Personal Data Protection

Coordinator LDH Ligue des droits de l'Homme

Partners AEDH – EDRI – IURE - PANGEA

NETHERLANDS NATIONAL REPORT

AEDH

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH, EDRi, AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

December 2009

TABLE OF CONTENTS

SYNTHÈSE

Methodology

The principle objective of this study is to understand and learn from the current situation with regard to privacy and data protection in the Netherlands. In particular, the aim is to explore practices, technologies and legislations that affect the everyday life of young people and finally to draw some conclusions.
The main questions asked were:

- How are European laws and EU policies relevant to data protection implemented in the Netherlands?
- What are the main risks for data protection in Netherlands?
- How are young people affected by these risks?
- How aware are young people of these risks?
- What is the role of the Dutch Data Protection Authority in eliminating these risks?
- What are the future challenges in this field?

This study is structured in 4 chapters: Mobility and Transport; Biological identity; Internet and telecommunications; Social Networks.

In order to determine the national situation, the observation method was largely used.
First, we have been supported by our member, the Dutch League for Human Rights (Liga Voor de Rechten van de Mens) as well as its partners and networks, who provided us measurable information on the four topics. We established a long and continuous correspondence with them which enabled us to exchange a lot of information and to confront the different points of view.
Using the observation method, the research panned out to gather data from all possible sources which include books, related internet sites, NGO reports, online newspapers, periodicals, academic publications, government studies, independent studies, papers from seminars and other institutional publications, to give us the widest choice of perspective on the subject area.
The direct communication method was used to conduct a face-to-face interview with Rick Van Amersfoort, from the Buro Jansen & Janssen, in the Netherlands. We got in touch with two Dutch academics, Corien Prins and Bert-Jaap Koops who helped us in the last steps. The reason why most data refer to the Dutch DPA is that - as it will be later on demonstrated - it is the main provider of information in this area. Most of the other sources were used to cross-check information, measure public awareness, determine public opinion and criticism.
Even though these sources have provided valuable information pertaining to data protection in the Netherlands, it should however be noted that, as the AEDH worked on 3 countries and the EU, this study and the attached cards are not as thorough as those prepared by the partners working only on their own countries (France, Czech Republic and Spain).
Consequently, for the drafting of the cards priority was given to technologies and practices that have not been dealt with by other countries or that ascertain the main privacy concerns in the Dutch society.

Legislation regarding privacy

There is no specific legislation for biometrics, neither for social networks. Before the EU Data Protection Directive was enforceable, there was a general privacy from 1992 that applied to the four areas examined in this study. This is in 1999 that the EU Data Protection Directive has been transposed into national law with the Personal Data Protection Act (the Wet bescherming persoonsgegevens "Wbp") which came into force on 1st September, 2001. This Act is unfortunately very vague, thus it is not always clear what data exactly need to be retained and there is a risk that the scope would be broadened for access to the data. Apart from that general privacy law, there are others specific law, like the Telecommunication Act ("Telecommunicatiewet") from 19th October, 1998 focusing on telecommunications; the Police Data Act ("the Wet politiegegevens") or the Municipal Database Act ("the Wet gemeentelijke basisadministratie).

Privacy and Data protection Control Authorities

The Dutch DPA supervises the compliance with acts that regulate the use of personal data. This means that the Dutch DPA supervises the compliance with and application of the Personal Data Protection Act, the Police Data Act and the Municipal Database Act.
The framework for performing its task has been set forth in the Personal Data Protection Act and other related legislation. In this context, the legislator has implemented Article 28 of the European Privacy Directive 95/46/EC, which explicitly provides for the existence of such a supervisory authority and which also provides that this authority should fulfil its task completely independently. The Dutch DPA has also a supervisory task which enables the DDPA to provide information and conduct studies on different topics.
The Dutch DPA is active five main areas: trade and services, labour, social security, healthcare and welfare, police and justice, government and international. Its tasks include: making recommendations regarding legislation, testing codes of conduct and regulations, preliminary examinations, informing citizens about their rights and obligations, mediation and handling for complaints, official investigation, enforcement and international tasks.
In order to fulfil its tasks efficiently, the Dutch DPA has to answer to several guarantees like the possibility of objection to and appeal against its decision before the administrative law courts and the possibility to complaint to the National Ombudsman. Moreover, as an administrative body, the Dutch DPA is of course also bound by the general principles of proper administration.
Each year, the Dutch DPA publishes a public report explaining its work and findings. This web site contains summaries of the annual reports for recent years.

Privacy Awareness

There have been some campaigns led by NGOs particularly in all the fields we explored. We can name for example the campaign led by internet access provider XS4ALL and BOF (Bits of Freedom) regarding the European directive on data protection.
Another initiative done by NGOs was the one launched by five Dutch consumers' organisations regarding the OV-chip card. They declared in a common position that they would not support the travel card anymore especially for price and security reasons. These organisations are campaigning against the OV-chip card and for freedom of choice for customers by allowing for a dual existence of paper and electronic tickets and by making sure that anonymous versions have the same possibilities as the personalized OV-chip card and that they are obtainable under fair conditions.
We noticed other initiatives like organisations of debate at the Schiphol airport on access by intelligence services on passengers' information.
Some campaigns must receive a particular attention since they will influence the legislative mechanism. That is the case for example for the road pricing system which could be implemented in some weeks. This project aims at providing cars which are regularly passing through the road pricing

system with a box that will record the trips as to pay the price directly. This project raises the question of the collect of data, of the access to data, etc… Debates and a referendum are taking place within consumers' advocacy groups and the result of the referendum will determine whether the Minister of Transport will pass the law.

The Dutch Parliament is also active in the debate regarding privacy. It seems that it has been more and more active for four years in the field of data protection. For example, there is a debate currently running within the Parliament about the purpose of the storage of data from OV chip card as to reduce the length of data retention and to narrow the possibilities of storage whereas the DPA already concluded that the rules on storage did respect the legislation in this field.
Depending on the topic examined, it seems clear that Dutch people are pretty aware of privacy concerns. Indeed, regarding the OV-chip card for example, even if people find that having a unique card for all the transports is a good initiative, a lot of them are asking for the anonymous card. That behaviour demonstrates that a lot of people want their privacy to be respected.
Most of people do not tend to reflect on what happens with their personal data however, some studies show that when they are asked, most people do not want their data to be shared with third parties and expect them to be treated confidentially.
Nevertheless, the mantra "if you have nothing to hide, you have nothing to fear" works well for many people. Especially for young people. It seems that young users are unconscious about the visibility of their profiles on social networks.

The overview

Mobility

The main tools used in the area of mobility are the OV chip card, the road pricing system and the Catch Ken/ ANPR highway actions.

- *The OV chip car:*

The OV-chip card is used as a mode of payment for public transport such as metro and tram. The stated goal is to simplify travelling and to prevent fare-dodging. It can also be used for electronic payments and in the future the package of services will probably be expanded. It is used as an access card for public transportation by uploading credit for a one-way journey, a return ticket or a season ticket.
For the moment, the OV chip car is mandatory - since it is the only way to travel - in Rotterdam where it is tested before it became mandatory in the rest of the country. But it is also available upon the wishes of the consumer in other cities of the NL.
People can choose between an anonymous card and a non-anonymous one. The problem is that people who would be eligible for a discount pass usually, do not have the possibility to get this discount with the anonymous card; therefore people have to pay for their anonymity.

The DPA did not issue any negative advice on the issue of the storage of the data contained in non-anonymous card because according to them, the conditions of storage are falling into the legal requirements. The data are stored for seven years and are used mainly for commercial purposes. At the moment there is a debate in parliament about the issue of the storage.
According to studies made, the security of the storage is minimal. Academics showed that it was quite easy to introduce into the system. Moreover, it has been noticed that people did not automatically know that their data were collected and stored. Besides, we do not know exactly how long the data are stored, who control the collect and who has an access do the data collected (intelligence services, police or only the travel societies?). And there has been no such debate as far as today at the Parliament or at the DPA on these critical issues.

- *The road pricing system:*

The government wants to pass a system on road pricing. Every car would have a box under the hood and this will track its movements. These movements are priced. Of course the debate is also about what happens with the data, where it stored is and who has access to the data. At the moment the ANWB holds a 'referendum' under its members to make out an opinion on the proposal and the Minister of Transport has made clear that he will wait for the decision to pass the system into law.

- *The Catch Ken / ANPR large scale police actions:*

It is important to make it clear what the system of ANPR and Catch Ken mean. Catch Ken is mainly a portable version of the ANPR so the system is the same. ANPR is used around Rotterdam and Zwolle. Catch Ken is used in cases where there are large scale police controls.
In January, it became clear from a report from the DPA that the data was stored up to 120 days (the no hit data). This is in breach of the law, therefore the Ministers of Justice and Home Affairs decided to change the law and are consequently proposing to store the data for a maximum of ten days. The Catch Ken system is used in large scale control actions mainly in the east of Holland. The system is used some kilometres before the action, whereby the highway is blocked and all vehicles are controlled. Catch Ken is used to look for speeding and to have information prior to the control.

