an increased differentiation between groups of people. In all three case studies one can see that people are being categorised. In the Baja Beach Club, people are being differentiated as VIP-members, people who are chipped and the regular visitor. The VIP-member is a privileged customer with a special area for VIPs only and custom-made services. In the other two case studies a distinction is made between non-members and members. Members receive discounts at the entrance; get special [free] invitations and can save credits for discounts on products in the web-shop. Moreover people can be put on a blacklist categorising people in risk and non-risk groups. In de Fakkel [the swimming pool case], many people of Moroccan origin used to visit the swimming pool, but they have stopped coming there. Instead of involving them in

discussion and going into a dialogue with them, trying to adjust their swimming pool behaviour, the 'problem' has shifted to other swimming pools. It has become a matter of control rather than trying to acquire the desired norms and values.

In **point C** the lack of accountability is addressed. In none of the case studies the technologies are airtight. In the disco [Alcazar] the biometrics system can easily be by-passed. If one does not want to be a member, he or she can always enter as a non-member. In that way, if the individual is a troublemaker and is not enrolled in the system, the individual has normal access to the disco. However the individual can be blacklisted if he or she makes trouble. Yet there is a leak in the system; if one is thrown out of the disco, the bouncer will have to ask the smart card. Many times the individual does not hand in the smart card, or the bouncer does not even ask for it. Consequently the bouncer depends on his memory and has to go to the database, see whether the troublemaker is enrolled in the system, if so, only than can the individual be blacklisted. Of course this is a very vulnerable procedure and errors can easily slip into this system. In the case of the Baja Beach Club, the VeriChip can be spoofed. The signal can be intercepted and one could have access to sensitive data, such as the amount of money on the chip and one could even impersonate to be the person in question.

In the last **point D** it is clear that the end-users are willing to give away their personal data as they see it as a price for their security. When I asked them, whether they knew what happened to their personal data, none of the respondents knew what happened with it. Moreover they trust the clubs for their integrity and the handling of their personal data with care. Finally I laid a scenario before the end-users; "What if your personal data is shared with third parties?" None of the end-users was happy with this scenario and everyone was worried about such a situation. Thus only after explaining them this scenario, were the end-users aware about this possible situation.

Recommendations

Biometrics has the potential to improve security without jeopardising individual's privacy. It may even be possible that data is stored securely and exchanged between commercial and governmental entities with a court order and that these technologies are only implemented if it offers a real advantage to individuals, outweigh the costs, accuracy is fully tested and guaranteed before implementation.

The dangers of biometric data being exchanged can be reduced if data is not stored centrally or if biometric templates are not reversible and thus cannot reproduce the biological features from which they are extracted. Because once biometric data has been compromised, biometric data cannot be revoked. Therefore it is very important to use strong encryption to protect biometric data during storage.

Another solution is to store the biometric data separately. A portion of the biometric data will be stored centrally, while a matching and necessary portion of the biometric data is stored on a smartcard, carried by the end-user. In that way no individual has access to the

entire data. Consequently it is not possible to make any reconstructions of the biometric without having access to both databases. A hacker in this way will only have one part if the data and will be unable to duplicate anyone's biometric information.

The government has a big role to play as biometric technology is becoming common in a day-to-day life. Some regulation is required in order to provide protection to the consuming public. Here are some recommendations:

- No biometric data should be collected by a private entity without notice, or in the case of government collecting data, no secret collection should be allowed without a court order.
- Biometric systems should not be compulsory, except in criminal cases.
- One should try to partially store biometric data in a decentralised manner, such as on smartcards carried by individuals.
- Biometric data should be stored in encrypted form to lessen the possibility of the data being exposed.
- Data should be stored using templates that cannot be reconstructed to the original biometric feature.
- Biometric data should never be shared with other entities without the consent of the enrolled individual, except for serious crimes.
- Biometric systems should explicitly acknowledge the possibility of errors and create a method to correct these errors.
- Biometric authentication should only be used when necessary for the security of a company or other entities.

Furthermore it is very important to create awareness [Migani, C., p.4, 2005] among end-users about biometric systems. They should be informed about privacy concerns; moreover they should have the last say about their biometrical data. End-users should know what the possible effects are if their data is being used.

Literature

Agre, P., [2003], 'Surveillance and capture: Two models of privacy', Wardrip-Fruin, Noah, Nick, Montfort, *The New Media Reader,* Cambridge: MIT Press, 2003, pp. 737-760.

Alcazar, [2007], http://www.alcazar.nl

Amersfoort, R., Buuren, J., Kalkman K., Schans van der W., [2006], '*Onder druk, Terrorismebestrijding in Nederland'*, Jansen & Janssen dosier 2, Papieren Tijger.

Anderson, J. R., [2001], '*Security Engineering: A Guide to Building Dependable Distributed Systems'*, John Wiley & Sons, New York, chapter 13, pp. 261- 276.

Artz, S.M., [2002], 'Beveiliging van Persoongegevens, De wet bescherming persoonsgegevens en biometrie: privacy, een technische vraagstuk?' *College bescherming persoonsgegevens.*

Baja Beach Club, [2007], http://www.baja.nl

BBC News, [29 May 2001], 'Q&A: What you need to know about Echelon', http://news.bbc.co.uk/2/hi/science/nature/1357513.stm

Binnenmaas municipality, [2007], http://www.binnenmaas.nl

Bocozk, K.; Buster, C. J.; III, S. F.; Vacca, E. E.; Welsh, J. & Wulf, T. [2005], 'Biometrics: Networks and Telecommunications In Business',

Burrows, R. & Gane, N. [2006], 'Geodemographics, Software and Class', *Social Class and Other Classifications* 40[5], pp. 793-812.

Campbell, D., [2000], 'Global Surveillance: the Evidence for Echelon', '*Computers, Freedom and Privacy, Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions'*, pp. 149-154.

Central Bureau for Statistics [2006], Statline, Puttershoek.

Central Bureau for Statistics [2006], Statline, Ridderkerk.

Central Bureau for Statistics [2003], *Binnenmaas op maat 2002*.

Centrum voor Recht, Technologie en Samenleving, [2005], 'Veiligheid en privacy in 2030: twee toekomst scenario's', Tilburg: Universiteit van Twente, *ICTWeb. Universiteit van Tilburg.*

Charters, D., [2002], 'Electronic monitoring and privacy issues in business marketing: The ethics of the Doubleclick experience', *Journal of Business Ethics,* Vol. 35, pp. 243-254.

Deleuze, G. [1992], 'Postscripts on the Societies of Control', October 1992, Vol. 59, *JSTOR*, The MIT Press, Cambridge, pp. 3-7.

Deleuze, G. & Guattari, F. [1987], '*A Thousand Plateaus'*, Minneapolis: University of Minnesota Press, pp.3-28.

Donselaar van, J. [2006],'Gemeenteraadsverkiezingen 2006 - Official website Anne Frank Stichting', http://www.monitorracisme.nl/content.asp?lid=1&pid=99.

Ench, C., [2006], *'Win doze'*, http://www.enchgallery.com/fractals/fractalpages/windoze.htm

Food and Drugs Administration, [2004], http://www.fda.gov

Fleming, S. T. [2003], '*Biometrics: past, present and future'*, IGI Publishing, Hershey, PA, USA.

Friesen, N., [2006], 'Experiencing Surveillance: A Phenomenological Approach', *School of Communication,* Simon Fraser University, Vancouver.

Fuller, G. [2003], 'Perfect Match: Biometrics and Body Patterning in a Networked World', *Fibreculture Journal*.

Gane, N. [2006], 'Geodemographics, Software and Class', Vol. 40[5], *Sociology,* Sage Publications, London, Thousand Oaks, New Delhi, pp. 793-812

Garfinkel, S. & Holtzman, H. [2005], '*RFID: Applications, Security, and Privacy'*, Addison Wesley Professional., chapter 2, pp. 15-36.

Giddens, A. [1991], '*Modernity and Self-identity: Self and Society in the Late Modern Age'*, Stanford, California, Stanford University, chapter 2.

Graham, S. [2004], 'The Software Sorted City: Rethinking the 'Digital Divide'', *The Cybercities Reader,* London: Routledge, pp. 324-331.

Guizzo, E. [2006), 'Loser: Britain's Identity Crisis [biometrics ID cards]', January 2006, Vol. 43[1], *IEEE Spectrum Magazine*, p.42-43.

Haaster van, F. [2003],'Kennismaking Biometrie', Technical report, Bedrijfskundige Ontwikkeling van InformatieVoorziening -- Haagse Hogeschool, Sector Informatica.

Hager, N., [1998], 'Exposing the Global Surveillance System', http://jya.com/echelon.htm

Haggerty, K. D. & Ericson, R. V. [2000], 'The Surveillant Assemblage', *British Jounal Of Sociology* Vol. 51, pp. 605-622.

Halamka, J., MD, Juels, A., Stubblefield, A., MD, Westhues, J., [2006], 'The Security Implicatios of VeriChip Cloning', Vol. 13[6], *Journal of the American Medical Informatics Association,* pp.601-607.

Hier, S. P. [2003], 'Probing The Surveillant Assemblage: On The Dialectics Of Surveillance Pratices As Processes Of Social Control', *Surveillance & Society*, pp. 399-411.

't Hof [2007], 'What do RFIDs tell about you? A user perspective on Identity Management', *Rathenau Institute,* European Parliamant, Scientific Technology Options Assessment [STOA], pp. 1-7.

InfoMil [Senter Novem] [2007],'Artikel 25, lid 1 - In de badinrichting wordt gedurende de openstelling in voldoende mate toezicht uitgeoefend', http://www.infomil.nl/aspx/get.aspx?xdl=/views/infomil/xdl/page&ItmIdt=29200&SitIdt=111&VarIdt=46.

International Biometric Group [2007], '*Biometric Market and Industry Report 2007-2012',* http://www.biometricgroup.com/press_releases/pr_2007_BMIR2007.html

Jechlitschek, C., [2006], 'A Survey Paper on radio Frequency Identification [RFID] Trends, pp.1-16 [http://www.cse.wustl.edu/~jain/cse574-06/rfid.htm]

Kappelle, I., and Schriemer, R., [2005], 'Klachten en meldingen over discriminatie in Rotterdam 2001-2005', Rotterdam Anti Discrimination Counsel [RADAR], http://www.radar.nl

Key, J.P., Oklahoma State University, [1997] http://www.okstate.edu/ag/agedcm4h/academic/aged5980a/5980/newpage21.htm

Laczniak, S. [2006], 'A "VeriChip" on Society's Shoulder: Positive and Negative Implications of the VeriChip', *Department of Engineering Physics,* University of Wisconsin-Madison, pp.1-17.

Langenderfer, J. & Linnhoff, S. [2005], 'The Emergence of Biometrics and Its Effect on Consumers', *The Journal Of Consumer Affairs* Vol. 39, 314-338.

Lessig, L. [1999], '*Code and Other Laws of Cyberspace',* Basic Books, Chapter 11.

Liberatore, A. [2007], 'Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union', *European Journal on Criminal Policy and Research* Vol. 13, 109-137.

Lips, M.; Taylor, J. & Organ, J. [2005], 'Electronic Government: Towards New Forms of Authentication, Citizenship and Governance', *Safety & Security in A Networked World: Balancing Cyber-Right & Responsibilities, The Oxford Internet Institute [OI]).*

Lyon, D., [2001], 'Terrorism and Surveillance: Security, Freedom and Justice after September 11 2001', *Privacy Lecture Series,* [http://privacy.openflows.org/lyon_paper.html]

Lyon, D. [2001], 'Facing the Future: Seeking Ethics for Everyday Surveillance', *Ethics and Information Technology* Vol. 3, pp. 171-181.

Lyon, D. [2003], 'Technology vs. 'Terrorism': Circuits of City Surveillance since September 11th', *International Journal of Urban and Regional Research* Vol. 27, pp. 666-678.

Mathiesen, T., [1997], 'The Viewer Society: Michel Foucault's 'Panopticon' Revisited', Vol. 1[2], *Theoretical Criminology,* Sage Publications, London, Thousand Oaks and New Delhi, pp. 215-234.

Migani, C. [2005], 'Is Biometrics "Big Brother" Watching You?', *Programming Fundamentals*, Ethical Issues in Computing, pp. 1-11.

Orwell, G. [1949], '*Nineteen Eighty Four'*, Secker and Warburg.

Plaggenborg, P., [2006], '*Social RFID, internet for things',* European Media Master of Arts, pp. 1-15.

