The Use of Privacy Enhancing Aspects of Biometrics

Biometrics as a PET (privacy enhancing technology) in the Dutch private and semi-public domain

Tilburg University
TILT – Tilburg Institute for Law, Technology, and Society
P.O. Box 90153
5000 LE Tilburg
The Netherlands
<a.c.j.sprokkereef@uvt.nl>

Paul de Hert
Annemarie Sprokkereef

January 2009

Centrum voor Recht, Technologie en Samenleving
Postbus 90153 • 5000 LE Tilburg • Bezoekadres > Warandelaan 2 • Tilburg • Telefoon 013 466 81 99 •
www.uvt.nl/tilt/

The Use of Privacy Enhancing Aspects of Biometrics
In the context of the main theme E-Participation/E Service of the "Alliantie Vitaal Bestuur" – EZ, BD, BZK

This report concerns the question to what extent biometrics are used as a PET (Privacy Enhancing Technology) in the Netherlands. The key issues addressed are:

- is PET a concept that plays a role in the use of biometrics in the semi-public and private domain;
- Is the current regulatory framework appropriate for fostering privacy-enhancing employment of biometrics?

The report consists of four parts:

[1] These case studies concern the use of finger scans in a primary school, a swimming pool, and a supermarket, and hand geometry in a private sports club.

We are indebted to Thijs Bosters, Karolina Owczinyk, and Irene Voets for their persistent efforts in gathering data for the inventory. Suad Cehajic has carried out most of the research for case study Two and Three. Vivian Carter has given excellent support throughout. We would like to extend our grateful thanks to the members of the Alliantie Vitaal Bestuur supervisory committee: Jaap-Henk Hoepman (TNO), Lotte Nijland and Tjabbe Bos (Dutch Ministry of Home Affairs) for their valuable comments and corrections. Any omissions/errors remaining are our own.

Chapter 1 The Legal Framework

1.1 Introduction

Technological progress in the development of biometric techniques is unmistakable. The technological functionality of available systems is maturing, showing improved capability. With biometric techniques, we refer to the identification or authentication of individuals based on a physical characteristic and using information technology and mathematical and statistical methods. [2] The average minister, official or parliamentarian involved in law making, will face difficulties in assessing the efficiency of the biometric techniques as used in commercial applications currently available on the market. The main reason for this is that the information available is often contradictory. According to a report of the TAB[3] the main problem is the blurring of boundaries between potential (=future) and current capacity of biometric applications. This is a source of technical and political confusion. [4] Even more complex, also for experts, is an assessment of the societal impact of the use of biometrics.[5] A systematic, constantly updated and forward looking analysis and assessment of the societal, economic and legal impact of further growth of the use biometric applications should inform the political process. This report should be seen in this light. It is primarily concerned with the regulation of the use of biometrics in the private sector in the Netherlands. It will focus on the evolving legal framework, the use of biometrics as PET and the use of biometrics in practice. This report will not discuss the current technical state of the art, unless it is directly relevant for a discussion of the legal framework or the concept of biometrics as a PET.[6] The first point we would like to make is that legislation has not acted as a barrier for biometric producers to place their products out on the public, semi public and private market. Over the last ten years, unlimited commercial possibilities have opened up in the areas of private electronic legal and commercial transactions, large scale national and international (EU) state systems (including production and use of millions of machine readable documents containing biometrics) and private and public sector arrangements of access to physical and electronic spaces.[7] In the EU, the existing data protection legislative framework governs the use of biometrics and there is no separate legislation. As the principled stand of data protection towards technology is characterised by an 'enabling logic' the law has not acted as a barrier to diffusion of biometric technologies. Whilst data protection legislation makes existing processing practices transparent, as a rule it does not prohibit them.[8] In other words, data protection regulations create a legal framework based upon the assumption that the processing of personal data is allowed and legal in principle.[9] Therefore, ownership of individuals regarding their