Social networks

According to a recent international study from the market research bureau Synovate, the Netherlands has the greatest amount of online social network members relative to its size. In the Netherlands, 49 percent of the population is a member of social network sites versus a global percentage of 26 percent.
According to a research made by Vodafone Nederland**,** nearly half of the interviewees use social networking sites on a daily basis, of which one quarter even several times a day. 84 percent of the interviewees use Hyves and around 20 percent Facebook. Hardly 4 percent is active on Twitter.
In July 2008 Hyves announced that they had reached 7 million users, of which about 5 million were Dutch. This amounts to about a third of the entire population of the Netherlands. At the moment, they have about 9 million members.
The Dutch Data Protection Authority refers on its website to the Rome Memorandum by the International Working Group on Data Protection in Telecommunications (i.e. the Berlin Working Group) and the recent opinion of the Article 29 Working Group on the use of social networking sites. Both issued a series of guidelines for all parties involved with social networking sites for the protection and securitization of the personal data of network participants. The Berlin Working Group takes the view that data protection in the context of social networking sites needs a different approach than traditional data protection legislation since most of the personal data is placed online by the participants of social networking sites itself.
From the Dutch people between the age of 13 and 34, 80% uses Hyves on a regular basis. It seems that young users are unconscious about the visibility of their profiles and there seems to be little awareness of the possibility to limit information to a defined group of users. Hyves provides their users with a Privacy Declaration, and dedicates a category in the FAQ section to the issue of privacy as well as a large description of rights en duties of its users. These 'Terms of Use' and the 'Privacy Policy' are submitted to new members but could easily be ignored.

Biometrics

There are plenty of tools which use biometrics in the NL but in different ways. Some of them use fingerprints (ID card and passports, private card like the Alcazar card as to enter a disco or the Fakkel

card in order to enter a swimming pool, the SIRENE system, VIS…), iris scan (Privium, the system used to enter the Schiphol airport), facial recognition (especially used for football games) and DNA used for criminal investigations and sometimes for family reunification).
In the Netherlands there is clearly an increased use of biometric technology in everyday live. For example, there are already many places that use biometric systems for controlling access (Alcazarn, Fakkel and football games). Most people do not see any problems in these technologies and consider them as the logic next step in the evolution of our modern and technology based societies. Most of all, they are swayed by the idea of a more 'secure' environment, by the discounts that are offered, the 'easiness' it brings.
The Dutch Data Protection Act provides in article 18 and article 23 for exceptions to the principle ban on processing sensible data such as biometrics depending on the purpose of the processing. For the Dutch Data Protection Authority, the maintenance of order and security can be an acceptable purpose but we have to be aware that it can lead to abuses of course. Also, the principle ban does not count if the person involved gives it explicit and informed consent. Nevertheless, the DPA does not agree that these data can, then, automatically be used for other purposes, such as commercial ones. Overall, the DPA criticises the way in which people were informed in current cases where biometrics were involved because people were hardly ever well informed about the system and the use of their personal data before they consented.
Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care. In the cases mentioned above, one can wonder whether the conditions of necessity and proportionality have been met, although the Dutch DPA concluded so.

Private communications

According to the ENISA 2009 report, the Netherlands has reached one of the most advanced levels of development of information society. Indicators show that they are at the forefront of dissemination of ICTs in the economy and that there is a high level of ICT skills in the population and in the workforce. Since telecommunication services are increasingly interwoven in people's daily lives and since telecom operators and Internet service providers (ISPs) register (although temporarily) most of the log data of these communications, there is a risk of an invasion to our right to privacy and of a limitation of our autonomy.
For example, in January 2008 one of the system administrators of Planet, a Dutch Internet service provider, stored a backup of all client data in a user account, as the result of a typing error (the user's account and the system administrator's differed by only one letter)[1]. The user warned Planet, but Planet did not take any immediate action. The file contained the user names, aliases, IP addresses, encrypted passwords and used services of all private and business Planet accounts. Using hashmaster, the user could decrypt all passwords but Planet ignored the matter until the story spread. It then asked the user to delete the file. Planet claims that it will change its back-up policy.
The opinion of the Article 29 Working Group on Internet search engines from February 2009 has had a positive impact on search engines in the Netherlands who started to present a more privacy related image as a way to differentiate between each other. Some search engines even stated that the proposed retention period of 6 months for browsing data by the Article 29 Working Group should become a standard for the entire industry.

One of the most controversial tool used in the NL is SMS message that you receive from the police when a crime has been committed in a certain area. In fact, when a crime is committed somewhere, in a certain part of Amsterdam for example, the police will freeze the data from the mobile phone antennas in the neighbourhood of the crime. The issue made by this tool is that if the recipient of the

[1] http://www.spaink.net/dutch-data-breaches/#2008-09-22.

message does not answer to that message, he/she can be suspected as guilty or at least, it put a suspicion on him/her.

We should watch a current revision of the intelligence services law which has already passed the Parliament and which is currently being discussed in the Senate. It would allow intelligence services an unlimited access in all kinds of databases be it health care or telecom. For example, an article of this proposal provides that intelligences services will be able to use legally a mobile telecom antenna (the IMSI catcher) in order to divert the telecommunication directly to the police.

Conclusions and recommendations

The issue of privacy seems to be rather well-known in the Netherlands since as we can notice with the amount of people applying for an anonymous OV chip card, people want their privacy to be respected.

In the area of public sphere, anonymity should be default. People should not have to apply for an anonymous card; they should be given one instead of a non-anonymous as soon as they are registered as a consumer of Dutch public transportation. Moreover, the right to private life should not be profitable. The anonymous card should cost the same price as a non-anonymous card because you can not profit from privacy. People must have the choice when systems have an impact on their right to privacy. That means that they must be able to choose and to apply for such devices and societies or companies must ensure that people are aware of all the implications generated when they give personal information. Authorities should make sure that people are aware of their rights regarding privacy.

There should be, as soon as a proposal for a law is launched, a mandatory consultation of the Dutch Data Protection Authority as to make the right to private life respected in every piece of legislation. Therefore, it would be an important safeguard if an independent third party, such as the Dutch Data Protection Authority, watches over the rightfulness of the collecting, storing, processing and transferring of these personal data. That way, people who were for example wrongfully put on a blacklist have an institution to complain to and to protect their interests.

There should be a general legal framework defining precisely the collect of data, data retention, purposes of such systems, and access to data…so that in moments of stress police and intelligence services cannot use the ‘vague’ descriptions to get access. There should also be a maximum length for storage which could not be exceeded even in “exceptional circumstances” as terrorism. The data should be stored encrypted both preventing ‘criminal’ and ‘non criminal’ abuse.

Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care.

Use of search engines which do not hold your IP addresses and researches.

The fact to retain traffic and location data constitutes a serious violation of the right to privacy and therefore, turns citizens into potential suspects.

1-MOBILITY AND TRANSPORTATION

OV-CHIP CARD

Identification of technology	The OV-chip card[2]
Technology used/tool	The OV-chip card is a plastic smart card with the size of a bankcard and it contains a chip that can be read out from a distance. The microprocessor chip consists of a memory, a central processing unit (CPU) and some contact points, which means that it is not only capable to communicate, but also to make calculations. This means that the smart card can receive input that it can process and deliver as output. The OV-chip card is a contactless smart card based on two different technologies. The disposable chip card uses the 'MIFARE ultralight' chip and the anonymous and personal chip card are based on the 'MIFARE classic' chip.
Country/use area	The first pilot projects were held in the Netherlands in 2004. By the end of 2005, the OV-chip card was introduced in Rotterdam and by mid 2006 also in Amsterdam. Since 29 January 2009, the OV-chip card has been made compulsory for metro, tram and bus in Rotterdam. Paper tickets are no longer issued or accepted.
Frame of use	The OV-chip card is used as a mode of payment for public transport such as metro and tram. The stated goal is to simplify travelling and to prevent fare-dodging. The OV-chip card can also be used for electronic payments and in the future the package of services will probably be expanded. The card is used as an access card for public transportation by uploading credit for a one-way

[2] The following information is based on an interview with Buro Jansen & Janssen (12/06/09), official documents from the Dutch DPA on http://www.cbpweb.nl/themadossiers/th_ovc_start.shtml, and on the following website http://nl.wikipedia.org/wiki/OV-chipkaart.