Ploeg v. d., I. [2002], 'Biometrics and the Body as Information: Normative Issues of the Socio-Technical Coding of the Body', *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination,* Routledge: London and New York, pp. 57-73

Poole, P. S. [1999], 'Echelon: America's secret global surveillance network', http://fly.hiwaay.net/~pspoole/echelon.html

Prakken, T. [2005],'Naar een cyclopisch (straf)recht', http://www.burojansen.nl/artikelen_item.php?id=140 .

Privacy International [2006], http://www.privacyinternational.org/ .

Putte van der, T. & Keuning, J. [2000],'Biometric Fingerprint Recognition: Don't Get Your Fingers Burned', *IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, pp. 289-303.

Rotterdam municipality, [2007], http://www.rotterdam.nl

SAR [2007],'Secure Access Road', http://www.sa-road.com

Security [2007], http://www.security.nl/article/16424/1

Simpson, I. [2006], 'Biometrics: Issues and Applications', *6th Annual Multimedia Systems, Electronics and Computer Science, University of Southampton*.

Smith, A.D. [2005], 'Exploring the acceptability of biometrics and fingerprint technologies', Vol. 1 [4], *International Journal of Services and Standards,* Inderscience, pp. 453-481.

Srivastava, L., [2005], 'Ubiquitous Network Societies: The Case of Radio Frequency Identification', *International Telecommunications Union,* pp. 1-36.

VeriChip Corporation [2007], http://www.verichipcorp.com/company.html.

VROM [2007],'Ministerie van VROM', http://www.vrom.nl/.

Walters, W. [2006], 'Border/ Control', Vol. 9 [2], *European Journal of Social Theory,* Sage Publications: London, Thousand Oaks, CA and New Delhi, pp. 187-203

Weber, K. [2006], 'The Next Step: Privacy Invasions By Biometrics and ICT Implants', *Ubiquity - ACM IT Magazine and Forum* Vol. 7.

Wikipedia [2007],'Facial recognition system', http://en.wikipedia.org/wiki/Facial_recognition_system.

Wikipedia [2007],'Smart Card', http://en.wikipedia.org/wiki/Smart_Card.

Wikipedia [2007],'Michel Foucault', http://en.wikipedia.org/wiki/Michel_Foucault.

Ziegler, R., Mitchell, D.B., [2003] 'Aging and Fear of Crime: An Experimental Approach to an Apparent Paradox', *Experimental Aging Research* Vol. 29 [2], p.175.

Zournazi, M. [2002], '*Hope: New Philosophies for Change'*, Chapter 10, Navigating Movements, A conversation with Brian Massumi, Routledge, New York, pp. 210-242.

Zureik, E. [2004], 'Governance, Security and Technology: The Case of Biometrics', *Studies in Political Economy* Vol. 73, 13-137.

Appendices

Interviews Suppliers

Interview with Gerben Bazuin van Secure Access Road B.V. 2 May 2006

Alcazar is the local mega disco in Puttershoek, a village close to Dordrecht in the Hoeksche Waard. It has a capacity of 5000 people in one night. Every Saturday the place is packed with young people coming from different places. The population of Puttershoek is 6000 people. About 10% of the village is member of Alcazar.
Alcazar exists 25 years now. It slowly grew from a capacity for 600 people to 2000 people; after the third rebuilding it now has a capacity for 5000 people. Every Saturday 300 new people come to visit Alcazar, sometimes even from Belgium and Germany.

Troubles started a few years ago; on an average evening there used to be 15-20 incidents with the visitors. The owner had to employ 30 bouncers for one evening.
In 2000 Alcazar approached a company in Arnhem, as they saw a solution in biometrics for this problem. But the system didn't function properly. It was not stable and they were not able to solve the problems.
Gerben and his friend were working behind the bar in Alcazar in weekend and studying informatics. One day the owner of Alcazar asked the boys, whether they couldn't do something. So they evaluated the project and saw the shortcomings and tried to advise the company. However the company didn't do anything with the rapport.

In 2002 they held their first pilot study. It was successful. The owner of Alcazar was interested to market the product, because he was sure that other discos and catering industries would be interested in this product. So they started their company end of 2002, beginning of 2003. Alcazar has a network of about 10 discos all over the Netherlands, where they have implemented this system.

Now they facilitate:

- 10 disco's
- 1 swimming pool
- 3 coffeeshops

They are negotiating with banks and with some companies in Belgium and Turkey as well. Also a new project together with InterPay is being developed.

Mostly the SarFunGuard Totem is used. It is a pillar, in which two biometric systems are integrated. It is a combination of a face scan and a finger scan.
None of the biometric technologies are watertight yet. The iris scan is most reliable, but it takes a lot of time before you are registered. However with the SarFunGuard it just takes 15 seconds to get yourself registered into the system.
First of all a picture is taken with the camera built in the pillar. 16 pictures are saved and 4 are used for comparison. Next the visitor has to put his/ her finger on the finger scan. The user is asked to put his/ her finger 4 times on the scanner and all four scans are saved in the system. In the begin stadium the finger scan wasn't working well at all; people had to dry, clean their fingers; the optical sensors were dirty in no time, it made it unfriendly for customers to enter. People don't want to go through a lot of hassle in order to enter a disco. However this problem has been solved and the flow of people entering is fast again. 30.000 people have registered themselves at Alcazar.

A swimming pool in Ridderkerk a small town close to Rotterdam has also introduced the SarFunGuard Totem. Here they were especially having problems with Moroccans. 3% of the visitors raised objections against the biometric entrance system. Most of them were elderly people. They made a connection with the Second World War, especially because they didn't find themselves to be dangerous people; so why should we have these cards. But it was easy to convince this group of people to include them in the system; since there are advantages connected to the membership. If you swim 10 times, the 11th time you can swim for free. So most people are convinced by these discounts. The swimming pool has 10.000 registered people. In this swimming pool case it is an agreement with three parties; the police, the judicial power and the swimming pool of the municipality. Here the SarFunGuard Totem fulfils a public function. In practice it means that once you have been sent out of the swimming pool, you immediately get charged, since it is legally grounded.

The power of the system lies in three functionalities:

- Registration
- Identification process
- Verification process

In this system the face scan is used as identification process, 1-on-many, meaning to say that if a person stands in front of the pillar, your face scan is taken and it tries to identify your face from the list on the blacklist. This is done, because the system isn't flawless yet; it means that when a face is scanned and it has to compare 30.000 faces, the chances the system makes mistakes are big. That is why the system compares the faces from the blacklist, since there are about 165 people on the blacklist and the chances that a mistake is made are smaller.
Verification occurs when your fingerprint is put on the scan. It verifies with the system, whether your fingerprint matches the one in the database.

If you are recognized as a person from the blacklist the system starts beeping, entrance is not allowed into Alcazar. However if you have been drunk and have misbehaved in some way and you can come on a weekday to apologise. In such cases it is possible that you can be removed from the blacklist depending on the offence. Dealing in drugs, consuming drugs and fighting are absolutely prohibited. These people remain on the blacklist.

One can see that the incidents happening on an evening/ night at Alcazar have decreased. There are 70-75% less incidents on a Saturday night than before. Since the biometric technology has been implemented there are fewer incidents at Alcazar; the reason is that people are taken out of anonymity and behave more calm. The technology is not discriminating either, since every person gets a fair chance to enter the disco. Only if you misbehave you will be blacklisted.

In the case of the disco and the swimming pool it is proven that the performance of the SarFunGuard Totem has been cost-effective. Since there is order; one reduces the costs in personnel. Before there were 30 bouncers and now it has been cut down to 18 people. The same is for the swimming pool, at first there were six pool attendants and now there are three.

We work together with the Belgian company BioWise. The demand of biometric technologies is an interplay between the catering industry and companies into biometrics. We usually find our clients on fairs. One 'pillar' costs □10.000. If a client decides to take a network system, it will be cheaper.

In order to use the pillar one needs to insert a smartcard, this costs □3.50. The end-user pays □5.00 for the smartcard. Thus the costs can easily be covered. We also rather have 10 serious clients than 30 fools who just keep the Totem in a corner of their bar; since this would be bad for the name of our product. We especially focus on small medium-sized enterprises - SME's. Whereas other big companies in the Netherlands, such as Nedap, LogicaCMG and ...do projects for the government. Last year we managed to make a small profit. The total turnover last year on the biometric market was 330%.

Malasia and Canada are quite far with the technology; they use it at border passes and driving licenses respectively.

People are easily swayed, when we explain that it diminishes nuisance and trouble. In Ridderkerk, there were 15 people who were against the new technology in the swimming pool at the entrance. We spoke to all of them and explained about situations such as a 55-year paedophile and other harassing people and that it would make the swimming pool safer. They were all convinced, except for one particular strict Christian couple. It was against their believe to use biometrics, since the bible refers to it as the devil. This couple can enter the swimming pool without any usage of the Totem; everybody knows them in the swimming pool.

In Alcazar people don't make complaints out of principal grounds, rather they call up to say that they are fed up of sms's and emails from Alcazar. People can make their own profile on Alcazar's website.

At this point we are really glad, because we have a place at Alcazar where we can test unconditionally. Now we are experimenting with cameras in the main dance hall. We are also brainstorming about the smartcard. We might want to use it at the bar with a photo, but not for payments, since our public doesn't have much money. Since most of the visitors are youngsters, with little money to spend. All the money goes in their mobile phone and clothes. At this point to use the smartcard as a payment card is a second step. A third step would be to link the fingerprint at the bar for age limits.

We are not allowed to share the data from our database with other discos; at least that is the case in 'disco land'. However in swimming pools it is possible to share data with one another, because it is judicially grounded. Therefore if one is not allowed to enter one swimming pool, that person would not be able to enter any other swimming pool within that municipality.

Interview with Frank B.T. Wieland en ir. Hans J.W. Lammers van LogicaCMG

22 May 2006

Logica and CMG merged in 2003. LogicaCMG is a major international player in IT services. It employs 30,000 people across 36 countries. The company provides business consulting, systems integration and IT and business process outsourcing across diverse markets including telecoms, financial services, energy and utilities, industry, distribution and transport and the public sector.

I spoke with Frank B.T. Wieland – Project Manager and with ir. Hans J.W. Lammers – Consultant for the Public Sector.

LogicaCMG has had various clients. They did a project for the European Union; the VIS project, which integrates biometric characteristics in the visa, such as fingerprints and digital facial images. Also these procedures were used earlier with the Immigration and Naturalization service for foreigners. Furthermore they worked in the criminal law sector for the Ministry of Justice and Ministry of Internal Affairs in the case of identity fraud, when someone else is sent for the crime in jail, instead of the person convicted. Their major clients are the police, the government and the Ministry of Justice.

Since September 2001 they have also been involved with the private sector. The Schiphol airport has been their client in the Privium – iris scan project. In the nineties we played a role at Schiphol, for they wanted to speeden up the process at the customs. First they thought to implement a finger/ hand scan, but the match was not accurate, because of various disturbing factors, such as sweaty hands and people touching each others luggage, etcetera. So they adapted to the iris scan technology. Schiphol paid for all the costs. Moreover September 11 2001 was a good safety reason to actually proceed with the Privium service.

According to Frank and Hans biometrics can never be seen as total solution for safety. Currently the government, police and justice are our main clients.

We also mediated for Schiphol with the Privium project. Within the framework of efficiency we advised Schiphol to take this step for frequent flyers.

There is a tension; the US is hermetically closed, with many problems at the gate. At Schiphol the concept is service oriented.

In the 90s we played a role in the iris scan project, in order to fasten the process at the customs. With finger and hand one can quickly move on, but then it was found that clammy hands going all over suitcases it would not seem very reliable. So we decided to use the iris scan. All the costs are made by Schiphol.

11th September is often used as a reason to invest in biometrics. Since then we can see a growing trend in biometrics; however the question is: how to guarantee safety, and how to optimise this.

Actually when one uses biometrics, one needs to measure someone's 'biometric data' several times, in order to see 'changes' in the structure for example in the fingerprint etcetera, since biometrics indicates who you are.

Biometrics is used in various fields; by police, at the border on the base of enrolment. It is also used in casinos, catering industry and the like. Here the owner only permits those an entree if they are a known visitor. One is compared to the internal system, if one is not in the system, one cannot enter.

But how accurate is the technology? The iris scan, or for that matter any technology should have a right enrolment in which the whole process is fluid.
Face recognition is a technology which is time consuming; it is difficult to recognise a face from a distance. A shopping mall in Rotterdam a pilot study had been set up in order to test the patterns of movement.
At Heathrow another test had been conducted in order to photograph passengers at the airport; a poster of a nude woman was put on the wall; every passer-by was distracted and looked up, at the same time a photo was taken of the face.