[2] The definitions used for biometrics vary (also by Dutch authors compare R. Hes, 1999; Prins, 1998; Van Der Ploeg, 1999 and 2003; De Leeuw, 2007; Grijpink, 2008) but will not be discussed here.
[3] Conclusion of the TAB working report no 76, Petermann (2002) p 1.
[4] The view of biometrics as a technology in the making can also be a political strategy. On theories of technology as political strategies see: Van der Ploeg, 2003.
[5] See Grijpink (2005); Ashbourn (2003) and Sprokkereef (2008).
[6] See for a description and analysis of latest developments for example Grijpink, 2008; and EBF, 2007.
[7] More specifically, the applications used commercially in the private or public sector can be divided into five groups: user access control, personal identification, equipment/data system access control, electronic access to services, a range of 'other' convenience areas.
[8] There are exceptions: namely those parts of the data protection regime that provide for a prohibition of processing (e.g. sensitive data, secretly collected personal data) actually fall under a privacy or opacity ruling.
[9] An outright processing ban effectively applies only to special categories of sensitive personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

data is not recognised, but individual controlling rights are granted instead. In fact, data protection does not recognise any ownership rights at all. Neither the individuals, nor collector for his intellectual contribution or the institution where data are collected, are property rights holders with regard to the data. There is also no question of shared ownership. Data flow and belong to everybody. Concerns with regard to privacy, data protection *and* intellectual property rights may lead to certain regulations that aim at distributing certain procedural rights and patrimonial rights, but their reach remains within strict limits far away from all suggestions of a property right.

Below, we will focus on the technology-law interface. [10] In a description of the legal framework, we will try to throw some light on the relationship between the legal and the technical. The focus will be on the question whether the current regulatory framework is appropriate for fostering privacy enhancing employment of biometrics.

In chapter 2 (PET) and in chapter 3 (case studies) we will subsequently assess to what extent biometrics can be used as privacy enhancing technology and whether these possibilities are used and applied in current Dutch practice.

1.2 Legal Principles Governing Personal Data

We take as a starting point that all biometric data are personal data protected by data protection legislation. This means that the legal framework in the Netherlands consists of Article 10 of the Dutch Constitution, Directive 95/46/EC (hereafter 'The Directive')[11], The Wet Bescherming Persoonsgegevens[12], and a number of other specialized laws and regulations such as the Wet op de Geneeskundige behandelingsovereenkomst, de Wet Gemeentelijke Basisadministratie and the Telecommunicatie wet. Before dealing with this legislation in detail, we will first extract some basic principles behind these laws and will formulate some questions that show how these principles might affect the choice or even admissibility of the use of certain types of biometrics.

In accordance with Article 6 of the Directive, personal data must be collected for specified, explicit and legitimate purposes only and may not be further processed in a way that is incompatible with those purposes. In addition, the data themselves must be adequate, relevant and not excessive in relation to the purpose for which they are collected (principle of purpose). Once the purpose for which data are collected has been established, an assessment of the proportionality of collecting and processing these data can be made. Thus, some data protection principles relevant in the context of this report are confidentiality, purpose specification, proportionality and individual participation[13]. If we translate this into day-to-day biometrics these principles can lead to questions such as:

Confidentiality: Has the biometric system concerned been sufficiently tested to warrant a minimum level of confidentiality protection?

[10] A first attempt to answer this question was made by Artz and van Blarkom, 2002.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, of 23 November 1995, 31 also available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (part 1) and http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf (part 2) (last visited on 29 September 2008).

[12] The Dutch framework law ("Personal Data Protection Law") of 2001 implementing the Directive.

[13] (Article 29 Working Party: working document on biometrics 12168/02, 1.8.2003 and 11224/04, 11.8.2004)

Purpose specification: Is there sufficient protection against unauthorised use of the biometric data for purposes beyond the original goal. Can purposes keep being added? To what extent does the collection of biometric data aim to discriminate?

Proportionality: Are the biometric data adequate, relevant and proportional in relation to the purpose for which they are collected? More specifically, is verification being used, when there is no need for identification? Is one biometric more proportional than another? Is the use of one finger scan easier to justify than the use of three or even ten?

Individual participation: Are fallback procedures put into place in cases where biometric data, be it raw images or templates, become unreadable or in case individuals are not able or willing to provide a biometric?