	journey, a return ticket or a season ticket. The passenger needs to place the OV-chip card within a 10cm range of the card reader when getting on or off a bus or tram or when checking in or out of a metro station. The travel distance will automatically be calculated when getting off or checking out and the price will be automatically deducted from the balance on the chip. There are three versions of the OV-chip card: a disposable (anonymous) OV-chip card, an anonymous OV-chip card and a personal OV-chip card. Personal OV-chip cards are connected to the identity of the cardholder and are not interchangeable. These cards can be uploaded with a certain amount of money for travelling and for other services, such as season tickets. When the balance is to low for travelling, the chip card can automatically transfer money from your bank account. Anonymous OV-chip cards are not connected to the identity of the card holder(s) and can be interchangeable. These cards can also be uploaded with a certain amount of money for travelling and for a selection of other services. However, they can't be used for a traditional season ticket nor do discounts apply to them. Disposable OV-chip cards can't be uploaded. They can be used for a fixed set of days or journeys.
Population concerned: target and age	Everybody using public transportation in Rotterdam and Amsterdam. Children up to 4 years old do not need an OV-chip card and can travel free of charge.
% of users/of young users	No specific numbers.
Trends (measured/supposed)	The card will be made compulsory in Amsterdam by July-August 2009. In the near future, it will probably be introduced on a general basis, which means for the entire sector of public transportation (trains, trams, buses, metros) and throughout the Netherlands.
Known or potentials dangers/Risks	There is a risk that traveling with anonymous OV-chip cards leads to a poor service package and sometimes such cards are not obtainable under fair conditions. There is also a risk that transport companies will pressure customers into personalized OV-chip cards by setting high prices for anonymous ones. At the moment, this is not (yet) the case but certain services are only accessible with a personal OV-chip card. Also, the Dutch DPA criticized the fact that customers are not well enough informed about the OV-chip

	card for them to give a deliberate and informed consent. All the information is out there, but not in an easy accessible format to potential customers. Also, there have been many problems with the securitization of the data on OV-chip cards. The security of these cards is minimal since they are expected to be profitable. Therefore, it is easy to hack them and certain research groups at universities have done this regularly to demonstrate the security problem. The result is that not only people can travel free of charge, but also with the balance of others using a hacked chip. Off course, sensitive personal information can be gathered as well without the knowledge or consent of the person involved. This becomes even more problematic when the service package of the OV-chip card will be expanded in the future. Finally, the use of contactless smart cards on this scale presents a risk for privacy, since it offers a range of new possibilities for the illicit tracking of the movements of people using these cards.
Others	/
Generated data bases	
Associated data base/creation	The application for and use of the OV-chip cards is recorded in a central database. The massive computer system includes card readers and sensors in each public transport vehicle or station.
What justifies the inscription in the file/Risks?	The application for and use of an OV-chip card.
Purposes/contents, main data included/Risks?	The information is stored in a central database for managing the OV-chip card system and to aid transport capacity planning. The personalized OV-chip card requires the retention of personal data of travelers such as name, address and domicile, but also additional information such as made journeys, mode of payment and used services (e.g. the renting of a bike at the station). However, the Dutch DPA demands that these data are processed and stored in a way that they can no longer be linked to an individual. Concerning disposable and anonymous OV-chip cards, the only information that can be stored is the journeys made and mode of payment.
File masters? Risks?	The OV-chip card is a joint initiative of the five main public transport companies, i.e. Connexxion, GVB, HTM, NS and RET. These companies set up Trans Link Systems (TLS) to prepare together the introduction of the OV-chip card. TLS issues the card and is responsible for the central system that registers all travel data and processes all

	electronic payments. In the near future, the application form for a personal card without subscription will be send immediately to TLS, since they are responsible for issuing the card. The individual transport companies than will no longer retain the personal data of those customers.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	It is unclear for which purposes, and by whom, the data can be accessed and used. For example, it has happened already that these personal data are sold for marketing purposes. The Dutch DPA declared that the collection and use of detailed travel information concerning personal OV-chip cards can never be justified for marketing purposes (unless the explicit consent of the customer in question and with respect for the Dutch privacy law) and can only be used to a certain limit for enhancing services such as refunding customers in case of delay.
Data retention delays/risks Right to be forgotten	It is unclear how long these personal data are retained but it should only be possible for a relatively short period. Also in cases where such data can be used for enhancing services, they can only be used and stored for a limited period and it is necessary to observe a strict purpose specification. The Dutch DPA also demanded that customers with a personal OV-chip card would have a right to opt out.
Rights to know or to modify data?	Unclear.
Covert purposes/Risks/uncontrolled future evolution	Since the card is used as an 'access key' to the stations, it is expected to help in pushing back 'nuisance' on platforms and in trains, trams, buses and metros.
Others (interconnections…)	/
Legislation in application	
Law/rules/others (?)	The general Dutch privacy law of 1992 applies.
Risks for freedoms despite the law	The illicit tracking of people and the unauthorised access to and usage of the information stored on these travel cards.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen.
Conformity with the European right (Charter of fundamental rights, directives…)	
Implementation (or not) of the legislation? /Risks	
Others	/
This tools and young public or young adults	
How far are young people concerned?	Unknown.
Awareness of issues or of risks	The travel card received some public criticism after its introduction since it was theoretically possible to connect the traveler's identity with

	travel route information. After the Dutch DPA publicly criticized this practice, transport companies changed their policy.
Indifference or reaction	However, most of the public debate concerned the lack of securitisation of the smart cards and after a while the public debate subsided.
Awareness campaigns/results	The lack of security concerning the data stored on the smart card has been pretty much the only issue in the public debate and there have been no campaigns to oppose the OV-chip card as such. Nevertheless, 5 Dutch consumers' organizations (Consumentenbond, ANWB, Rover, LSVB en CG-raad) declared on 22 September 2008 that they will no longer support the OV-chip card system since they find that it has introduced more problems for consumers than advantages. Mostly, this concerns the price of these cards, privacy-issues and some practical problems in the implementation of the card[3].
Good practices	The transport companies will have to carry out an independent privacy audit once every two years in view of the above-mentioned problems.
Campaign to be led. On which themes?	The above-mentioned consumers' organizations are campaigning against the OV-chip card and for freedom of choice for customers by allowing for a dual existence of paper and electronic tickets and by making sure that anonymous versions have the same possibilities as the personalized OV-chip card and that they are obtainable under fair conditions.
Others	/
Conclusions	There is a risk that traveling with anonymous OV-chip cards leads to a poor service package and sometimes such cards are not obtainable under fair conditions. There is also a risk that transport companies will try to pressure customers into personalized OV-chip cards by setting high prices for anonymous ones. Customers are not well enough informed about the OV-chip card for them to give a deliberate and informed consent. All the information is out there, but not in an easy accessible format to potential customers. Also, there have been many problems with the securitization of the data on OV-chip cards. The security of these cards is minimal since they are expected to be profitable. The result is that not only people can travel free of charge, but also with the balance of others using a hacked chip. Off course, sensitive personal information can be gathered as well without the knowledge or

[3] http://www.consumentenbond.nl/actueel/persberichten/perberichten_2008/geen_vertrouwen_ov_chipkaart.

	consent of the person involved. This becomes even more problematic when the service package of the OV-chip card will be expanded in the future. Finally, the use of contactless smart cards on this scale presents a risk for privacy, since it offers a range of new possibilities for the illicit tracking of the movements of people using these cards.
Recommendations	Make sure that consumers maintain a real freedom of choice by allowing for a dual existence of paper and electronic tickets and by making sure that anonymous versions have the same possibilities as the personalized OV-chip card and that they are obtainable under fair conditions. Last but not least, provide for adequate security measures.