At Charles de Gaulle one was forced to look up a certain angle, while going down the escalator, they accomplished this by emitting sounds from the escalator, the passer-by would look where the sound would come from and a photo was taken. It is important that the photo from the front is clear.

Video streaming sees people walking, and takes photos, without the passer-by noticing; it takes 3-D photos from various angles. One cannot identify, but one *can* recognise.

Nowadays more and more documents contain biometric data. People with bad intentions won't pick up their e-ticket themselves at the desk, but will rather pay someone to get the e-ticket.
But soon the e-ticket will contain a fingerprint, decoded on the magnetic strip and verify whether the person is truly the one in question. It also means that a lost ticket cannot be used by anyone else anymore.

If you are not known in the 'system', with biometrics it is impossible to estimate with whom one is dealing with.

We have been working with The Ministry of Justice in the criminal law branch. Personal details, biometrical data and other data, from various branches are searched , consequently one can get a good picture and one can link these various data with one another and make conclusions for example about the misuse of social services.

With camera surveillance, this data is sent to the police; in this manner the police can act more proactive instead of reactive, as is the case now.
For example in Amsterdam's city center, everywhere surveillance cameras have been set up, and one can read trends from these images. If a robbery takes place, one can reconstruct patterns, where someone was before or his/her daily routine etcetera. It gives one the opportunity to sort data, also called data mining, one collects vast amount of information about where someone literally might 'end up'.

The police focus on 'looking ahead' and use biometric technologies as a tool for accomplishing their objective. It is supposed to be purely supportive.

In another pilot study at a parking lot one tries to map patterns of walking and combine this with audio and facial data.

At the Amsterdam Police Headquarter at the Elandsgracht the command and control center contains 6000 photos of backsliders. Moreover people can also send in photos made by their mobile phones, which can also be matched with the system, depending on the quality of the photo. It means one can also ask photos, information, and data from citizens.

If there are 1000 people, one can say that there is 95% reliability on the technology. However one must keep in mind that technology has its shortcomings and cannot be used for all objectives.

For example in Australia one uses finger scans, but it doesn't have such a good enrolment, since the technology is not completely airtight. If one has the intention to falsify ones fingerprint, one can for example use wax or more extreme measures are burning of your fingerprint with acid.

The iris scan is the:

- Fastest
- Most reliable
- Most expensive biometric technology

At Schiphol-Oost, Dartagnan, partner of Schiphol Group have been developing the iris scan. They have been trying to set up a direct exchange of passengers between JFK-Airport and Schiphol for frequent flyers. This concept has been taken up at various airports and now one can see experiments going on with various biometric devices in all kinds of settings.

In Indonesia, a combination of the fingerprint and the iris scan is being used at the immigration at the airport.
The technology is developing fast; nowadays one makes an iris scan of both eyes, which makes the reliability even more accurate, secondly the procedure has been simplified too.

Biometrics are used for access control for buildings, for security in banks, for a gas company in Groningen as it is sensitive to terrorism, Shell in Rijnmond for personnel.
For a logistics company, they take the biometrical data from external people; so everybody is subjected to surveillance.

The idea is that you are known somewhere in a database, and the system checks whether the registered person is the correct person or not. For example when trying to find people from between the mass, with big cameras or using the iris scan or face recognition system for hooligans. But the facial recognition system is not airtight, since the hooligans can easily walk into the stadium, and one doesn't know who the hooligans *actually* are.

The iris scan is a very advanced technology; it can read the iris pattern through contact lenses, spectacles and sunglasses.

Biometric technologies can be applied at big events, as well at the border against terrorism, vandalism etcetera. However the technology is very expensive. At NEC 200 engineers are working on algorithms, which are very expensive and brings a lot of risks along with it.

In the Middle-East, Dubai and Portugal, identification on a country level, biometric characteristics are taken from citizens and stored in a central database. In the Netherlands only the police works with a central database, in which the identification of criminals is compared with the database. Verification is done with the biometric passport; this means that the identity is verified at the point of entry with the document you carry.
At this point justice has not allowed verifying fingerprints in crimes with the fingerprints stored in the database.

It is also easy to imitate and steal a biometric characteristic. However the iris scan is unique and moreover it is more reliable, as you cannot leave your iris scan behind (at the scene of a crime for example in comparison to a fingerprint). It is easy to leave someone else's DNA material at the scene of the crime and in that way mislead the investigation or even worse make someone else a suspect of a crime he or she did not commit.

People have to go a long with the time; this also means that we have to go a long with biometric technology. For example the KLPD, (the national corps police services), works

actively and preventive. They work with 10.000 cameras and it works preventive. If you think from the perspective of the region, these technologies are very effective.
But the common citizen doesn't see criminals being captured, but they do see cameras allover, on highways. Everywhere there is surveillance on the stream of goods and people. But how to handle these technologies, since one's privacy is in danger and everything is visible to 'others'.
The danger, which such executive systems is that the system says something; for example that the biometric characteristic does not match; the system interprets the information and says that the person is a thief; consequently the system is not doubted.
In order to make these technologies acceptable, one has to give tailor-made information with personal attention.

McDonalds had a lawsuit for serving hot coffee; a customer burnt herself, when she spilled the coffee on her lap. Now they decided to set up cameras, make a database, to see which people react to what in which manner and to know what kind of people they are dealing with.
It has to act like an alerting system.

The criminal law prevents to link personal data, with biometric data for privacy reasons. At this stage it is still prevented to combine various sources of information. Now the identity of a person is just a number; for example everybody has a social security number or drug addicts have a number, but it is not allowed to convert these numbers so that it can be traced back which person is connected to which number. However we can see that the legislation is following the technology and is catching up. Now there are 900 databases with camera surveillance data.

At the A16, Hazeldonk highway, many cameras have been put up, but politicians differ from perspective. According to Rita Verdonk, regarding the foreigners' law, one must be able to use biometrics and store data in a central database. It works proactively. However a privacy organization Bits of Freedom (BOF) our privacy might be at stake, when our biometric data is stored in a central database.

When we think of the London bombings on the 7th of July; after the terrorist attack, one could identify the terrorists, since the information was recorded and stored. The question could immediately be answered; who were the terrorists?
In such situations one has to question what is more important: the national security or our privacy?

Maybe in the future there will be one national biometric central database. Biometric technology should be used as a support, in order to find out something about a particular case.

The problem with a central database is that information is known and patterns can be reduced which could tell us about someone's behaviour. But how can one prevent that you are not known as an annoying person everywhere? The problem with biometric technology is that one can easily invade someone's personal space/ privacy.

Now there are already AT machines where cameras are placed; a photo is required on the cash card, this photo is then taken up in the database and one can find compare the photo at the ATM with the one in the database, whether it is a recidivist or not. With huge cash withdrawals, the facial characteristics are kept in a database in order to support ongoing investigations. But how to recognise a person, to what extent is it *actually* the person in question?

An iris scan needs to be taken from close-by; half a meter distance is required.
It is important to keep in mind when first applying biometric technologies in a certain environment, is to see how to make things easier. For example when taking a fingerprint many aspects have to be taken in account:

- warmth
- the print
- enrolment
- finger temperature
- reliability
- does the technology scan the patterns under de skin, under the fingertip

Most important when implementing such technologies, is to have in mind, what one wants to accomplish. Is it efficient to apply biometric technology? When checking a person's identity it takes 12 seconds when done by humans, and 30 seconds when done by a biometric device; in such a case it is ineffective to apply biometrics. One must consider the costs and benefits per situation; does biometrics *actually* add any value?
On the other hand biometrics is also a method to gather information/ evidence and gives one an idea with whom one is dealing with.

If one has an enrolment of 10 million people per year, there are still about 100.000 people who cannot get through the system. One has to take various variables in mind; the quality of the fingerprint, the reliability, the chance that things go wrong.

NEC for example has a high reliability rate, however it costs extra time at the embassy, for the person, there are many people involved and about 10 million euros just to get the administration right.

The common notion is that technology can solve every problem. But one has to keep in mind and see whether the technology *actually* add any value. One has to look at the problem and see what biometrics can do to solve the problem, and if one cannot solve the problem and biometrics isn't the solution to the problem, then it cannot be practical.

It is often reasoned that biometrics creates an illusion of safety; that it is the solution to every problem, and can predict every 'terrorist' attack. The world doesn't revolve around the West, some things happen beyond your perception. Biometrics doesn't combat everything.

Within the criminal law; biometric evidence can be used to verify the identity. Personal details are checked and if one connects this data to biometrics one can find the culprit. But one has to be sure, moreover one must consider what the consequences are if the data doesn't match. Furthermore there are more problems; someone's identity can also be stolen. Therefore it is important to test biometrics with pilot studies, for example in cooperation with the police; match the photos with recidivists. It is teamwork and eventually gives a solution to the problem, where one works together on the end product.

The concept works in three stages:

1. Technology
2. Process
3. Policy – future vision

One has to see, what technology can do; we look at the process; the policy procedures, until it becomes a real concept, otherwise it doesn't make sense. In a business case, one has to see what one wants to achieve:

- efficiency
- most importantly, one should not go ahead with the technology if it is not going to work

Technology is seen as the driver behind the process. How can one use technology for a certain process. Then one has to look at the legal barriers/ frameworks. Usually laws lag behind the technology and one cannot foresee what consequences it has.

Eventually it is a money issue; who is going to pay for the system; justice or the police.

In the private sector; companies pay for the technology, café's, pubs can stay open for more hours, but only if they implement CCTV. Now already we can see CCTVs at petrol stations and shops. The lawmaking has been adapted to these processes. But it is just a matter of time; how far do we want to go and do we want to be confronted with cameras?

Customers, companies also need to grow together with the technology. It is important to develop the technology in a user-friendly way or one will loose the customer.

The Privium project is a good example:
There are several important conditions:

- procedures go in a natural way
- It takes 11 seconds to check the identity, 1 second faster than checking the identity by the military police
- Does it add value?
- Is it practical?

For example opening a car with your fingerprint might seem useful at first against theft, but it also means that one cannot lend one's car to friends anymore.
Our clients are:

- AVUS – fingerprints
- The government is a big client of ours
- Airports
- Certain branches in trade and industry
- Events, like football matches etcetera.
- Private companies, but they are skeptical because of privacy issues

Interviews Clients

Presentation by Clarissa Slingerland – Baja Beach Club – 24 May 2006
We wanted something to bind our customers to the Baja Beach Club, moreover we were interested to get media attention, for our VIP-deck we wanted something outrages.

So we found VeriChip. It costs 1500 euros in total to be chipped; 500 euros for the chip and 1000 euros expenditure money. Privacy is completely guaranteed.

The idea is that only VIP-members can be chipped; you are always recognized and have access to the VIP-deck, you get special invitations, and we also have a branch of our club in Barcelona. Advantages are that you don't need to bring your wallet with you.

We introduced the VeriChip 2 years ago at the Baja Beach Club and it has had a lot of positive publicity. BBC, CNN, Dutch TV, all have come to interview us. It is still very original and very advantageous for the users.

We have 70 happy customers. It is just for VIP members and we want to keep it available for just for VIPs. These members have certain privileges and the more customers we have with a chip, less exclusive it will be.

We are just keeping the usability of the chip the way we have it now, we are not thinking of changing anything at the moment. The catering industry is not all ready for this step, but

several clubs have approached us and have shown interest in this system. Moreover the RFID acceptance is high with our customers.

Sari – the first customer at the Baja Beach Club to be chipped; it is all beautiful. We have a lot of space at the VIP-deck, on Saturdays for example it is very crowded, and so you have space there. It only has advantages, everything is better, you cannot feel the chip. It will just stay in my body. Well actually the chip is not scanned at all, because they know me there, I get a drink and once in a while I deposit 100 or 200 euros on the chip at the counter.

What data is attached to the chip?
The name, RFID-number, birthday, we know what they drink, what there custom drink is, the amount of money on the chip, and once on a while you bring your wallet to deposit money.

Interview with Conrad Chase – Director Baja Beach Club – Barcelona – 22 July 2006
Two years ago in February 2004 we started the program. We were open for 7 years. We built a VIP area, for that we needed VIP cards, for our customers; a customer loyalty system. We thought we need technology. I was looking into smartcards etcetera. Then I found out about RFID on the Internet. It exists already 20 years.