1.3 The European Data Protection Framework

Three first pillar instruments govern the EU data protection framework. First, by a general Directive 95/46/EC[14] (hereafter called the Directive). Second, by a specific Directive 97/66/EC[15] concerning the processing of personal data and the protection of privacy in the telecommunications sector (replaced by the privacy and electronic communications Directive 2002/58/EC in 31 October 2003)[16]. Third, by Regulation No 45/2001 of the European Parliament and of the Council of 18 December 2001, on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.[17]

As already made clear above, the Directive constitutes the main and general legal framework for the processing of personal data. [18] Although the Directive does not mention biometric data as such, its legal provisions and principles also apply to the processing of biometric data. It has been claimed that the Directive does not apply to biometric data in specific processing circumstances, that is to say when the data can no longer be traced back to a specific identifiable person. Nevertheless, one has to acknowledge that the essence of all biometric systems per se is that the data processed relate to identified or identifiable persons. These systems use personal characteristics to either identify the person to whom these characteristics belong or to verify that the characteristics belong to a person that has been authorised to use the system. [19] In most cases where biometric data are concerned

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal,* L 281, 23 November 1995, 31-50.

[15] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; *Official Journal*, L 024 , 30 January 1998, 1-8

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *Official Journal* L 201, 31 July 2002. Article 3 §1 states: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". On the scope of application of the new Directive, see: Louveaux and Perez Asinari, 2003, 133-138.

[17] *Official Journal*, L 8, 12 January 2001

[18] Article two (a) of the Directive defines personal data as 'any information relating to an identified or identifiable natural person'.

[19] According to the Biovision Best Practice report (Albrecht, 2003): personal data that relate to the implementation of a biometric at least include: the image or record captured from a censor; any transmitted form of the image or record between sensor and processing systems; the processed data, whether completely transformed to a

there is a link to the person at least for the data controller, who must be able to check the final proper functionality of the biometric system and cases of false rejects or false matches. For more detail on the interpretation of the four key elements to the definition of personal data ("any information", "relating to", "identified or identifiable" and "natural person") see Article 29 Working Party below.[20]

The general Directive applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data that form part of a filing system or are intended to form part of a filing system. It does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and to procession of personal data in the course of an activity that falls outside the scope of Community law, such as operations concerning public security, defence or State security.
In summary, in a generic biometric system, processes can be broken down in five groupings: data collection, transmission, signal or image processing, matching decision, storage.[21] Therefore, in the meaning of the Directive, all these five processes in biometric systems should be considered as processing of data.

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down rights for the person, whose data is processed, and guidelines and duties for the controller,[22] or processor[23] determining when this processing is lawful. The rights, duties and guidelines relate to: data quality; making data processing legitimate; special categories of processing; information to be given to the data subject; the data subject's right of access to data; the data subject's right to object to data processing; confidentiality and security of processing; notification of processing to a supervisory authority.

With the adoption of the Directive, the biggest breakthrough was its scope. The Directive brings electronic visual and auditive processing systems explicitly under its scope. The preamble says "*Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques uses to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data*".[24] Processing of sound and visual data is thus considered as an action on which the Directive is applicable. *Processing* is very broad: it can be automatic or manual and can consist of one

template or only partially processed by an algorithm; the stored image or record or template; any accompanying data collected at the time of the enrolment; the image or record captured from the sensor during normal operation of the biometric; any transmitted form or image or record at verification or identification; the template obtained from the storage device; any accompanying data obtained at the time of verification or identification; the result of the matching process when linked to particular actions or transmissions; any updating of the template in response to the identification or verification.

[20] And World Data Protection report 2007, p 26 and for specifics on biometrics: Albrecht, 2003, p16.

[21] Albrecht, 2003, p 13.

[22] Directive 95/46/EC, Article 2(d): "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

[23] Directive 95/46/EC, Article 2(e): " 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

[24] Directive 95/46/EC, Preamble, § 14.

of the following operations: collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission and so forth. The sheer fact of collecting visual (for example face scan) or sound data can be considered as *processing.*

The Directive contains a detailed set of rules for transfers of personal data from a Member State to a third country. These transfers are authorised when the country in question has an 'adequate level of protection'. However, they may not be made to a third country, which does not ensure this level of protection, except in the cases of the derogation listed.