2-BIOLOGICAL IDENTITY

Identification of technology	**a) The Alcazar Pleasure Card**[4] **b) The Fakkel-card**[5] **c) The VipChip**[6] **d) VIS 2000**[7] **e) Facial recognition at large public events**[8]
Technology used/tool	**Biometric systems for controlling access**
Country/use area	The Netherlands: a) In Alcazar, a local mega disco in Puttershoek which is a village close to Dordrecht in the Hoeksche Waard. b) In a public swimming pool called De Fakkel, situated in Ridderkerk which is a small town close to Rotterdam. c) In the Baja Beach Club in Rotterdam. d) Unclear. e) Unclear.
Frame of use	a) Alcazar introduced the Pleasure Card for members in 2002. It is a smartcard system used as an entrance pass with biometric features. It is used in combination with the SarFunGuard Totem, in which two biometric systems are integrated (face and fingerprint recognition). The company admits that none of the technologies are watertight and that an iris scan would be more reliable, but the disadvantage of an iris scan is the long registration time. With this system it only takes 15 seconds to get registered and that is "what customers want". The stated goal of using biometric technologies is according to the manager of the disco to prevent (violent) incidents. They claim that since the

[4] The following information is based on an interview with Buro Jansen & Janssen (12/06/09), official documents from the Dutch DPA on http://www.cbpweb.nl/themadossiers/th_bio_publicaties.shtml and on BANSAL, L., *Biometrics: the Solution for a Safer Society?*, Master thesis Science & Technology Studies – University of Amsterdam, 2007, p. 43-48.
[5] The following information is based on an interview with Buro Jansen & Janssen (12/06/09), official documents from the Dutch DPA on http://www.cbpweb.nl/themadossiers/th_bio_publicaties.shtml and on BANSAL, L., *Biometrics: the Solution for a Safer Society?*, Master thesis Science & Technology Studies – University of Amsterdam, 2007, p. 49-58.
[6] The following information is based on an interview with Buro Jansen & Janssen (12/06/09), official documents from the Dutch DPA on http://www.cbpweb.nl/themadossiers/th_bio_publicaties.shtml and on BANSAL, L., *Biometrics: the Solution for a Safer Society?*, Master thesis Science & Technology Studies – University of Amsterdam, 2007, p. 59-67.
[7] The following information is based on official documents from the Dutch DPA on http://www.cbpweb.nl/themadossiers/th_bio_publicaties.shtml.
[8] The following information is based on official documents from the Dutch DPA on http://www.cbpweb.nl/themadossiers/th_bio_publicaties.shtml.

	introduction of the Pleasure Card there are 70-75% less incidents on a Saturday night, because people are taken out of anonymity and behave more calmly. Through this card system Alcazar knows at any time who is inside the club. Moreover they justify the system by stating that the technology is not discriminating: every person gets a fair chance to enter the disco, only if you misbehave you will be blacklisted. Perhaps more importantly from a commercial point of view, the system 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. Another reason for introducing the Pleasure card was (and is) to prevent fines for serving alcohol to minors. Civil servants come and check regularly whether minors are being served alcohol. If so, Alcazar gets fined. To become a member, one has to give a fingerprint, which is stored on the smartcard, and a face scan is made too, which is stored in a central database. 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, they have to put their finger on the scan which tries to identify the fingerprint from 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. The photo of the visitor appears on the screen and third parties (e.g. guards) verify whether the face scan matches the one in their system. If you are recognized as a person on the blacklist, the totem starts beeping, prohibiting you to enter the club. Nevertheless, in an interview made by Bansal in 2007 (see reference) youngsters comment that it is easily to circumvent: you can just enter using the other entrance hall where you remain anonymous if you pay €10. You can get on the blacklist when you are kicked out of the club because of drunkenness or other misbehaviour, but you can get removed from the blacklist if you apologize at the club during a weekday. However, dealing in drugs, consuming drugs, possessing arms and fighting are

	absolutely prohibited and can't be excused. b) In August 2005 the public swimming pool called De Fakkel introduced the Fakkel-card. It is the same smartcard system as used in Alcazar and it has also been introduced for safety reasons. Visitors who don't obey the rules are registered on a blacklist and refused entrance. The system allows De Fakkel to know at any time who does or doesn't belong in the swimming pool. At the entrance in front of the recreational pool there is a SarFunGuard Totem, the biometric system with an integrated face- and finger scan to verify your identity and to check whether you're not on the blacklist. The management of the swimming pool claims that the system works preventively by taking youth out of anonymity. They also work in close cooperation with the police and the judiciary. When they block a Fakkel-card the police automatically come and if necessary the matter will be pursuited. The management of De Fakkel claims that the aggressive behaviour towards employees has reduced and that there is a decrease of people being thrown out of the swimming pool. They also consider the SarFunGuard Totem as cost-effective: at first there were six pool attendants and now there are three. c) In February 2004 the Baja Beach Club in Rotterdam introduced the VipChip as a means to stay hip and be a trendsetter. 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. The VipChip is a product from VeriChip Corporation, a company that specialises in implantable RFID microchips for the purpose of automatic identification. The microchip measures 12 mm long and 2.1 mm in diameter, roughly the size of a grain of rice. The device is implanted above the triceps in the left upper arm. It is inserted just under the skin with a syringe and the insertion procedure is performed under local anaesthetics. Customers got chipped at the club by a registered, certified nurse who gave the injection after the clearance of a doctor who checks the medical condition of the customer. The Baja Beach Club used a release waver, saying that they can't be held responsible when the chip is removed. They claim that the chip can be easily removed in hospital since the chip is

	placed under your second skin, but so far nobody wants to have the chip removed. The chip is invisible to the eye and is made of glass that cannot break. The chip contains a unique 16-digit identifier which is used as an electronic identification method. Once it is inserted under the skin, the VipChip can be scanned with a handheld or wall-mounted chip reader but the microchip is passive, which means that the chip will only be activated when a reader with the proper frequency responds to the dormant chip. When this happens the chip emits a radio frequency signal, transmitting the individuals' unique verification number. The chip can be read from 2 cm distance, but there were plans to make the scanner stronger to catch the signal from a bigger distance. The estimated lifetime of a VeriChip is over 20 years. The Baja Beach Club used the VipChip as a way to bind their VIP-clients to their club by offering them luxury services in exchange, as a sort of customer loyalty system. Off course, it was also used as a way to receive media coverage and they received a lot of positive publicity from BBC, CNN, Dutch TV-channels, etc. The integrated chip system was initiated in a special zone in the club, a VIP-deck with a jacuzzi, designed for only VIP visitors. It allowed VIP-members to identify themselves or pay their drinks without showing any identification. The system worked as follows: a scanner scans the chip in the left upper arm and one can see the photo of the person and his/her identification-number and how much money the person has on the chip. With a password customers could load and withdraw money. As a VIP-member you also always had free entrance to the club and access to the VIP-area, also you could bring one guest along. Next to this you were invited for free on special occasions. The Baja Beach Club asked €1000 for a membership with a VipChip, and customers got in return a credit of €1500 on their chip. d) The company Interstrat created in 2001 a biometric access control system for the catering industry and sports centres, called 'VIS 2000'. The stated goal of this system was to maintain order and to ensure a safer environment for visitors and personnel. In order to do this, they claim it is necessary to identify possible 'troublemakers' and thus they need to register the personal data of every visitor. The system works as follows: every person that

	visits an establishment or a sports centre, connected to VIS 2000, for the first time is obliged to be seated in front of a 'bio-engine'. Then, a digital image of the face will be made by a camera and this image will be translated into a template, which is a binary representation of the body traits. In addition, a scan will be made of the index finger, which is also translated into a template. The 'bio-engine' contains also a monitor, a card reader and a printer. The machine is connected to a personal computer which registers the data in the database of the proprietor. People considered as 'troublemakers' are placed on a central blacklist and can be refused entrance. Sometimes, the proprietor will use the images of video surveillance to find out who caused the incident. In that case, video images will be compared to the templates of the facial scans made by the bio-engine of the visitors. However, people also have the possibility to become a member of a given establishment, although some make it even compulsory. In that case, people are asked for additional data. In return, the member receives a smartcard that contains his or her membership number and his or her biometric data. When visiting the establishment, the member has to put his or her smartcard in the reader of the 'bio-engine', which will verify the templates of the face and the index finger registered on the smartcard with those retained in the central database. e) There are plans to create a system of facial recognition for access control at large public events, for example at football games. The claimed need for such a system would be to fight vandalism and enhance security. In order to do this, organizers of such events claim they need a sharp access control system which allows the identification of possible 'troublemakers' afterwards. Whether or not the visitor acquires access to the event will be an automatic decision made by a machine. The biometric method they want to use is based on facial traits. Visitors will only obtain access to the event after they get a smartcard. The smartcards are issued by the organizer of the event and requires the visitor to have a digital facial image taken. This digital facial image will be translated into a template, which will be stored on the smartcard together with an identification number, name, address and a validation period.