Then I encountered the Verichip – which has an official American Food and Drug Administration (FDA) approval. It is an idea, it is unique and not everybody is going to accept it. Nowadays everybody has silicones, tattoos, piercings, so it is not so strange. Let's give it a try. We like to take advantage of technology.

We want to have a better service for our VIP customers. We have handhold device for ordering, laser systems, and fresh mixing systems etcetera.

The Vipchip – We were the first to have the VIP-card, there is another in Galicia, as a method of payment.

Is it possible to deduct money directly from your account?
It will be possible in the future to do this, but there are many doom scenario's, where the truth is twisted. Nobody creates a story, which is true. But no, we don't store any personal information on the chip. Just an ID-number, name and a picture.

Katherine Albright founder of Caspian, she is against the VIP. She is putting false information on the Internet. She has written a book, a spy-book. She does this to sell her book, since it is very controversial. She is against the VeriChip. According to her, the chip can track you and can trace your spending habits, and therefore loose your civil liberties. She is against RFID-tags - but is totally impossible. According to her one can be tracked by databases, but it is not connected to any database.
Unfortunately people believe her; it is very unfortunate that she is sending bad information.

Also CNN and the BBC have been here. The BBC journalist had put a chip in his arm. Also Liberation was here, a French newspaper, they were very informed.

Where do customers get chipped?
We do it here; a registered, certified nurse gives the injection. We don't do it on the spot, but in a controlled, clean environment to avoid risks and complications.

How many people have the chip implant?
In Barcelona we have 94 customers. There are many benefits:

- You don't have to carry money with you
- No credit card
- No VIP-card
- You can't loose it
- Can't be stolen
- Can't forget it
- Free entrance
- Access to VIP – area

We only use it for VIP-people. We have a lot of interests, but it is only for exclusive clients. On the VIP-deck we only have exclusive clients and those who want to make use of the bottle service, because there we only offer bottle service. It is a higher range.
One can order; champagne, whiskey, vodka etcetera.

What kind of people get chipped?

Normal people; boys, girls, fashionable, young and old, everything.

Did people have any problems?
We never had any medical complication. When the first customers got it done, they liked it. In the beginning it was to test it. People enjoyed playing with it and we were quite pleasantly surprised that it was received so well. More people want the chip.

In Rotterdam we have 72 people with a chip.

Ik kom uit America bij Florida vandaan, daarna heb ik 6 jaar in Rotterdam gewoond en nu in Barcelona al tijdje.

Laten vrienden soms samen een chip implanteren?
Een keer kwamen een vader en een zoon samen die een chip laten zetten. Vrienden doen ook soms samen, maar meestal komen mensen los.

In Nederland vragen we een andere prijs dan in Barcelona. In Barcelona vragen we €125,-. Ze krijgen €100,- op de chip, ze hebben dus in principe maar €25,- uitgegeven.

In Nederland vragen we €1000,- en krijgen ze €1500,- tegoed op de chip. Het is een voordeel voor hun.

Zijn in Nederland andere klanten dan in Barcelona?
In Nederland is het meer exclusief en komen er mensen op af met meer geld. We zijn eerst in Spanje begonnen; we wisten niet of het zou aanslaan, maar het werd wel geaccepteerd. En in Nederland werd het duurder, dat durfden we wel te vragen. We willen in Spanje eigenlijk hetzelfde doen.

In Nederland zijn er meer mensen met geld. Hier is het iets meer normaal; wel mensen die iets meer geld hebben, maar niet zoals in Nederland.

In Nederland bestaan we 11 jaar en in Spanje 9½ jaar.

In zomer zijn er vooral toeristen hier. We hebben een capaciteit van 1600, maar komen 2000. Vrijdag en zaterdag zijn de drukste dagen, we zijn 7 dagen dag en nacht open van eind juli tot en met augustus. De rest van het jaar zijn we open van woensdag tot en met zondag.

Wie levert u de chips?
VeriChip wordt in Boca Raton tussen Miami – West Palm beach geproduceerd. They don't sell it to just anyone. Het is een correct bedriif. Er worden 50 chips per keer besteld voor Nederland en Spanje. Ik ben de distributeur. Het bedrijf heet Metro Risk Management in Miami, ze zitten ook in Zuid Amerika.

Kunt u wat zeggen over de chip?
De chip is zo groot als een rijstkorrel. Het is een 'passive'RFID chip – geen batterij. Hij wordt alleen actief als die naast een reader is. Leesafstand is 2 cm. Als de chip wordt geactiveerd, zendt een klein zendertje de identificatiecode naar de radar.

Wat is volgens u de reden dat mensen een chip laten implaneteren?
Om VIP te zijn, it is a nice piece of conversation. Het is iets unieks.

We hebben een release waver; bewust gedaan, dat de Baja niet verantwoordelijk wordt gesteld als het eruit wordt gehaald.

De BBC journalist wilde hem eruit halen, na 1 dag, maar werd geadviseerd later eruit te halen, na het genezingsproces.

Ik ben ook in Big Brother in Spanje geweest in 2004. Ik had net die dag ervoor die chip laten zetten en in september ging in het huis. Ik was de eerste met de chip.

Waarom heeft u de chip laten zetten?
Ik heb het gedaan als voorbeeld.

Verder als je mijn naam op Internet intikt, kom je op mijn website, maar meteen de tweede link eronder - prisonplanet, die doet een doomsday prophecy.

Interview with Patrick Vermeulen– Manager De Fakkel – Ridderkerk – October 2006

1. Wanneer is het biometrische systeem van start gegaan?

Vorig jaar augustus.

2. Wordt het systeem altijd gebruikt voor iedereen?

Het wordt gebruikt voor het recreatiebad, dat is dus woensdag van 13.00-17.00, vrijdag van 19.00-22.00 en zondagmiddag van 13.00-17.00. En we hebben bewust gekozen voor speciaal die dagen dat het systeem gebruikt moet worden, omdat we dan de grootste mix tussen jong en oud hebben. De grootste groep van de jeugd zijn die dagen aanwezig.

3. Wat zijn de redenen voor het invoeren van het systeem?

Het werkt preventief en het is een marketingmiddel/ spaarmiddel. Jeugd die voorheen vervelend was, wordt uit de anonimiteit gehaald. Ze kunnen hun gegevens 'faken', maar vingerafdruk kan je niet vervalsen. Je kan ze blokkeren en de politie komt altijd.

4. Wat zijn de voordelen van het systeem?

Het agressief gedrag naar medewerkers is afgenomen en er is een daling van uitzettingen. Zwaardere vergrijpen, zeer agressief gedrag, handtastelijkheid is minder geworden. Medewerkers ervaren het als positief; het is relaxter aan het bad. Normaal gesproken is de druk hoog als er vervelende gasten zijn, maar nu is het relatief rustig.

Ander voordeel is de bezoekers, die staan er vrijwel allemaal positief tegenover. Zijn een klein aantal mensen die tegenstanders zijn, en wat oudere mensen, die met vingerafdrukken hebben moeten werken in de Tweede Wereldoorlog. Ook zie je dat hoogopgeleide mensen sneller kritisch zijn met betrekking to de wet van privacy. Die denken verstand te hebben over de privacy. Eén stel was er tegen, wegens religieuze redenen. Zij waren christelijk en geloven dat biometrie op den duur zal leiden tot een vorm van dictatuur, ookwel 'merkteken van het beest' genoemd.

5. Aan wat voor incidenten moet ik denken?

Op vrijdag avond hebben we combi zwemmen in het bad, mensen die banen komen zwemmen hoeven geen pas. Ook hoeven mensen die een kleine meid meenemen of nieuwe bezoekers zijn geen pasje te laten maken.

6. We hebben meegedaan aan een benchmark, klanttevredenheid en veiligheidsonderzoek. We scoren niet op alle punten het beste, maar op veiligheid scoren we een 8, volgens onze eigen bezoeker. Het onderzoek werd door Price Waterhouse Coopers gedaan.

7. Jeugd komt sporadisch, ze komen vooral op dinsdag avonden. Als ze uit het bad worden gegooid wordt achteraf alsnog hun naam geregisteerd. De eerste keer wilde de politie niet meewerken met het systeem, maar toen zeiden we: "maar jullie hebben er ook baat bij,

misschien staan dezelfde mensen ook op de lijst". De politiekorps zijn gedecentraliseerd, dus die spelen dat door aan de wijkagent. De wijkagent werkt ook bij Alcazar en we willen een vergelijkbaar systeem hier opzetten.
8. Ze vertonen agressief gedrag, ze doen vervelende handelingen bij meisjes, in zulke gevallen komt de politie altijd.
9. We hebben 4 uitzettigen in een jaar gehad, dat zijn er natuurlijk wel 4 te veel, het waren allemaal zedelijke handelingen en dat levert een negatieve imago op.

10. In het begin zijn we gewoon gestart, toen bleken er heel veel 'kinderziektes'in het systeem te zitten, we hebben een beter beleid nu, betere communicatie, we laten nu niet iedereen tegelijk een pas maken.

11. Tilburg wil dit systeem nu ook invoeren en straks komt de Meerkamp uit Amstelveen kijken hoe het systeem werkt. Ook andere gemeentes zijn hier geweest. O.a. ook de KNVB voor voetbalstadions in verband met hooligans.

12. Wij zijn voorlopers van het SAR systeem; het is niet de bedoeling om uniek te zijn, maar uit allerlei windstreken krijgen we aandacht, SBS6, RTL4, RTL7.

13. Ongeveer 1% van onze bezoekers had problemen met het systeem. Bij een half procent hebben we de negativisme weg kunnen halen. Bij de andere helft is het niet gelukt, die koste wat het kost, maar die bezoekers wilden geen kaart, "je hebt mijn gegevens niet nodig om te zwemmen".
De andere, half procent konden we overtuigen, zonder dat ze hun vingerafdruk hoefden te geven. Oudjes waren vooral makkelijk te overtuigen, omdat die konden sparen, "ik ben hier nu voor de 11de keer en dan kan ik gratis zwemmen".
Een oudere vrouw wilde absoluut geen kaart. Maar ja zij horen toch niet bij de doelgroep.

14. Alle bedrijven werken tegenwoordig met NAW gegevens en gezicht foto's. Bunkers, daar kom je ook niet in. Ze kunnen het toch niet achterhalen wat je vingeradruk is, want de gegevens zijn gescheiden.

15. Bezoekers worden kenbaar gemaakt op onze huisregels. Bovendien haalt het systeem iemand uit de onbekendheid.

16. We hadden iets van 30 principiële bezwaarders op gesprek. Volgens mij zitten ze allemaal nog hier. We hebben iets van 10.000 kaarten per jaar en vooral voor preventie, tegelijkertijd is het een spaarkaart.

17. We willen het in de toekomst gebruiken als een marketingmiddel, je kunt er geld op laten zetten, bijvoorbeeld 10 euro, en dan doe je de kaart in de automaat en wordt tegoed automatisch erafgehaald.

18. Nu vragen we op de inschrijfformulier of de bezoeker emails wil ontvangen, anders val je onder spam en dat is strafbaar.

19. Je kan mailen over zwemdisco voor alle jongeren tussen 12-16 jaar. En ik kan bepalen wie ik bereik.

20. Hoofdmoot van de bezoekers komt uit Ridderkerk, Rotterdam, Cappelle (een druppel) en omliggende gemeenten.

21. Eén iemand heeft het lidmaatschap 'opgegeven', omdat deze was overleden, of verhuisd, en deze mensen worden per direct uit systeem gehaald, als we niets horen, blijven ze in het systeem.

22. €3.50 is de kostprijs van de pas. Eigenlijk verliezen we erop, omdat bij het aanmaken van de pas, je gratis entree hebt. Entree kost €3.15, dus het is een cadeau.

23. Het systeem kiest de beste twee foto's van de vier die er worden gemaakt. Het zijn gewoon ordinaire digitale foto's geen gezichtscan, en die dienen als eerste verificatie. Het nummer is het persoonlijk dossier met NAW gegevens. Inschrijven duurt maximaal 2 minuten; 10 seconden voor het activeren van de pas en de rest van de tijd het opschrijvan de gegevens.

24. Er worden vier vingerafdrukken genomen en het systeem kiest weer de beste, dat kunnen we niet wijzigen. In principe is het je rechterwijsvinger.