Without going into too much detail, we will make a quick scan of the provisions of the Directive in relation to biometrics.[25]

Article 2 (e) of the Directive defines the controller and the processor of data. In this meaning the data controller or processor of biometric data will be the operator who runs the system in most cases. The instances were consent is necessary are stipulated in Article 7 (a). Article 8 (2) states a general prohibition of processing of sensitive data to which some exemptions apply. In general, processing of sensitive biometric information (relating to ethnic origin for example) will need the explicit consent of the data subject. Sensitive data in terms of biometrics can include medical, ethnic/racial, behavioural information, or data concerning sex life. Article 6 (d) states that data must be accurate and, where necessary, kept up to date. In terms of biometrics, this imposes the obligation to use only such biometric systems that have low false match rates so that there is only a small likely hood of processing incorrect data. Article 20 states that the Member states shall determine processing operations likely to present specific risks to the freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. An assessment of risks created by biometrics is subject to interpretation by member states. The margin of interpretation regarding this provision has turned out to be wide. Whilst the French authorities regard every biometric system as presenting potential risks, other national data protection authorities have come to different conclusions (see below). The Dutch data protection authority has so far not used the power of *prior checking* as given by this provision. Finally, Article 15 (1) lays down the rules on automated decisions on individuals. Central here is the notion of a human intervention before a final decision is taken. Examples of an automated decision using biometrics could include border crossing and immigration processes in the public sector, and biometric processes at the working place in the private sector. In cases where the biometric application is only used to support an authentication process and the legal decision is not based solely on the biometric process, Article 15 ought not to apply to biometric processing.

1.4 The Article 29 Data Protection Working Party

The Article 29 Data Protection Working Party (hereinafter the WP29) is an independent European advisory body whose membership consists of representatives of national supervisory bodies. The statements and opinions of WP29 not only have an impact on national judiciaries but also on the

[25] See also, Hes, 1999, 33-39 and Kindt, 2007.

national supervisory bodies themselves.[26] In fact, one of the core objectives of WP29 as established by the Directive has been to help Europe's data protection practices to move together instead of moving apart. As part of this mission they have undertaken a review of the interpretation of personal data across member states and adopted guidance to help clarify the position.

In August 2003, the WP29 provided specific guidelines for the processing of biometric data in a working document on biometrics.[27] These guidelines are highly relevant for biometric identity management systems in general, whether used in the public sphere or for private commercial purposes. The use of biometrics in applications controlled by governments, such as in passports, travel documents and ID cards and in large scale databases such as a Visa Information System (VIS) and the second generation Schengen Information System (SIS II), has been the subject of intense scrutiny after several opinions of the WP29 pointed to the risks of the implementation of biometrics in these applications in its current form.[28] WP29 has further reflected on the meaning of biometric data in an opinion on the concept of personal data.[29] In this opinion, the functionality of biometric data to establish a link with an individual and to function as identifier was stressed. The working party therefore just ran short of regarding biometric data as sensitive data under the directive. The advantages offered by using biometrics as a key identifier are contested. As all biometric applications and especially large scale systems are still in the roll out phase, many technical experts find it a dangerous strategy to place complete reliance on the security and reliability of biometrics as a key identifier.[30]

1.5 Data Protection Agencies

The national Data Protection Agencies (the DPAs) have all embarked on the task of the interpretation of the data protection legislation applied to biometrics for use in the private sector. In most countries national data protection legislation based on the Directive does not explicitly mention biometrics. In the majority of cases, DPAs have reviewed the processing of biometric data upon request for a preliminary opinion by the data controller or upon notification of the processing. In France, it has become mandatory since 2004 for controllers to request such opinion. The controller needs this opinion, in fact an authorization, before the start of the processing of biometric data.[31] France is hereby one of the few countries that has acted proactively to the emerging trend of the use of biometric data by imposing such prior authorization.[32] This has created an enormous workload for the CNIL, resulting in the creation of the concept of 'unique authorisations' to help ease the task in 2006.