	These data will also be stored in a temporary database for the time of the event. Whenever the visitor passes the entrance a digital picture will be taken and the system will verify whether it corresponds to the template on the smartcard. The system also uses a central blacklist with persons to be refused entrance. This database contains the template of the facial traits and the identification number of the smartcards in question and will be retained as long as 'necessary'. In case of an incident, images of surveillance videos will also be used to identify 'troublemakers' on the basis of their templates. This can be done by private security firms or by the police.
Population concerned: target and age	a) Alcazar has a capacity of 5000 people and is every Saturday packed with young people coming from different places, even from Belgium and Germany. The Alcazar Pleasure Card is only for members and it is not compulsory to become a member in order to access the disco. Nevertheless, 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 (birthdays, parties) etc. Also, the entrance fee for non-members is €10 instead of €7. However, it is anyway free if you come before 11.00 p.m. Most people become members, since it is easier, faster and cheaper with an Alcazar Pleasure Card. The end-user pays only €5 for the smartcard. For example, about 10% of the village Puttershoek is member of Alcazar. In total, about 30.000 people have registered themselves with Alcazar. There is however an age limit, one can only obtain the card from the age of 16. b) Most pool visitors come from Ridderkerk and surrounding municipalities. Also there are many visitors coming from Rotterdam, especially during holidays. The swimming pool has 10.000 registered people. In contrast to Alcazar, visitors of De Fakkel pretty much no longer have a free choice: without signing up to the smartcard system people have very limited access to the swimming pool. For example, on Wednesdays (1.00 pm - 5.00 pm), Fridays (7.00 pm - 22.00 pm) and Sunday afternoons (1.00 pm - 5.00 pm) the Fakkel-card has been set compulsory for the recreational pool from the age of 12. These days and times were deliberately chosen because then the largest group of young people is present. The other days

	the card is not obligatory. However registration will be made compulsory after an incident. Moreover during holidays it is compulsory -each day- to have a Fakkel-card from the age of twelve. A Fakkel-card, including entrance, costs €3.50. The target group for which this system has been introduced are mostly young, male migrants since they are believed to 'cause all the troubles' in the public swimming pool. Bansal tries to explain this in her research by pointing out the strong racist tendencies in Ridderkerk. c) The VipChip was meant only for VIP-customers, so it was not compulsory to get chipped in order to access the club. There are about 70 people who got a VipChip and most of them live in or around Rotterdam. Most of the people who are chipped are regular customers, not necessarily friends. Especially older men (with a lot of money) got themselves chipped. d) Everybody visiting a given establishment or sports centre that is connected to 'VIS 2000'; some make membership even compulsory as a result of which extra information will be stored. e) Not yet introduced.
% of users/of young users	a) No specific numbers, but they are the main target group. b) No specific numbers, but they are the main target group. c) No specific numbers, but since the VipChip was aimed at VIP-customers with a lot of money, young adults are not really concerned. d) No specific numbers, but one can assume that they are part of the main target group. e) Not yet introduced, but one can assume that they would be part of the main target group.
Trends (measured/supposed)	a) The Alcazar Pleasure Card was introduced as a pilot study in 2002. Since it was evaluated as a success by the management of Alcazar, they decided to market the product because they were sure that other discos and catering industries would be interested in the product. By the end of 2002 they started a company, *Secure Access Road B.V.*, and now they have a network of about 10 discos all over the Netherlands (together with 1 swimming pool, *De Fakkel*, and 3 coffee shops), where they have implemented this system. At the moment they are also negotiating with banks to introduce a similar system. b) More and more swimming pools are interested in this system; people from Tilburg and Amstelveen have already visited De Fakkel to see

	how the system works. c) At the end of 2006 - in the beginning of 2007 the Baja Beach Club (temporarily?) stopped with implanting chips because they wanted to keep the chip exclusive. The Club claims there was still a lot of interest from customers. There are also plans to make the scanner stronger to catch the signal from a bigger distance. e) In the future, such a system could be used on a national scale.
Known or potentials dangers/Risks	Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care. By combining several data sets (e.g. personal information when registering, location data from the RFID/smart card technology, etc.) with biometric data, one can create a very detailed picture of a given person without the knowledge or consent of this person. After all, biometric data reveal al lot more information than strictly necessary for the identification purpose, thus there is a risk that this information will be used for other purposes. Moreover, since this kind of sensitive information is collected and stored by private companies who have as their prime objective making profit, there is a considerable risk that they will not implement the most effective (and thus expensive) security measures against security breaches and unauthorised use of the information. Finally, such systems do not allow people to make mistakes (e.g. (“once a thief, always a thief”).
Others	/
Generated data bases	
Associated data base/creation	a) The application for and use of the Pleasure Card is recorded in a central database. There is also a central blacklist of people who misbehaved and are no longer allowed to enter the disco. b) The application for and use of the Fakkel-card is recorded in a central database. There is also a central blacklist of people who misbehaved and are no longer allowed to enter the swimming pool. c) Unclear; the management of the Baja Beach Club claims that the VipChip is not connected to any database. Yet, they need some sort of database concerning the application for and use of the VipChip in order to manage the general system.

	d) The simple entering of an establishment or sports centre connected to VIS 2000 is recorded in a central database. Also, the application for and use of a membership card is recorded in this central database. There is also a central blacklist of people who misbehaved and are no longer allowed to enter any of the establishments or sports centres connected to VIS 2000. e) The simple access to a large public event will be recorded in a database.
What justifies the inscription in the file/Risks?	a) The application for and use of the Pleasure Card justifies the inscription in the general database. Drunkenness or other misbehaviour justifies the inscription in the central blacklist, but you can get removed from the blacklist if you apologise at the club during a weekday. However, dealing in drugs, consuming drugs, possessing arms and fighting are absolutely prohibited and can't be excused. b) The application for and use of the Fakkel-Card justifies the inscription in the general database. Misbehaviour justifies the inscription in the central blacklist. c) Presumably, the application for and use of the VipChip. d) The simple entering of an establishment or sports centre connected to VIS 2000 justifies the inscription in a central database. Also, the application for and use of a membership card justifies the inscription in this central database. Misbehaviour justifies the inscription in the central blacklist. e) The simple access to a large public event will justify the inscription in a database.
Purposes/contents, main data included/Risks?	a) The information is stored in a central database for managing the Pleasure Card system and in a central blacklist for controlling the access to the disco. When applying for a Pleasure card, personal data are stored in a central database as well as a fingerprint and a facial scan. The central blacklist registers what kind of misbehaviour took place, linked to the member in question. b) The information is stored in a central database for managing the Fakkel-card system and in a central blacklist for controlling the access to the swimming pool. When visitors apply for a Fakkel-card they have to fill up a registration form with their personal data. Next four photos and a fingerprint are made, which are stored on the smartcard and in the central database. De Fakkel also considers

	including medical data in the system. This is considered to be useful when, for example, a visitor has an epileptic attack or a heart attack. The central blacklist registers what kind of misbehaviour took place, linked to the member in question. c) The VipChip contains a unique 16-digit identifier which is used as an electronic identification method. The management of the Baja Beach Club claims that the chip contains no other data, but since it is used as a way of payment it contains off course your personal credit balance. Also, when you decide to become a member of the club a lot of personal data is requested (e.g. ID-number, name, birthday, a picture, what they like to drink, their custom drink, etc) and it is unclear how they use this information and which information ends up on the chip. For example, when your chip is scanned at the entrance, they know how you are and immediately they bring you your favourite drink. Presumably, (a lot of) this information is also held in a central database in order to manage the general system. d) The information is stored in a central database to maintain order and to ensure a safer environment for visitors and personnel and in a central blacklist for controlling access. For a simple visit, a template of the facial scan and the index finger are retained in the central database. When people decide, or are obliged, to become a member additional data (such as name, address, age, hobbies, preferences, etc) will be stored as well. The central blacklist will register the personal data together with a code for the misbehaviour that took place. e) The information will be stored in a central database in order to fight vandalism and enhance security. It will contain at least the template of the facial scan. The central blacklist will register the template of the facial traits and the identification number of the smartcard in question.
File masters? Risks?	a) The management of Alcazar disco, which are also the owners of the company Secure Access Road B.V. The fact that privately-held companies own such sensitive data, and this without the necessary checks and balances, is a frightening evolution. b) The management of De Fakkel. The fact that privately-held companies own such

	sensitive data, and this without the necessary checks and balances, is a frightening evolution. c) The management of the Baja Beach Club. The fact that privately-held companies own such sensitive data, and this without the necessary checks and balances, is a frightening evolution. d) Unclear whether this is Interstrat and/or the different proprietors that take part in VIS 2000. When different parties can alter information in the central database, mistakes are more likely. Again, the fact that privately-held companies own such sensitive data, and this without the necessary checks and balances, is a frightening evolution. e) Unclear.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	a) The management of Alcazar has access to the files. It is unclear if they share their data with third parties although the manager of Alcazar stressed that they were not allowed to share the data from their database (and thus blacklisted persons) with other discos. b) The management of De Fakkel has access to the files. They also work in close cooperation with the police and the judiciary, but it is unclear to what extent they have access to the database. c) The Baja Beach Club in Barcelona also uses the VipChip and they share their database with the Baja Club in Barcelona (and vice versa). This proves that some sort of database is held, only it is unclear what type of information is stored. d) At least the proprietors that take part in VIS 2000, but it is unclear whether or not Interstrat can access the database as well. Also, the data can be handed over to law enforcement agencies to investigate criminal offences, but it is unclear under which conditions. e) Unclear. Possibly also private security firms and the police.
Data retention period/risks Right to be forgotten	a) Unclear. b) Unclear. c) Unclear. d) Unclear concerning the data stored on members. People who simply entered a given establishment or sports centre connected to VIS 2000, but did not apply for membership; those data are only retained until closing time unless there was an incident. The personal data, together with a code for their misbehaviour, of people on the blacklists are kept as long as 'necessary'. e) Unclear/Not yet introduced.
Rights to know or to modify data?	a) Unclear.