25. Het is ook handig om je uiteindelijk medische gegevens in het systeem te hebben, als er een epileptisch aanval is, of hartaanval, zijn er mogelijkheden en zaken waar wij rekening mee kunnen/moeten houden.
Als iemand een hartaanval heeft in een zwembad, weet je wel waar hij woont ongeveer, als je pas erbij pakt, en in 1 minuut zou je zijn vrouw kunnen inlichten.
Het heeft veel meer waarde zo'n pas ook met kinderen (vanaf 12 jaar moeten ze ook verplicht een pas). "Jongen breekt been, kan je ouders meteen informeren".

26. Secure Access Road doet het hele beheer van alle software, het complete onderhoud. Als er een storing is; per direct bellen, ten alle tijden. Ze werken 9 uur hier, en daarbij wordt bij Alcazar 's nachts ook gewerkt.

27. Jeugd heeft geen enkel probleem in het geven van zijn gegevens, ze zijn ermee opgegroeid. Totaal vet, cool, en hebben er geen problemen mee. 45-plussers zijn veel bezorgder.

28. In de disco worden dergelijke technologieen eerder geaccepteerd, omdat je daar eventueel gefouilleerd wordt, ook bij voetbalstadions heb je bewaking.

29. Bij ons moet je eerst iets gedaan hebben, je komt blanco binnen, maar als je iets flikt of weigert je pas in te leveren dan kom je direct op de blacklist.

30. Als je van alle zwembaden met alle mensen uit de blacklist een centrale database opzet met zedelijke delicten, hoeft zo'n iemand nooit meer te zwemmen.

31. Wij hebben direct contact met de politie, maar eigenlijk mag dat niet, alleen bij uitzetting mogen de gegevens doorgespeeld worden.

32. In Tilburg zijn drie zwembaden, ze mogen hun gegevens niet met elkaar delen. Het is een openbaar gebouw. De verantwoordelijkheid ligt bij de gemeente. De gegevens worden bij de gemeente opgeslagen en dan mogen ze met elkaar de gegevens delen.

32. Elke keer wordt ook gesproken over Wet van Privacy, komt door de media, beeldvorming. Dit systeem is eigenlijk veel softer in plaats van security guards bij je zwembad zetten.

33. Je kunt ook camera's gebruiken, maar heb je goed apparatuur nodig van goede kwaliteit, goede opnamemechanieken. Je hebt heel veel nodig voor camera's. Je krijgt 'big brother is watching you' gevoel. Camera's schrikt af. Kleedhokjes film, waar en wanneer en is heel duur. We hebben ze wel, maar doen er niets mee.
Dit is absoluut geen big brother-systeem. En om de veiligheid te verhogen zou ik direct dit systeem kiezen.

34. Dit jaar hadden we 8 incidenten, 3 Antilliaanse jongens. Ze wilden het spelmateriaal in het zwembad houden, en toen hadden ze drie badmeesters in het zwembad gegooid.
Voor het systeem stuurden we brieven, nu kunnen ze er een maand niet in. Gaat op het moment van uitzetting in. Uitzetten betekent dat de politie erbij betrokken is.
We hebben iets van 4/5 uitzettingen per jaar. Vier jongens en twee zaken. Het is een soort opvoedigkundig proces. Hoe meer verveling, hoe meer ze toeslaan. Ook als ze problemen op school hebben, dan zie je dat terug hier. Als er iets broeit tussen twee groepen.

35. Wij volgen het vrolijk & veilig protocol van de politie.

36. Maximale uitzetting is 5 of 6 jaar voor aanranding. Dat hebben we nooit gehad hier.

37. Als je eruit wordt gezet, pasje laten maken, als je een nieuwe bezoeker bent. Of pas inleveren, vingerafdruk weer afgeven en dan uitzetting, vervolgens kom je dan op de blacklist. De politie komt ook.

38. Het SAR systeem is niet opgenomen in de huisregels, op 'papier' staat wel dat het gebruik van de Fakkelcard verplicht is gesteld op bepaalde tijden en als er een calamiteit is, achteraf gegevens genomen kunnen worden.

Interviews with Alcazar End-users

Respondent 1

1. Dordrecht
2. Vertegenwoordiger van veevoer
3. 22 jaar
4. Ik kom hier iets van 2/3 jaar
5. Ik kom hier ongeveer 8 keer per jaar op zaterdagen.
6. Ik zie het nut eigenlijk niet in, van het systeem. Ik heb er geen last van. Ik ben niet verplicht om kaart te nemen. Ik kan ook gewoon naar binnen, maar je krijgt wel kortingen.
7. Je moet eerst een formulier invullen. Er wordt een foto gemaakt en je moet een vingerafdruk achterlaten. Je hoort ook je ID nummer op te zetten.
8. Nee, ik heb geen problemen met het systeem.
9. Je krijgt korting, de enige korting is een voordeel van 3 euro. In plaat van 10 euro kost het 7 euro.
10. Nee, er zijn geen nadelen.
11. De gegevens worden hier opgeslagen, en je krijgt sms-jes, die zijn soms wel handig.
12. Ja, ik ken wel wat mensen die ook een Pleasure card hebben.
13. Ik ga ook wel 'ns uit in Dordrecht, ook naar schuurfeesten, da's wel leuk!
14. Toen ik hier eerst kwam, moest ik meteen pasje halen, maar het was niet verplicht.
15. Ik heb nooit iets gezien, ook niet gehoord van gevechten.
16. Een leuke sfeer
17. Niet echt speciaal een lid
18. Nee. Ik heb er geen last van, dus geen reden.
19. Ik vind het wel goed, dan heb je er tenminste nog wat aan.

Respondent 2

- Rotterdam
- Ik studeer ondernemen en webdesign. Verder werk ik als autospuiter.
- 19 jaar
- Ik kom hier al 3 jaar.
- Ik kom hier op zaterdagen, iets van 10x per jaar, iets van 1x per maand.
- Ja, ik heb de kaart.

- Ik moest mijn wijsvinger eropleggen. Ik vind het een voordeel, want ik kan altijd doorlopen. Mensen die uit Rotterdam komen, mogen doorlopen. Ja, ik moest ook een formulier invullen, en een foto laten maken en ID nummer geven.
- Nee, ik heb geen bezwaren, ik heb weer een pasje erbij en dat is wel grappig.
- Opvulling van portemonnee, en het is veiliger, vind ik niet hoor, maar dat zeggen ze.
- Je foto is geregistreerd, geen privacy, bacterieën en ziektekiemen die kunnen verspreiden.
- Nee weet niet wat er met de gegevens gebeurt.
- Ik ken twee anderen met een kaart.
- In Rotterdam, de Baja, Outlet, en soms naar Zoetermeer en een paar keer naar Groningen. Baja is het leukst.
- Ik weet geen voordelen, er zijn geen kortingen. Als je je kaart vergeet, kost toch weer 10 euro.
- Je gegevens worden geregistreerd. En het is hier ook een kindertent aan het worden.
- Er is geen verschil in Alcazar van voor en na de invoering van het systeem.
- Het wordt steeds slechter, alle zalen gaan dicht, steeds slechter muziek.
- Ik kreeg een keer een asbak naar mijn hoofd, ik gaf een klap tegen de ander. De ander werd weggestuurd. Hij hoefde zijn kaart niet in te leveren. En je kan toch weer naar binnen als je 10 euro betaalt.
- Ik ben absoluut geen lid.
- Nee, laat maar zitten, moet je je weer helemaal uitschrijven, geen zin in, kost te veel tijd.
- Ik vind het niets. Maakt me niet zo veel uit, omdat ik niet vervelend ben. Af en toe gezeik met Ajaxieten en autospuiters.

Respondent 3

1. Strijen, iets van 5 km hier vandaan.
2. Ik studeer toerisme, ik werk voor twee promoteams.
3. 19 jaar
4. Ik kom hier elke week, op zaterdag en ook soms optreden hier (rap). Ik kom hier al 4 jaar.
5. Ik vind het een goed systeem.

6. Ja ik heb een pleasure card.
7. Formulier invullen, foto, vingerafdruk, ID, ook kinderen onder de 16. Je hoeft soms helemaal geen ID te laten zien.
8. Juist goed, geen bezwaren.
9. Je kan sneller binnenkomen en als je jarig bent krijg je gratis kaartje.
10. Niets, geen nadelen.
11. Nee, ik weet niet wat met gegevens gebeurd.
12. Ik ken hier toch heel wat mensen (ongeveer 80 ofzo). Ik kom soms met een groep van 10 en soms met ons tweeën.
13. Soms in Rotterdam.
14. Hier is het leukst, omdat ik iedereen ken.
15. In plaats van 10 euro kost het 7 euro en sommige evenementen zijn gratis.
16. Ik merk geen verschil in Alcazar van voor en na het systeem. Het is alleen een beetje krom, als je je pas niet bij je hebt, kan je toch weer naar binnen.
17. Nee er is geen andere sfeer.
18. Gezellige sfeer.
19. Ja,ik heb heel vaak gevechten gezien. Niets discriminerends, maar het zijn vaak Turken en Marrokanen, die vervelend doen, met vechten enzo. Ze staan vaak bij de achterste muur en dan gaan ze een beetje stoten. Het is jammer, krijgen ze een slechte naam. Er komen nog steeds dezelfde mensen, geen ander publiek.
20. Het systeem heeft het er niet echt veiliger gemaakt en je kan toch weer naar binnen via andere ingang, waar je 10 euro betaalt.
21. Ja voel me echt een lid
22. Nee joh, 10 euro kost het, muntjes moeten wel goedkoper, drankje kost 2 euro.
23. Heel goed; dan kan je vervelende mensen weglaten. 1 keer vervelend 1 maand niet komen, 2x vervelend 2 maanden wegblijven etc. Eigenlijk zouden ze bij de open ingang, iedereen die naar binnenkomt op vingerafdrukken moeten laten scannen. Het is ook kostenloos, waarom niet. Dus verplichten van scannen bij binnenkomst.

Respondent 4

1. Mijns Heeren Land
2. Ik zit nu op 5 Atheneum. En werk bij supermarkt en doe kranten.
3. 16 jaar
4. Ik kom hier al 2 jaar, illegaal. Ze zijn niet zo strikt en ik ben niet klein gebouwd. Ik

kom best vaak ±30 keer per jaar.

5. Vandaag aangemaakt, die pleasure card. Ze zijn best persoonlijk, ze willen alles weten; alle persoonsgegevens ID-nummer, alles, maar is best handig; kan je doorlopen. Bij de andere ingang sta je te wachten.
6. Nee, ik zie alleen maar voordelen van het pasje.
7. Je hoeft niet te wachten, voor 11 uur is gratis, als je later komt is het 10 euro, maar met pas 7 euro.
8. Het is wel een nadeel, dat ze alles moeten weten, ze gaan nooit controleren.
9. Geen idee wat er met mijn gegevens gebeurt. Ik heb wel gehoord van anderen, dat als je jarig bent, dat je gratis kaartjes krijgt opgestuurd en je krijgt emails; is best handig.
10. Mijn vrienden hebben hem ook en ik sta dan in de rij, terwijl iedereen langs loopt, dus dacht, laat ik ook maar een pasje maken.
11. Nu is prima hier, anders naar Rotterdam. Het is te veel gedoe om naar Rotterdam te gaan, duur met taxi's en shit.
12. Als je te laat bent 7 euro en geen 10 euro.
13. Gewoon altijd hetzelfde.
14. Elke zaterdag gaan mensen wel op de vuist. Elke week wel iets, maar dan moet je oprotten, soms zo erg dat je alles moet zeggen en dan mag je niet meer komen voor een paar jaar.
15. Vroeger was het heel druk, toen zat alles echt vol, 5 of 6 zalen, maar gaat slecht met de tent.
16. Mensen van de Hoekse Waard hebben het allemaal wel gezien hier. Ze moeten het vooral hebben van mensen uit Rotterdam.
17. Geen idee of er andere mensen komen nu of voor invoering van het systeem.
18. Nee voel me geen lid, en ik kom wel vaak hier, maar ken niet iedereen.
19. Nee
20. Goed, je gaat uit om plezier te maken en niet de boel te fukken.

Respondent 5

1. Strijen
2. Op school, 4de klas
3. 16 jaar
4. Om de 2 weken, ik kom hier vanaf mijn 12de.

5. Handig systeem, je mag elk vinger gebruiken en dan kan je naar binnen, is handig.
6. Naam, adres, leeftijd alles wat op de ID kaart staat.
7. Handig systeem, het moet ook beveiligd zijn.
8. Als je later dan 11.00 binnenkomt,krijg je korting.
9. Geen nadelen.
10. Nee ik weet niet wat met gegevens gebeurt.
11. Bijna iedereen die ik ken.
12. Ik ga wel 's uit in Strijen, maar dit is het leukst.
13. Na 11 uur krijg je korting.
14. Nu veel drukker, verder nee, is er geen echte verandering.
15. Wordt hier niet gevochten, ik heb nog nooit iets meegemaakt.
16. Nee, voel me geen lid.
17. Nee wil hem niet inleveren. IK heb hem gratis gekregen.
18. Iedereen verdient wel een paar kansen, maar anders niet meer naar binnen, als die kansen op zijn, bedoel ik.

Respondent 6

1. Strijen
2. Ik ga vanaf februari naar school naar de Albeda Spinoza weg.
3. Bijna 17 jaar.
4. Sinds mijn 13de kom ik hier, sinds anderhalf maand kom ik hier weer elke week, zeg maar sinds ik weer vrijgezel ben. En daarvoor kwam ik wel 2 of 1 keer per maand.
5. Goed beveiligd.
6. Ja ik heb de pleasure card.
7. Als je vervelend bent geweest, dan kan je er niet meer in, je wordt geblokkeerd, door vingerafdruk of foto.
8. Je ID, een foto en een vingerafdruk moet je afgeven.
9. Ik vind het wel in orde.
10. Na 11 uur 7 euro en anders 10 euro en bij sommige dingen kan je gratis naar binnen.
11. Meenemen, ik vergeet het pasje wel 's mee te nemen.
12. Je moet je vingerafdruk en foto op apparaat geven en dan kan je doorlopen. Ik wrijf even aan mijn broek of t-shirt voordat ik mijn vinger erop leg, zodat het goed gaat.

13. Naar Hollywood in Rotterdam, soms 1 keer per maand of 1 keer per 2 maanden ook op vrijdag en donderdag.
14. Soms kan je gratis naar binnen.
15. Toen ik hier kwam, was het systeem er al.
16. Verschillende groepen, nu zijn er meer zalen open en toen minder. Vroeger was gezelliger; we gingen naar Alcazar Light, we gingen dan met een groepje mensen en kenden veel meer en nu niet meer.
17. Vorige week ben ik er 2 keer uitgezet; mijn ex-vriendin, we waren 2 jaar bijelkaar, ging voor me neus zoenen, die lokte het uit en ging uitlachen, en duwen. Maar ik heb de bewaker omgeluld en kon weer naar binnen, door mijn vriend sorry te zeggen voor de neus van de bewaker. Er zijn maximaal 1 keer per maand ruzies.
18. Alcazar Light is voor kinderen tot en met 16 jaar, en komen vooral uit de Hoekse Waard, daar kende ik veel meer mensen en nu zijn er heel veel uit Rotterdam en is het minder gezellig.
19. Ja, echt een lid.
20. Nee, wil mijn pas niet inleveren.
21. Lullig, maar wel slim van ze, iedereen kan wel 's een keer ruzie hebben en dan 3/ 4 keer vergeven, maar na 3 keer dan ben je over je limiet, dan is het over.

Respondent 7

1. Puttershoek
2. Oud Beijerland, 3de klas
3. 15 jaar
4. Dit is nu mijn vijfde keer bij Alcazar. Ik heb nog geen pleasure card.
5. Ik vind het leuk.
6. Bij Alcazar Light kan je al vanaf 12de komen.
7. Best goed eigenlijk, aan je vingerafdruk kan je zien of je binnen mag ja of nee.
8. Nee, alleen bij Alcazar.
9. Hier krijg je drank mee en bij Light moest je zelf thuis drinken en nu hoeft het niet meer. Die man bij de ingang kent mijn vader en hij laat me dan soms binnen. Andere vrienden zeggen dat ze hun legitimatie zijn vergeten en kunnen dan binnenkomen.
10. Vorige week was er nog gevochten. Er waren twee jongens uitgezet. Ze zaten bijdehand te doen tegen de bewakers; uit te dagen en ze kwamen steeds terug en

toen zijn ze geslagen. Die jongens mogen er nu nooit meer in of in ieder geval voor een hele lange tijd.

11. Nu niet, want ik moet maar zien of ik naar binnen kan, maar als ik denk ik een kaart heb, voel ik denk ik een echt lid.
12. Dat vind ik eigenlijk niet kunnen, als je een avond rot voelt of kut en loopt je hele avond niet goed, betekent niet dat volgende keer weer zo is ergens anders.

Respondent 8

1. Puttershoek
2. Ik zit op school, 2de klas en ik werk ook in de electro.
3. 17 jaar
4. Ik kom hier al 4 jaar, bijna elke week.
5. Nergens op slaan, ze weten toch wie je bent.
6. Ja ik heb de pleasure card.
7. Nee, weet niet.
8. Alles geven, ja ook je ID nummer.
9. Hoeft minder geld uit te geven.
10. Weet geen nadelen.
11. Nee weet niet wat gegevens gebeurt.
12. Ja ken veel mensen met pleasure card.
13. Nee bijna niet, ik kom maar vooral hier.
14. Nee krijgt geen andere kortingen.
15. Nee geen verschil tussen toen en nu.
16. Komen altijd andere mensen.
17. Wel 's een gevecht gezien, maar ik weet verder niets.
18. Nee ik voel me geen lid.
19. Nee wil m'n kaart niet inleveren.
20. Is grauw, niet goed.

Respondent 9

1. Oud Beijerland
2. Albedak College – niveau 4
3. 17 jaar
4. 5 jaar geleden kwam ik hier voor het eerst.

5. Ik vind het systeem erg goed – vanwege kortingen.

Respondent 10

1. Dordrecht
2. Ik zit in de 4de klas.
3. 16 jaar
4. Ben hier een paar keer geweest, kom hier elke week.
5. Goed systeem, ik heb de pleasure card.
6. Je moet een lijst invullen, met foto en vingerafdruk.
7. Nee, geen bezwaren.
8. Ik weet geen voordelen.
9. Geen nadelen, gewoon goed.
10. Nee, ik weet niet wat er met gegevens gebeurt.
11. Nog 2 vriendinnen hebben de pleasure card.
12. In Dordrecht ga ik ook wel 's uit, maar hier is het leuker, veel gezelliger hier.
13. Gratis volgens mij, kweet het niet wat voor kortingen aan pasje zijn verbonden.
14. Woordwisseling meegemaakt, maar geen gevechten. Mensen die zijn gewaarschuwd.
15. Zelfde, ik merk geen verschil.
16. Ja ik ben echt een lid.
17. Nee wil mijn pasje niet inleveren.
18. Raar slaat nergens op, je mag gewoon overal naar binnen.

Respondent 11 – Bewaker

1. Mensen weten nu dat er een vorm van registratie is en of het bewust is of niet, mensen zijn er wel huiverig voor.
2. Nu zijn er de helft minder incidenten dan voor de invoering van het SAR systeem.
3. Ik zie alleen voordelen van het systeem.
4. Nu is het nog niet verplicht, maar misschien wordt het over 2 jaar wel verplicht gesteld. Ze krijgen ook voorrang.

Interviews with de Fakkel End-users

Respondent 1 - vrouw

1. Zuidland
2. Verpleegkundige
3. 60 jaar
4. Mijn kleinkinderen wonen hier in Ridderkerk, zo kom ik hier af en toe.
5. Iets van 2 keer per jaar
6. Ik hoefde niet mee te doen met het vingerafdruk systeem, gewoon betaald aan kassa.
7. Ik weet dat ze het overal willen invoeren; irisscan hebben ze toch? Is toch hetzelfde?
8. Ik heb er geen bezwaar tegen, ik denk wel dat het goed is.
9. Ik denk dat je toch niet anoniem bent. Je bent al zo bekend overal. Het is handig, het is vlot voor afhandeling. Het idee dat je anoniem bent, bestaat niet. Alles is gekoppeld. Dit is zowat de laatste koppeling. Toen de postcode werd uitgevonden, daar was ik zo tegen, heb ik jaren nooit ingevuld, maar je moet er aan toegeven. Zeker nu met één EU, zou je het zeker moeten hebben en niet dat ik het leuk vind hoor.
   In 20 jaar stel je je hele ideeën bij. Je hebt weinig privacy. Je denkt dat je privacy hebt en in een democratie leeft, maar het heeft zijn beperkingen, het is een luxe gevangenis. Zolang je een brave burger bent en meedoet, is er niets aan de hand.
10. Ik vind het systeem een nadeel, want één een dief, altijd een dief. Je kunt nooit meer een foutje maken. Je wordt meteen geregistreerd; het moet steeds 'idealer'; dit benadeelt het geluk.

Respondent 2 - vrouw

1. Ridderkerk
2. Ik werk in de thuiszorg als verzorgende.
3. 35 jaar
4. Ik kom hier al 9 jaar, sinds mijn zoon geboren is.
5. Elke zomer kom ik, in de winter doe ik er helemaal niets aan.
6. Ik vind het een heel goed systeem.
7. Ik ben in bezit van Fakkelcard.
8. Je moet Fakkelcard erin doen en dan met je wijsvinger erop.
9. Ik weet niet welke data ik moet afgeven.
10. In het begin was het niet leuk, want er was een hele lange rij, je wil gewoon zwemmen, maar dat kan dan niet, want het nieuwe systeem wordt ingevoerd

11. Het is handig, omdat ze kunnen zien welke jongens vervelend zijn; ze krijgen 3 waarschuwingen en dan horen ze niet meer te komen, vooral met meisjes enzo. Dat vind ik goed.
12. Nee, dat je zonder pas niet naar binnen mag, verder weet ik niet.
13. Nee, ik weet niet wat er met mijn gegevens gebeurt.
14. Ja, ik ken best veel mensen met een Fakkelcard.
15. Ik zwem wel eens bij de Lauwert in Ambacht en Zwijndrecht.
16. Het verschil; andere mensen, maar daar betaal je en zwemt.
17. Ik kom alleen zomers en rest van het jaar helemaal niet, dus ik weet niet over kortingen.
18. Ik zie geen verschil van hoe het nu is en toen was.
19. Het is allemaal hetzelfde, er is geen andere sfeer.
20. Ik vind het best wel leuk hier, zondags komen allerlei soorten mensen, dan kan je helemaal niet zwemen. Ik kom meestal doordeweeks.

21/22. Ik heb nooit voorvallen meegemaakt, ook nooit gehoord van vrienden of bekenden.

23. Ja, ik voel me wel lid, en dat komt mede door de kaart. Ik voel me niet verplicht om hier vaker te komen.

24. Nee, ik heb er niet over gedacht, om Fakkelcard in te leveren.

25. Discussie over privacy is goed. Ik ben alleen niet bewust van de discussie. Ik wil dat de data hier blijft en niet ergens anders. Dat is niet goed, want anders kan je nergens meer komen. Het kan ook zo zijn, dat iemand anders misdraagt en jij gepakt wordt, en dat is ook niet de bedoeling.

Respondent 3 – informele discussie met Sander, Evert en Mark

1. Waar komen jullie vandaan?

Ridderkerk

2. Hoe oud zijn jullie?

alle drie 11 jaar

3. Hoe vaak komen jullie in de Fakkel?

50 keer per jaar, 4 of 5 keer per maand, dan weer met de hele klas en dan weer met ons 10-en.

4. Hebben jullie de Fakkelcard?

Nee, mijn 2 broers en zussen hebben wel de Fakkelcard.

5. Weten jullie waarvoor die Fakkelcard is?

Als je vervelend bent krijg je een pas en staat je vingerafdruk op ofzo.

6. Hebben jullie wel eens incidenten, gevechten meegemaakt?

Afgelopen keer was er iets bij de glijbaan, neger had opgestopt. Na zwem 4- daagse, hele grote opstoppingen, mensen gingen achterstevoren glijen.

Ik heb liever dat ze weggaan, badmeester stuurt ze niet zo snel eruit.

Eén keer toen deed ik helemaal niets en toen zeiden ze allerlei dingen, vloeken enzo, dat heb ik tegen de badmeester gezegd en toen zijn ze eruit gezet.

7. Stel, je bent een keer vervelend, dat betekent dat je er niet meer in mag, wat vinden jullie daar dan van?

Als je hele klas erin mag en jij mag er niet in, dat is niet zo leuk, als je hele hele vervelende dingen doet is het toch handig.