	b) Unclear. c) Unclear. d) Unclear. e) Unclear/Not yet introduced.
Covert purposes/Risks/uncontrolled future evolution	a) There is a risk that these data are used for commercial purposes. b) There is a risk that these data are used for commercial purposes. c) There is a risk that these data are used for commercial purposes. Also, there is a risk that the Vipchip can track people and trace their spending habits, hence invading their civil liberties. However, the Baja Beach Club states firmly that the chip contains no Global Positioning System (GPS) tracking capabilities. d) The registered personal data in VIS 2000 can be used for commercial purposes (e.g. for marketing purposes) or for management purposes. Also, the data can be handed over to law enforcement agencies to investigate criminal offences, although this is not a primary goal of VIS 2000. e) Unclear/Not yet introduced.
Others (interconnections…)	a) Secure Access Road B.V. (i.e. the management of Alcazar) provides this SarfunGuard system also to other discos (a swimming pool, etc) so there is a risk that the respective databases are/become interconnected although the manager of Alcazar stressed that they're not allowed to do so. b) More and more swimming pools are interested in the system, and people from Tilburg and Amstelveen have already visited De Fakkel to see how the system works. The management of De Fakkel considers to share their databases with other swimming pools, which would have for effect that if a person is no longer allowed to enter one swimming pool, that person would also not be able to enter any other swimming pool within the associated network. Also, swimming pool De Fakkel uses the same supplier as Alcazar, which is the company Secure Access B.V. c) The Baja Beach Club in Barcelona also uses the VipChip and they share their database with the Baja Club in Barcelona (and vice versa).
Legislation in application	
Law/rules/others (?)	a) In the Netherlands there is no specific legislation for the use of biometrics. There are however general rules for the protection of personal data that also apply to biometrics and determine the conditions of usage. For example,

	one has to look at proportionality and necessity and question whether the use of biometrics weighs up in relation to the problem. The general privacy law of 1992 applies. b) There is no specific legislation adopted; the general privacy law of 1992 applies. c) There is no specific legislation adopted; the general privacy law of 1992 applies. d) There is no specific legislation adopted; the general privacy law of 1992 applies. e) There is no specific legislation adopted; the general privacy law of 1992 will apply.
Risks for freedoms despite the law	Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care. By combining several data sets (e.g. personal information when registering, location data from the RFID/smart card technology, etc.) with biometric data, one can create a very detailed picture of a given person without the knowledge or consent of this person. After all, biometric data reveal al lot more information than strictly necessary for the identification purpose, thus there is a risk that this information will be used for other purposes. Moreover, since this kind of sensitive information is collected and stored by private companies who have as their prime objective making profit, there is a considerable risk that they will not implement the most effective (and thus expensive) security measures against security breaches and unauthorised use of the information. Finally, such systems do not allow people to make mistakes (e.g. (“once a thief, always a thief”).
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	a) Not foreseen. b) Not foreseen. c) Not foreseen. d) Not foreseen. e) Not foreseen.
Conformity with the European right (Charter of fundamental rights, directives…)	On European level, there is also no specific legislation for the use of biometrics; only general rules for the protection of personal data apply. One can wonder whether it complies with the conditions of finality, proportionality and necessity of article 8 ECHR.
Implementation (or not) of the legislation?/Risks	c) The Baja Beach Club claims they never had to deal with the general privacy law or other privacy issues.

Others	/
This tools and young public or young adults	
How far are young people concerned?	a) According to the research made by Bansal (see reference) young people hardly make complaints on principal grounds, such as an invasion to their right to privacy, but rather about the overload on SMSs and emails they receive from Alcazar. They agree with the fact that it can enhance security, but they don't always feel this in reality. For example, one boy stated that Alcazar wants to know everything, but never checks the information they receive from customers. b) According to the research made by Bansal (see reference), most young people have no problems at all with the Fakkel-card and are ready to give their personal data at any time. They are grown up with these technologies and find them cool and hip. Also, they are confronted with it in many settings (e.g. discos, football stadiums) and consider it normal practice. d) Unclear. e) Unclear/Not yet introduced.
Awareness of issues or of risks	a) see above b) According to the research made by Bansal (see reference) both employees as most of the visitors experienced a better and 'safer' atmosphere after the introduction of the Fakkel-card. Anyhow, they see the Fakkel-card as a much 'softer' system than placing security guards at the pool. Nevertheless, around 3% of the regular visitors of De Fakkel raised objections against the biometric entrance system. Most of them were elderly people who made a comparison with the Second World War, especially because they didn't find themselves to be dangerous people. Also, Bansal noticed in her research that highly educated people have a more critical view on privacy. However, most people were easily swayed, when explained that it diminishes 'nuisance' and 'trouble' but mostly because of the discounts. If you have a Fakkel-card the fee is €3.15 otherwise it costs €3.40 and if you swim 10 times, the 11th time you can swim for free. The mantra "if you have nothing to hide, you have nothing to fear" works well for many people. Most of all, people don't tend to reflect on what happens with their personal data and they didn't ask this either when applying for a Fakkel-card. However, when asked by Bansal most people do not want their data to be shared with third parties

	and expect them to be treated confidentially. c) In an interview made by Bansal in 2007 (see reference) most customers didn't see any problems with the VipChip, although not everyone wanted it for themselves. d) Unclear. e) Unclear/Not yet introduced.
Indifference or reaction	a) Some youngsters like the Pleasure card since it is "an extra card in their wallet" what makes them feel important. b) Some people notice a difference: "prices have gone up, they dislike the cameras, there are fewer people and more 'white' people since coloured people are strictly watched and sent away". Nevertheless, according to the management of the swimming pool, even those people with fundamental problems concerning the biometric system did not leave De Fakkel; they only swim on days when the Fakkel-card is not compulsory. c) Most people remain quite reluctant to get a 'foreign' thing in their body. Therefore, the Club launched an action to win people over: the first 25 people got the chip for free. Also, 3 employees got themselves chipped as an example for other customers. d) Unclear. e) Unclear/Not yet introduced.
Awareness campaigns/results	a) No awareness campaigns. b) No awareness campaigns. c) The Baja Beach Club received a lot of positive media coverage from BBC, CNN, Dutch TV-channels, etc. However, there was also some public resistance against the VipChip. Katherine Albrecht, for example, from the organization C.A.S.P.I.A.N. ("Consumers Against Supermarket Privacy Invasion and Numbering") claims that the Vipchip can track people and trace their spending habits, and therefore invades our civil liberties. C.A.S.P.I.A.N. owns a website with background information and Katherine Albrecht also wrote a book ("SPYCHIPS: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move") on this topic, but it is unclear to what extent they were successful in raising awareness. The Baja Beach Club always continued to deny their message. d) No awareness campaigns. e) At the moment there are no awareness campaigns.
Good practises	/
Campaign to be led. On which themes?	/

Others	/
Conclusions	Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care. In the cases mentioned above, one can wonder whether the conditions of necessity and proportionality have been met, although the Dutch DPA concluded so.
Recommendations	Apart from the above-mentioned question whether or not the maintenance of order and security can be an acceptable purpose for the use of biometrics, it is important that it happens with the best security measures, effective rights for the data subject and independent oversight.