8. Merken jullie verschil in het zwembad van voor de invoering van de Fakkelcard en erna?

Ik merk wel verschil, nieuwe glijbaan, dat ding – camera, prijzen zijn verhoogd €0.20 ofzo. Er zijn minder mensen, meer blanke mensen. De bruine mensen gaan naar Ambacht, hier worden ze streng in de gaten gehouden en worden eruit gestuurd. Veel kleine kinderen en banen zwembad is minder open dan eerst. Eerst kon je ook van half 9 tot 7 uur, de hele dag zwemmen voor €4.50. Nu moet je eruit en dan zit er een tussenstop in en dan moet je ook nog 's een nieuw kaartje kopen.

Vorig jaar had ik een prijs gewonnen, omdat ik 4 miljoenste bezoeker was bij de Fakkel. Ik kreeg:

- een taart
- weekendje Euro Disney
- 1 jaar lang gratis zwemmen

9. Wat zijn volgens jullie de voor en nadelen van de Fakkelcard?

Voor kleine kinderen is het veiliger, maar het is ook irritant als je je pasje vergeet, dan mag je er niet in.

10. Stel, je bent vervelend, dat betekent dat je er niet meer in mag. Verder zijn jullie gegevens bekend bij dit zwembad. Als je dan een keer in een ander zwembad wil zwemmen, dan is het mogelijk dat dit zwembad jullie gegevens aan het andere zwembad doorgeeft, wat vinden jullie hiervan?

Wel irritant als je hier niet kan zwemmen, straks mag je nergens meer. Ben je één keer vervelend en ergens anders wel goed gedraagt, dan mag je nergens zwemmen, niet echt leuk.

11. Waar zwemmen jullie allemaal?

Ik zwem altijd hier. Lauwert, de Zwaaf, Davel. Meestal hier en heel soms bij de Lauwert.

12. Zijn jullie zelf wel eens betrokken geweest bij een incident?

Ik kreeg een waarschuwing; buitenbad stinkt altijd; rioolluchten. Ik zwem toch meestal binnen.

Respondent 4 - vrouw

1. Rotterdam
2. Huisvrouw
3. 32 jaar
4. Ik kom vaak zwemmen; ± 3 keer per maand.
5. Ik kom meestal bij recreatie zwemmen.
6. Vandaag heb ik de Fakkelcard voor het eerst gebruikt, ze hebben hem aangeboden. In begin was het moeilijk, maar op zich ging het wel makkelijk.
7. Laatste keer dat ik kwam was in mei. Ze hebben me die Fakkelcard aangeboden en ik heb gewoon ja gezegd.
8. Ze vragen om naam, adres, tel.nr. en ID.
9. Geen bezwaren, ik vind het juist fijn. Als er iets gebeurt dan weten ze gelijk wie je bent, wie of wat en adres.
10. Er zijn geen nadelen.
11. Nee weet ik eigenlijk niet, ik heb het niet gevraagd. Het zal wel goed zijn.
12. Nee, ik ken geen andere mensen met de Fakkelcard.
13. Ik kom alleen maar hier zwemmen.
14. Wat ik hoorde, als je 10 banen-kaart koopt, krijg je 11de of 12de gratis.
15. Ik voel eigenlijk geen verschil. Vanmiddag is een beetje druk, hele lange rij en moet worden uitgelegd hoe en wat.
16. Geen verschil in sfeer.
17. Ik vind het een gezellig zwembad.

18/19. Ik heb geen voorvallen gehoord of meegemaakt.

20. Nu voel ik me wel echt een lid met de Fakkelcard, daarvoor niet.

21.Wat vindt u van de privacy discussie? Wat als u gegevens aan andere instanties worden doorgespeeld, wat vindt daarvan?

Dan moeten ze maar niet vervelend doen. En het is vooral voor jongeren denk ik, want ouderen zullen niet zo snel vervelend doen.

Respondent 5 - vrouw

1. Rotterdam
2. Ik ben begeleider van verstandelijk gehandicapte kinderen.
3. 56 jaar
4. Gemiddeld 2 keer per week met de kinderen.
5. Bij recreatie
6. Voor mij is het een heel fijn systeem, maar voor de kinderen wel moeilijker.
7. Vanaf de eerste dag heb ik hem.
8. Ik weet niet meer welke data ze wilden.
9. Ik heb geen bezwaren, ik vind het gewoon veilig.
10. Dat de raddraaiers er snel uitgaan is een voordeel, is fijner.
11. Nee geen nadelen.
12. Ik neem aan dat ze vertrouwelijk behandeld worden.
13. Heel Humanitas gebruikt het systeem.
14. Inge de Bruin bad in Barendrecht.
15. na 10 keer is het één keer gratis. Gaat heel hard, voor mij altijd.
16. Er is minder tramalant dan voor de invoering van het systeem. Niet voor mij een merkbaar andere sfeer.
17. Ik heb een veilig gevoel, gevoelsmatig is het hier prettiger.
18. Ik heb nooit voorvallen meegemaakt of gehoord.
19. Ja ik voel me echt een lid nu na de Fakkelcard.
20. Niet aan gedacht om geen lid meer te zijn.
21. Ik weet wat het systeem doet, en tja en je moet met de tijd meegaan. En ze hebben heel weinig gegevens van me, geen rekening nummers e.d.

Respondent 6 - vrouw

1. Ridderkerk
2. Ik werk met verstandelijke gehandicapten.
3. 35 jaar
4. Ik kom niet veel, iets van 4 keer per jaar.
5. Wel goed systeem, wel een veilig systeem, maar ik heb niet het gevoel dat het echt nodig is hier.
6. Ja, vandaag voor het eerst.
7. Je naam, adres, geboortedatum, ID.
8. Ik heb geen bezwaren.
9. Als mensen zich misdragen, dam kunnen ze eruit gezet worden en dat is wel een fijn gevoel.
10. Dat je hem vergeet of kwijt raakt, er zijn zo veel pasjes tegenwoordig.
11. Ik weet niet wat ze er mee gaan doen.
12. Ik ken 1 iemand nog met de Fakkelcard.
13. Nee, ik zwem niet ergens anders nog.
14. Ik weet niet of er korting aan vast zit, is niet vermeld.
15. Ik merk geen verschil in het zwembad.
16. Het zou zijn dat van die vervelende gastjes, dat die dan weggaan, maar ik weet het niet.
17. Nee, ik voel me geen lid. Ik heb het gedaan omdat het moest, voel me absoluut geen lid.
18. *Wat vindt u van de privacy discussie? Wat als u gegevens aan andere instanties worden doorgespeeld, wat vindt daarvan?*

    Vind ik logisch, ik denk ook niet dat je zomaar eruit wordt gestuurd. Het is de bedoeling van het systeem, dat het signaleert. Het kan wel zo zijn dat probleem zich verplaatst; als ze hier er niet in kunnen dan naar een ander zwembad.

Respondent 7 - vrouw

1. Ridderkerk
2. Pedagogische medewerker
3. 40 jaar bijna
4. Ja, met regelmaat, één keer per 6 weken, alleen recreatie.
5. Heel goed systeem; ik heb de Fakkelcard nog niet.
6. Prima, kan mij niet veilig genoeg, nu kunnen ze achterhalen, er gebeuren zulke rare dingen in zwembaden, Ridderkerk is er mee gestart.

7. Registratie is heel belangrijk, als iets gebeurt kan je het traceren, maar als er iets gebeurt is dan is het wel al te laat, maar bij treiterij in kleedhokjes of verkrachtingen dan kan zo'n iemand er niet meer in.
8. Nee, geen nadelen, wel invullen van formulier, maar op zich geen, nog een pas erbij in portemonnee.
9. Ja, waren een aantal meisjes, die hadden zo'n kaart, als je een feestje hebt, hoef je maar 1 kaart te laten zien en dat is wel raar.
10. Nee, ik kom niet in andere baden.
11. Eenmalige bijdrage, ik weet niets over kortingen.
12. Ik merk eigenlijk geen verschil tussen voor de invoering van de Fakkelcard en nu. Er lopen genoeg mensen, gelukkig maar.

13. Wat vindt u van de privacy discussie? Wat als u gegevens aan andere instanties worden doorgespeeld, wat vindt daarvan?

Als je niets te verbergen hebt, dan mogen ze mijn gegevens, behalve mijn pinpas. Nee hoor, ik vind het goed, anders gaan ze van zwembad naar zwembad en die hoeven we niet.

14. Het veiligheidsgevoel is niet veranderd en ook personeel is goed aan het rondkijken en opletten hier.

Respondent 8 - man

1. Zwijndrecht
2. Declarant
3. 39 jaar
4. Ik kom hier de eerste keer zwemmen
5. Goed systeem, als er problemen zijn dan kunnen ze iemand eruit halen.
6. Naam, adres, legitimatie; algemene gegevens, leeftijd, krabbeltje.
7. Geen bezwaar, ik niet.
8. Volgende keer kan kaart erin, voor mij geen voordelen, maar voor als iemand misdragen heeft is het handig.
9. Geen nadelen, als je niets te verbergen hebt, maakt het niets uit, maar iemand die misdragen heeft.
10. Ik ga ervan uit dat in data bestandje wordt opgeslagen, en voor mailinglist wordt gebruikt, maar daar maak ik geen gebruik van.
11. Volgens mij niet, als ik 10 keer kom, dan is het de 11de keer gratis.
12. Ik voel me geen lid.

13. Ik vind het beetje doorgeslagen. Er wordt te veel beschermd, onder mom van privacy kan het niet en ja als niets te verbergen hebt, dan tja.

Respondent 10 – meisje

1. Bergse Hoek
2. 16 jaar
3. Middelbare school
4. 4/ 5 keer per jaar
5. Ik hoefde geen pasje je gebruiken
6. Ik heb er ook niet van gehoord
7. Ik ken ook geen anderen die hier komen zwemmen.

Respondent 10 – 2 meisjes

1. Ridderkerk/Rotterdam
2. 14 jaar en 15 jaar
3. Middelbare school
4. We komen hier iets van 5 keer per jaar.
5. Recreatie
6. Onnodig, maar aan de andere kant blijven de vechters wel weg.
7. Eerst gegevens invullen, dan foto's, dan vingerafdrukken.
8. Is wel prima, ik vecht toch nooit.
9. Bij vechtpartijen of als je wordt aangerand, dan kan je dat meteen aanwijzen.
10. Lang in de rij staan voor je pasje, kost tijd.
11. Ik weet niet wat met mijn gegevens gebeurt. Ik vind het niet erg om gegevens te geven, hangt ervan af wat erachter zit.
12. Ja, we kennen iets van 15/20 mensen.
13. Binnenmaas, is een buitenbad, daar zijn veel badmeesters, binnenzwembaden gebeurt meer dan in buitenbaden.
14. Volgens mij niet.
15. Jongens die hier eerst kwamen om te vechten zijn er nu niet meer.
16. Nu hangt er een rustige sfeer, je hoeft niet bang te zijn. Eerst waren er ook wat meer Marokkanen. Zeiden dan: "Kom met me mee", maar die zijn er nu niet meer.
17. Vroeger kwamen er hele groepen en nu niet meer.
18. Een vriendin werd een keer hoer genoemd, toen was er een hele ruzie.

19. Nee, geen voorval na systeem.
20. Voelen ons niet echt lid, kom hier niet zo vaak.
21. Nee, is een fijn zwembad.
22. *Stel je bent een keer heel vervelend, je mag niet meer in het zwembad komen, maar die gegevens worden doorgespeeld aan andere zwembaden dat je vervelend bent, dan kan je daar ook niet meer zwemmen, wat vinden jullie daarvan?*

    Dat je 1 maand niet mag komen en daarna wel, dus dat je daarvan leert.

Respondent 11 – 1 meisje

1. Rotterdam
2. 14 jaar
3. Ik ga naar de middelbare school
4. Om de maand kom ik hier ongeveer zwemmen.
5. Het is wel een goed systeem
6. Je moet kaart erin steken en dan vinger erop leggen, die je hebt opgegeven, die erop leggen.
7. Gezichtsafdruk en vingerafdruk
8. Nee, geen bezwaren
9. Beter, ze kunnen je wel herkennen.
10. Niets, zijn geen nadelen
11. Nee, ik weet niet wat er met mijn gegevens gebeurt.
12. Paar mensen uit de buurt hebben ook de Fakkelcard
13. Ja Sportfondsen, hier is beter geregeld, badmeesters letten meer op.
14. Als je Fakkelcard hebt €3.15 anders kost het je €3.40.
15. Nee ik merk geen verschil in bezoekers.
16. Heb ik nooit op gelet.
17. Hetzelfde gevoel.
18. Ik heb nooit incidenten meegemaakt of ervan gehoord.
19. Soms wel, soms niet, geen verandering van ervoor of na de invoering van de Fakkelcard.
20. Nee
21. *Stel je bent een keer heel vervelend, je mag niet meer in het zwembad komen, maar die gegevens worden doorgespeeld aan andere zwembaden dat je vervelend bent, dan kan je daar ook niet meer zwemmen, wat vinden jullie daarvan?*

Is wel beter, maar echt voor de ergere dingen.

Respondent 12 – 2 jongens

1. Beverwaard, hierachter / IJsselmonde
2. 16 jaar/ 15 jaar
3. Middelbare school
4. We komen hier al 9 jaar.
5. Recreatie
6. Maakt niet uit, geen echte moeite mee, is voor veiligheid.
7. Folder invullen, pasje krijg je, 3 keer rechter vingerafdruk geven. Bij 11 keer mag je gratis zwemmen.
8. Naam, waar je woont, telefoon, email adres, ID, maar dat vult bijna niemand in.
9. Was meteen ok, wordt best wel veel aangerand door Turken en Marokkanen dus dat is wel goed.
10. 11 keer zwemmen is 1 keer gratis.
11. Niet echt, als je je pasje bent vergeten gaan ze best wel moeilijk doen. Ik ken alle badmeesters best goed, dus ze doen niet moeilijk.
12. Nee volgens mij niets.
13. Iedereen die binnenkomt.
14. Ja dit is kleiner.
15. Hier is prettiger, meer mensen die je kent.
16. Zelfde mensen die komen
17. Zelfde sfeer
18. Nu is Ramadan, maar anders zit vol met Turken en Marokkanen normaal gesproken, en die zitten daar (wijst achter in zwembad) en gaan wel ruzie zoeken.
19. Zien gebeuren, ik heb geen voorvallen meegemaakt na invoering van het systeem.
20. Ja iedereen kent mij, mijn naam, alles.
21. Nee, wil die Fakkelcard niet teruggeven
22. *Stel je bent een keer heel vervelend, je mag niet meer in het zwembad komen, maar die gegevens worden doorgespeeld aan andere zwembaden dat je vervelend bent, dan kan je daar ook niet meer zwemmen, wat vinden jullie daarvan?*

    Dat slaat nergens op, dat andere bad heeft er toch niets mee te maken, wat we in dit zwembad doen.

Interviews with the Baja Beach Club End-users

Baja Beach Club respondents

Observations: first customer comes in; you are welcomed by girls in bikini and a cocktail and men in shorts. The DJ plays loud music in the middle of the hall on a speedboat. Everybody is extremely kind and there are short acts/ performances done on the bar by the Baja 'crew' to entertain their customers. On every first Tuesday of the month, employees are invited of various companies to have a buffet and enjoy the night. On these particular Tuesdays one can see all sorts of people, young, old, men, women, and various ethnicities.

Conversation with Marlies and Irving:

On the VIP deck I talked with Marlies and Irving about the implanted chip. Marlies does the PR for the Baja Beach Club. Irving has been working for 2,5/ 3 years for the Baja Beach Club; he is a bartender on the VIP-deck.

There are about 70 people who are chipped. We have just put a stop to chipping, because it has to remain exclusive.
The scanner scans the chip, which is implanted in the left upper arm. When you scan the arm one can see the photo of the person and his/ her number and how much money you have on the chip. With a password one can load and withdraw money, you pay directly at the bar and hand the money to Irving. The chip is made of glass and cannot break. If you get chipped, you get papers for your health, but I don't have any health complaints.
You can feel a small lump in the upper arm. Everybody gets the chip in his/ her upper-left arm, so you can't ask for it in your leg.
On the VIP deck, people can make use of the Jacuzzi.

The minimum entrance for the Baja Beach Club is 23 years, but eventually the host decides who can and cannot enter the club.

Most people who have been chipped live in or around Rotterdam. We have had a lot of publicity even from China, Hong Kong. Most of the people who are chipped are regular customers; so they aren't per se friends.

Irving got himself chipped to be an example for other customers. In total there are 3 employees who got themselves chipped. People who are chipped can come on the VIP-deck and those who buy a bottle of drink for maximum 3 persons.
We are open from Thursdays until Sundays. We have very varied public. On Tuesdays people come after there work from various companies such as Fortis, Telemobile and other big companies, they come in their suit, but we also have very different visitors.

The Baja exists 11 years. There are several 'fake' Baja's, they try to imitate our atmosphere, but they usually all come down. Our club is especially famous because of its name, you just call it and everybody has heard of the Baja; (geholpen herinnering). There are even organized bus tours from Brabant (province in the south of the Netherlands).

The Baja has a capacity of 1600/ 1700 people. Mostly people come on Saturdays, this public really wants to enjoy, go out and have a party. On Sundays usually people who work in the catering industry come to the Baja to have a good time. Especially during holidays it is always extra busy, such as on: Easter, Pentecost and Christmas, about 1700 people come here.

During the first 'session' approximately 30 people were chipped, since then one-by-one over a period of two years.

Irving has been working for 2½ / 3 years, and before I used to come here already 10 years or something.

Saturdays and Sundays are most heavily visited days.
The whole system came from the idea that we wanted to offer something exclusive and special to our customers. All the co-owners/ managers came together and held a brainstorm session; consequently the chip was commonly agreed upon as a new way of paying and entering.

Once you become a member all your personal data is written down. As a VIP-member you always have free entree to the Baja, moreover you can take one guest. Not only do you have a free entree on regular days, also you are invited for free on special occasions, on all

holidays and special actions, on these days you cannot bring a guest along. Invitations are usually done by email.

Is it possible to remove the chip?

If you want you can get the chip removed in the hospital, the chip is placed under your second skin, but so far nobody wants to have the chip removed.

The entrance fee is €7.50 from Tuesdays till Sundays, except on Saturdays it costs €8.50. On special occasions it costs €9.50 such as on Easter, Pentecost etcetera. At the entrance chipped members are also scanned, there you cannot see the amount of money they have on their chip, but you can see this here on the deck. However it is still not very convenient, because you have to put your arm in a unnatural position to get it scanned, so we are thinking to make the scanner stronger, to catch the signal from a bigger distance. On the deck VIP-members immediately get their favorite drink. The chip is a stunt to have loyal customers and bind them to your club.

We have had a lot of publicity from the whole world: Japan, the biggest TV channel from China, Dutch TV, National Geographic, CNN, Discovery, we are the first in the world with a wallet under the skin.

In weekends we usually have our regular customers. On Tuesdays, companies and personnel come here; these people hardly come in weekends.

Mostly those who get themselves chipped are individuals, because most people are still quite reluctant to get a 'foreign' thing in their body.

Interview with Ismael Sari

1. Where are you from?
   Rotterdam
2. What work do you do?
   I am a process operator in the chemical industry.
   What is your age?
   I am 38 years old.
3. Since when have you been coming here?

Since the opening of the Baja, 11 years

4. Did it hurt, when you got chipped?

   No, I got anesthesia, you don't feel a thing, and it is like cold liquid.

5. Why did you get yourself chipped?

   There was an action; the first 25 people could get the chip for free. It is my second home here; it only has advantages, no disadvantages. I know everybody here, the owner, and my friends.

6. Did your friends get themselves chipped?

   From my own group of friends, nobody got chipped, not many of my friends come here anyway, I am the only one, who comes here a lot. But I have met many other VIP-members.

7. Do you go out to other places?

   To go out, I only come here and some favourite pubs, but I come here to party.

8. What offers do they have here for VIP-members?

   When entering you immediately get your favorite drink, mine is red bull and it is deducted from my balance.

9. Did you meet new people here on the VIP-deck?

   Yes, I made very good friends, I even had some relations.

10. Are there differences between the VIP-deck and over there?

    The only difference is I don't to want to show-off. Here it is quiet, down there it is crowded, and that is the only difference.

11. How many people own the club?

    There are in total 3 bosses.

12. Do you come here with friends?

    It is a very tight group here on the deck, but if you are here with a group, you still go down, because it is not so nice for the others.

13. Are there other people you know with a chip?

    There are two girls; they are also always here and probably also have a chip.

14. What do you like here?

    To look at people: boys and girls, it is really fun.

15. Do you have a feeling that you belong to the Baja?

    Yes, you really have the feeling that you want to belong to the Baja and yes, you really do belong!

16. Which days do you come here?

I am always here on Tuesdays.

17. I don't drink any alcohol

18. I am a widower.

Conversation with Clarissa Slingerland

Clarissa does the PR for the Baja Beach Club.

What type of people gets themselves chipped?

You cannot say what type. Most of the VIP-members are men with money, younger people aren't very pro. Especially older men get themselves chipped. According to me, it has nothing to do with not having money in your wallet, because nobody leaves their home without money. All these people really have a Baja feeling and get themselves chipped to really be a part of the Baja and belong.

In the weekend we have a lot of visitors from Brabant. At this point we have some 100 people on the waiting list who want to be chipped.

They never had to deal with the law for personal data and privacy.

Observations: At around 9.30 pm friends come in, people come and leave the deck. Three people have been sent away from the deck, because they have no chip.
A friend of Sari comes on the deck for girls, but a crew member sends him immediately away.

Conversation with Arno Gerbscheid

1. How old are you?

   I am 34 years old.

2. How long do you work here?

   I have been working here for 10 years. I am the manager of the Baja and I also work as a bartender.

3. Why did you get yourself chipped?

   I got myself chipped to show other people that it is not harmful, from a commercial point of view.

4. Since when do you have the chip-system?

We have the system here since October 2004 and I got myself chipped then.

5. What are the advantages and disadvantages?

   No disadvantages and no advantages; not directly with the chip, but indirectly the advantage is the tremendous media attention.

6. How many people got themselves chipped? What kind of people and for what reasons do you think?

   Around 40 to 45 people have a chip. It varies what kind of people, but most of them got chipped out of ease of the chip. If it is crowded in the Baja, you can go to the deck and you are taken care of, you get personal attention.

7. What age are the people who get themselves chipped?

   Between 20 and 55 years old, usually people have their own company, they want easy and comfortable. They are common people; it could be anyone who wants to be chipped. Condition is that these people don't mind having a strange object in their bodies which is not their own.

8. Is there a connection between the people with a chip?

   No, there isn't more or less connection with people with or without a chip.

Interview with Ryoni

1. Where are you from?

   Rotterdam

2. What work do you do?

   I have my own company in investments (real estate & trade).

3. What is your age?

   I am 22 years old.

4. Since when have you been coming here?

   I have been coming here, since 2005.

5. Which days do you come to the Baja Beach Club?

   I usually come here on Friday or Saturday, once a week.

6. What do you think about the implanted chip?

   It is very convenient

7. Why did you take the chip?

   Because of laziness

8. Could you explain what the procedure is, when chipped?

The Baja Beach Club makes a doctor's appointment; checks your medical condition; then the chip is injected. All-in-all it just takes half an hour. National Geographic asked my permission,whether they could film the chip implant for a documentary, I agreed.

9. What was your reason to be chipped?
   The main reason was, that you are a VIP. Moreover you can just walk into the club without paying etcetera.
10. What data did you have to give?
    You have to give your personal data, address, etcetera, the usual information.
11. What benefits does the chip offer you?
    I can take one person for free with mee; I can just walk on, the staff knows me and I don't need to pay cash anymore.
12. What are the disadvantages of the chip?
    I haven't had any disadvantages so far.
13. Do you know people with a chip?
    I don't know anybody with a chip.
14. This area is only for chipped people, right?
    It used to be like that, but not anymore since a couple of months.
15. Where all do you go out?
    Utrecht, Amsterdam, I don't have a fixed place where I go out. In Amsterdam I go out to Storm, Jimmy Woo, Supperclub.
16. Why do you think people get themselves chipped?
    According to me it is especially for lazy people; with the chip everything goed faster.
17. Do you feel a real member of the Baja Beach Club?
    I know the owner, but I don't feel a member of the Baja Beach Club. I don't really feel connected.
18. Did you ever consider to have the chip removed from your arm?
    No
19. Would it be covenient if the chip could be used at other clubs?
    Yes, but I would not get another chip in my arm, only if this one chip can be used at other clubs it would be really convenient.
20. What does the Baja Beach Club do with your personal data?

Nothing

21. When did you get yourself chipped?

I got myself chipped in January 2005.

22. Do you worry that your personal data may be misused?

I don't worry about this at all; if people want to do wrong they will find ways anyway. Anyhow, so this chip doesn't make a difference, it is for my convenience.