3-INTERPERSONAL COMMUNICATIONS

TELECOMMUNICATION SERVICES

Identification of technology	Telecommunication services
Technology used/tool	**(Mobile) phone and IP-based telecommunication services** (such as email, VoIP, instant messaging)[9]
Country/use area	The Netherlands (as the rest of the world)
Frame of use	For the transmitting of information in a quick and easy manner to people residing elsewhere without having to move itself (physically). Most people use it on a daily basis for different purposes in their private and professional life.
Population concerned: target and age	Nearly everyone uses it, especially youngsters.
% of users/of young users	No specific numbers
Trends (measured/supposed)	The applications and use of telecommunication services keep increasing; at the moment it has become very difficult to nearly impossible to take part in the (Dutch) society without using those services. According to the 2009 ENISA report[10], the Netherlands has even reached one of the most advanced levels of development of the information society. Indicators show that the Netherlands is at the forefront of disseminating ICT in the economy and that they have a high level of ICT skills in the population and in the workforce.
Known or potentials dangers/Risks	Since telecommunication services are increasingly interwoven in our daily lives and since telecom operators and internet service providers (ISPs) register (although temporarily) most of the log data of these communications, there is a risk of an invasion to our right to privacy and of a limitation of our autonomy. After all, individual choices are registered and can be passed on to third parties (such as governments). Also according to the ENISA 2009 report, general

[9] The following information is based on an interview with Buro Jansen & Janssen (12/06/09) and on the following link: http://www.edri.org/edri-gram/number7.8/data-retention-netherlands.
[10] http://www.enisa.europa.eu/doc/pdf/Country_Pages/Netherlands.pdf

	IT developments clearly impact on network and information security. In general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more network and information security gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats. In short, an individual's online security risk increases in parallel with the time he or she spends online.
Others	/
Generated data bases	
Associated data base/creation	a) The database retained by every telecom operator and ISP operating in the Netherlands. b) The database to be retained by the telecom operators and ISPs operating in the Netherlands when the European data retention directive (2006/24/EC) will be implemented.
What justifies the inscription in the file/Risks?	a) The fact that the data are necessary for the good operation of the communication network, to justify the amount of a given invoice, or when requested by the customer. It is also possible to retain data when these are needed for a market research when telecom operators and ISPs have the prior consent of the customers, although the latter is not always the case in practice. b) The fact that a European Directive requires those data to be retained although national member states tend to use this obligation to ask telecom operators and ISPs to retain additional data.
Purposes/contents, main data included /Risks?	a) The prior reason to keep a database for telecom operators and ISPs is to ensure the smooth running of the communication network and services. Next to this, it is also meant as a service to the customer by allowing him/her to verify the invoice. However, there is a risk that these data are abused for commercial purposes, such as direct marketing, without the explicit consent of the customer. The main data included are traffic and location data (such as caller, recipient, date, time and duration of a given call/SMS/email, the technology used (phone call, SMS, email, VoIP), etc.) combined with the information needed to identify the regular user (e.g. name, address for invoice, bank account). b) The stated goal on European level is to ensure the retention of traffic and location data for the investigation, detection and prosecution of serious crime, although the usefulness and

	necessity thereof have never been proven. As the European Directive, the Dutch data retention law is very vague, thus it is not always clear what exactly needs to be retained and there is a risk that they will broaden the scope for access to the data (exactly what constitutes as 'serious' crime). For example, whereas the European data retention directive does not require the retention of the destination for Internet use other than e-mail or telephony, the Dutch list does not make this distinction anymore. However, a royal decree will follow later with more details on the data retention obligation in practice. The main data to be included in the database will also be traffic and location data (such as caller, recipient, date, time and duration of a given call/SMS/email, the technology used (phone call, SMS, email, VoIP), etc.) combined with the information needed to identify the regular user (e.g. name, address for invoice, bank account). However, this database needs to be kept separate from the first one (see a)), thus obliging telecom operators and ISPs to a dual storage of these data.
File masters? Risks?	a) The respective telecom operator and ISP operating in the Netherlands. b) At first, the telecom operators and ISPs will store the data but this could change in the future. An amendment that would have restricted the possibility of claiming complete data sets by national security and law enforcement agencies didn't make it. Also, the question about storage of the data in centralized or decentralized facilities has been evaded. This will also be clarified in the royal decree.
Who accesses the files/ Sharing of the database? Access limits? /Risks	a) Telecom operators and ISPs have access to their respective database (see above). There is a risk that they sell their data to third parties for commercial purposes. National security and law enforcement agencies can demand certain data (e.g. traffic and location data, or even phone tapping) from telecom operators and ISPs under conditions set forth by law (e.g. when requested by a Prosecutor for a crime that is punishable with at least four years of imprisonment). b) As long as the telecom operators and ISPs will store the data, they will hand over the requested data to the requesting national security or law enforcement agency under conditions set forth by the law and the upcoming royal decree. However, an amendment that would have

	restricted the possibility of claiming complete data sets by national security and law enforcement agencies -to be used for data mining in the context of combating terrorism- didn't make it. So in principle, both national security and law enforcement agencies will have the possibility to claim complete parts of the collection of data to be retained.
Data retention period/risks Right to be forgotten	a) Unclear, presumably for the duration that an invoice can be challenged or as long as necessary for the good operation of the communication network and service. However, in the latter case, the traffic and location data must be stored in such a manner that they can no longer be traced back to the communicating individuals. b) The Dutch parliament has lowered the data retention term to 12 months for telecommunication data and to 6 months for Internet data (instead of the 18 months the government wanted). Time starts running from the moment the data are processed for the first time.
Rights to know or to modify data?	a) Customers receive a monthly invoice that they can challenge and they can always ask their operator or provider what kind of data is retained on them and ask for modification. However, as long as people are not informed about the processing of their data (e.g. in cases of direct marketing without prior consent), they can't exercise their rights such as the right to modification or deletion of their data. b) Unclear.
Covert purposes / Risks / uncontrolled future evolution	a) Direct marketing, spam, the unauthorised transferring (e.g. selling) of sensitive information to third parties etc. Also, there is a risk that national security and law enforcement authorities will increasingly ask for such data without the necessary guarantees. b) The government acting as an authoritarian State, placing every citizen under surveillance, thus limiting autonomy and fundamental rights. If telecom operators and ISPs need to retain such a huge amount of data, certainly since they will not be remunerated for it, they will not be very keen on installing high (and thus expensive) security mechanisms to prevent security breaches and unauthorised use. In the worst-case scenario they will even be tempted to do something lucrative with it.
Others (interconnections…)	/
Legislation in application	

Law/rules/others (?)	a) The general law on telecom-munications ("*Telecommunicatiewet"*) from 19 October 1998 applies. Access to the data by national security and law enforcement agencies is regulated by articles 28-29 of the law on intelligence and security agencies ("*Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten*") and by articles 126n and 126u of the Code of Criminal Procedure. b) The new law adapts the general law on telecommunications from 1998 and is called "*Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatie-gegevens)*". A royal decree with more details on the data retention obligation in practice will follow. Also, access to these data by national security and law enforcement agencies is regulated by articles 28-29 of the law on intelligence and security agencies ("*Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten*") and by articles 126n and 126u of the Code of Criminal Procedure.
Risks for freedoms despite the law	a) Direct marketing, spam, the unauthorised transferring (e.g. selling) of sensitive information to third parties etc. Also, there is a risk that national security and law enforcement authorities will increasingly ask for such data without the necessary guarantees. b) An invasion to the right to privacy and the risk of an authoritarian or Big Brother state. There is also a risk that telecom operators and ISPs will not be very keen on installing high (and thus expensive) security mechanisms to prevent security breaches and unauthorised use. In the worst-case scenario they will even be tempted to do something lucrative with it.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	a) Not foreseen. b) Royal decree expected due to European Directive 2006/24/EC. This means a significantly set back for privacy and human rights. Even worse, the Dutch Government sees the current data retention law as being of a limited

	nature. They already point to a possible extension of data retention at the European level, in particular a drastic extension of data retention obligations with regard to online communications, as well as its retention period.
Conformity with the European right (Charter of fundamental rights, directives…)	b) Since the European Directive is a clear violation of article 8 ECHR, the same counts for the Dutch data retention law. Even worse, the Dutch Government downplays the interference of the data retention obligation with fundamental rights. The Government sees the current data retention law as being of a limited nature. They already point to a possible extension of data retention at the European level, in particular a drastic extension of data retention obligations with regard to online communications, as well as its retention period.
Implementation (or not) of the legislation?/Risks	b) At the moment the Dutch data retention law isn't implemented yet and the practical implementation of the law concerning ISPs will probably take a lot of time.
Others	/
This tools and young public or young adults	
How far are young people concerned?	a) Unknown. b) Unknown.
Awareness of issues or of risks	b) There has been a lot of stir between the different political fractions, especially the Dutch Senate has been more critical of data retention in the last four years. Although the debate focused a lot on the retention term and the lack of evidence, there are many other issues that were debated. For example, the extent of parliamentary involvement with the contents of the decree which will contain more details about data retention in practice. The law now contains a list of data to be retained, but the list is not very precise. It is as general as the list in the directive and seems to contain a mistake. This political debate, together with the awareness raising campaign of some NGOs, made the Dutch public somewhat aware of the issues at stake. There has also been a case reported on TV of how an innocent woman became a victim of wrongfully processed telecommunication data[11].
Indifference or reaction	a) Unknown. b) Unknown.
Awareness campaigns/results	b) There have been some campaigns, mostly led by internet access provider XS4ALL and BOF (Bits of Freedom). Especially the latter has mostly been active on the European level when the

[11] http://cgi.omroep.nl/cgi-bin/streams?/id/NCRV/serie/NCRV_1239778/NCRV_1246780/bb.20070430.asf?start=00:17:11&end=00:30:00.

	European Directive was being discussed. Their campaign comprised of providing information to the public through their websites and by launching a petition together with other partners such as EDRI. The campaign was successful in the sense that it resulted in a stronger network of European organisations working on this topic and helping each other with information and analyses. The Directive however was voted despite the petition that managed to receive a lot of signatures. XS4ALL and people behind the BOF-organisation (it is no longer active as such) continued activating against a Dutch data retention law and managed to receive the support of some politicians. This certainly helped in lowering the data retention term from 18 to 12 and 6 months.
Good practises	/
Campaign to be led. On which themes?	b) The Dutch Senate passed a motion that asks the Dutch government, in view of all the questions about the implementation and efficiency of data retention that were discussed, to voice the concerns of the Senate in the European evaluation context. The Senate hopes something good can come out of this evaluation that will be carried out by the European Commission in 2010. However, a positive outcome will depend mostly on whether or not the German Constitutional Court (or any other Court where a case is pending) rules favourably.
Others	b) The costs of the data retention obligation for the sector and consumers were also an issue of debate, but the available cost estimates are still vague. One of the reasons off course is that the precise scope of the data retention obligation for Internet traffic is still unclear. The government will not reimburse general costs of data retention.
Conclusions	a) Telecom operators and ISPs operating in the Netherlands keep a database to ensure the smooth running of their communication network and services. Next to this, it is also meant as a service to the customer by allowing him/her to verify the invoice. However, there is a risk that these data are abused for commercial purposes, such as direct marketing or the unauthorised transferring (e.g. selling) of sensitive information to third parties without the explicit consent of the customer. Also, there is a risk that national security and law enforcement authorities will increasingly ask for such data without the necessary guarantees. b) A general obligation to retain traffic and

	location data is a serious violation of the right to privacy and it turns 16,3 million Dutch citizens into potential suspects. Also, a general retention obligation disrupts the professional secrecy of doctors, lawyers, journalists and clergy, as well as political and business activities that require confidentiality. Moreover, the necessity of it has never been proven and experts question the value of this measure not only because data retention turns out to be unsuited in practice, but also because it imposes a disproportionate financial and practical burden on all parties involved. Nevertheless, the Dutch Government downplays the interference with fundamental rights and even wishes to extend the data retention obligation through the European level.
Recommendations	a) Strong supervision of the Dutch DPA on the abidance of telecom operators and ISPs with the conditions set forth by the Dutch and European telecommunications laws. Strong competences and means for the Dutch DPA to allow them to do their job. b) No general retention obligation.

4-SOCIAL NETWORKS AND NEW GATE KEEPERS OF COMMUNICATIONS

HYVES

Identification of technology	**Hyves**
Technology used/tool	Social network site
Country/use area	The Netherlands
Frame of use	Hyves is a free Dutch social networking site which has been online since October 2004. The site was launched by Raymond Spanjar, Koen Kam and Floris Rost van Tonningen. The name Hyves comes from the English Beehive - not from Hives, hereby comparing the users to bees in a hive. Since the domain hives.nl was already registered, they chose to call their website Hyves. The focus of this website is on keeping in touch with existing friends and making new friends. There is no need to have knowledge of HTML for creating a Hyve-account. It is comparable with other social networking sites. Users can create personalized pages of themselves with rich media content, such as photos, videos, flash content and custom layouts. Hyves started a market place as well.
Population concerned: target and age	A lot of famous Dutchmen have a profile on Hyves. Politicians, sportsmen, authors, actors promote themselves through their profile on Hyves. Users that are not yet 16 may only create an account subject to the prior consent of their parents or guardian.
% of users/of young users	About 9 million members, of which two third checks its account at least once a month (5.5 million). The average user is 27. Between the ages of 35 and 49, 66% of the Dutchmen visit Hyves, above

	50, 30%. Between the age of 13 and 34, even 80% of the Dutchmen visit Hyves[12].
Trends (measured/supposed)	In July 2008 Hyves announced that they had reached 7 million users, of which about 5 million were Dutch[13]. This amounts to about a third of the entire population of the Netherlands. In 2007, the website was voted "most popular website of the year" in the "Website of the year" competition[14]. In 2006 and 2007 Hyves also won another "Website of the year" competition in the category for blogs and communities.
Known or potentials dangers/Risks	Young users seem to be unconscious about the visibility of their profiles. There seems to be little awareness of the possibility to limit information to a defined group of users.[15]
Others	/
Generated data bases	
Associated data base/creation	Data submitted by the users and collected by Hyves.
What justifies the inscription in the file/Risks?	The subscription to Hyves and thus the consent of the user with the prevailing user conditions.
Purposes/contents, main data included/Risks?	In order to be able to make optimum use of the Services offered by Hyves, users have to create a personal Hyves account. They are obliged to provide name and surname, e-mail address and user name. This information is sufficient in order to be able to use Hyves. But certain Services such as the market place cannot be used without providing more information. Users can indicate their interests as part of their profile. This is useful for other users and for Hyves to be able to adjust the site to the users' wishes. Users can indicate who is allowed to view their account (nobody, only your friends, everybody). Users can also indicate that they want to receive information from third parties. Hyves also collects automatically generated information about surfing behaviour during the use of Hyves. This information consists for instance of IP addresses, the browser type (computer program to enable the viewing of internet pages), the pages visited and "cookies".
File masters? Risks?	Hyves.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Profiles and other files are in general public, but can be restricted by users: this is an active process and does not occur automatically. According to Hyves the police will not access

[12] http://www.hyves.nl/index.php?l1=ut&l2=ab&l3=ns&pressmessage_id=1265944
[13] http://www.nu.nl/internet/1341428/hyves-verwelkomt-donderdag-5-miljoenste-lid.html
[14] http://onlineawards.nl/winners.php
[15] http://kathalijnebuitenweg.hyves.nl/blog/1433821/Exhibitionisme_3/a4ef/

	information unless they have a court order. This concerns the data that are restricted to friend groups. Other data are accessible for everybody.[16] The information placed on Hyves will not be used for commercial purposes, with the exception of the diversification of advertising.
Data retention periods/risks Right to be forgotten	Unknown.
Rights to know or to modify data?	Users can check and modify their data in their account. If they want to know which details Hyves has recorded or if they want to change details that they cannot change in their account, they can send a question via the site.
Covert purposes/Risks/uncontrolled future evolution	For technical and operational reasons users' data may be transferred to (servers of) companies affiliated to Hyves and/or advertisers in the United States or other countries outside Europe where the regulations in the field of privacy protection might not provide the same protection as in the European Union.
Others (interconnections…)	People who are active on Twitter also import information to Hyves; it resembles the Hyves-function "*WieWatWaar*" or "who, what, where"[17]. Also, Flickr can be used to upload pictures on Hyves.
Legislation in application	
Law/rules/others (?) (implemented for this data base or this technology)	No specific legislation was adopted; the general law on telecommunications ("*Telecommunicatiewet*") from 19 October 1998 applies. The manner in which personal details are saved and used has been reported to the Dutch Data Protection Authority under number 1328365.
Risks for freedoms despite the law	There is a risk that data posted on social networking sites are accessed without authorization (e.g. by hackers), are misused for profiling, can lead to discrimination (e.g. by future employers), etc.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen.
Conformity with the European right (Charter of fundamental rights, directives…)	
Implementation (or not) of the legislation?/Risks	
Others	/
This tools and young public or young adults	
How far are young people concerned?	From the Dutch people between the age of 13 and 34, 80% uses Hyves on a regular basis. It

[16] http://www.nu.nl/internet/735522/hyvesnl-ook-populair-bij-politie.html
[17] http://www.hyves.net/index.php?l1=ut&l2=ab&l3=ns&pressmessage_id=1265939

	seems that young users are unconscious about the visibility of their profiles. There seems to be little awareness of the possibility to limit information to a defined group of users[18].
Awareness of issues or of risks	See above
Indifference or reaction	As noted below (footnotes 8 & 9) Hyves delivers a large description of rights en duties of its users. These 'Terms of Use' and the 'Privacy Policy' are submitted to new members but could easily be ignored.
Awareness campaigns/results	Hyves provides their users with a Privacy Declaration[19], and dedicates a category in the FAQ section[20] to the issue of privacy.
Good practises	
Campaign to be led. On which themes?	/
Others	/
Conclusions	At the moment, Hyves is by far the most popular social networking site in the Netherlands. The focus of this website is on keeping in touch with existing friends and making new friends. The way it functions is comparable with other social networking sites. Hyves provides their users with a Privacy Declaration and dedicates a category in the FAQ section to the issue of privacy. Nevertheless, young users seem to be unconscious about the visibility of their profiles. There seems to be little awareness of the possibility to limit information to a defined group of users.
Recommendations	

[18] http://kathalijnebuitenweg.hyves.nl/blog/1433821/Exhibitionisme_3/a4ef/
[19] http://www.hyves.nl/privacy/
[20] http://www.hyves.nl/help/