[26] Gonzalez Fuster and Gutwirth, 2008, pp 23-24.
[27] See for the application of the Directive 95/46/EC to biometrics and the guidelines of the Article 29 Working Party', and Gasson 2007 (last accessed 28 September 2008).
[28] For an overview and discussion of these opinions, see above and also Hert et al 2007, part 1. The criticism can be brought back to the simple rules: *do not use central databases where not required and give users control over their personal data.* For an opposite opinion based on a higher emphasis on the prevention of identity fraud see: Grijpink, 2008.
[29] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 26 p. see also World Data Protection report Vol 7, no 8, 2007, p26.
[30] Hert and Sprokkereef, 2007; Grijpink, 2008; www.fidis.net.
[31] Later on, in 2006, the CNIL has issued some 'unique authorizations' which permit controllers, if they comply with all requirements, to file a declaration of conformity.
[32] See Chapter 3, 22nd Annual Report for 2001 of the CNIL, 2002.

The CNIL is not unique in being too understaffed a data protection authority to be able to carry out its tasks.[33]

The DPAs have many more competences to exercise. These competences include, according to the Directive, endowment with investigative powers, such as access to the (biometric) data processed by a controller and powers to collect all the information necessary. In addition, powers of intervention, including the competence to order the erasure of data or imposing temporary or definitive bans on the use of (biometric) data, and the power to engage in legal proceedings against controllers if they do not respect the data protection provisions.[34] The DPAs can also hear claims of individuals who state that their rights and freedoms with regard to the processing of personal data have been infringed or hear claims of organisations representing such individuals.[35] Appeals against the decisions of the DPAs are in principle possible before the national courts of the country where the DPA is established. Appeals should conform to the existing procedure for appeal against such (administrative) decisions. In the United Kingdom, for example, the 'Information Tribunal' has been set up (formerly the 'Data Protection Tribunal') to determine appeals against notices and decisions served by the Information Commissioner.[36]

In practice, Member States, and more in particular the national DPAs, have a considerable large margin of interpretation in deciding whether specific biometric systems are in conformity with the legal provisions of their countries, or not. The decisions of the DPAs on the use of biometrics relate primarily to the situations where the controller has requested a preliminary opinion on the deployment of a biometric application.

The margin of interpretation for the DPAs is thus considerable, and may even lead to conflicting opinions in different Member States on very similar biometric applications. Hence, the DPAs applying the general national data protection laws in their member state use different national criteria which results in diverging views.

1.6 The Dutch Data Protection Authority (DPA)

In the Netherlands, the general data protection law of 2000, as modified, (hereinafter the 'Data Protection Act') is in principle applicable to the collection and processing of biometric data. The Data Protection Act, however, does not contain specific provisions that mention biometric data as such.

In contrast to France (see above), in the Netherlands it is not mandatory to request an opinion on the processing of biometric data. Normally, an administrative check apart, the DPA does not take further

[33] See for example: Mr R. Thomas, The UK Information Commissioner: on funding in evidence to the House of Commons Justice Committee on the Protection of Personal Data Report, H of C Justice Committee report: Protection of private data, HC 154 Jan 08, 12.

[34] See Article 28.3 of Privacy Directive 95/46/EC ; The DPAs, however, are often confronted with too limited resources to engage in these tasks, especially for biometric identity management systems, which deployment has considerably increased in 2006 and 2007. See in this context, the press release of the French DPA of 1 June 2007, available at http://www.cnil.fr/index.php?id=2230&news[uid]=470&cHash=7cc69e6c38.

[35] An example of an organization active in the European Union that could possibly represent individuals which have a claim that their rights under the data protection legislation are breached, is Privacy International. Privacy International is a human rights group, established in 1990, which conducts research and informs the public on privacy invasions by governments and businesses. Their website is http://www.privacyinternational.org.

[36] For details of how the Tribunal is re-writing the definition of personal data and privacy in the UK see: Turle, 2007, p11-18.

steps after it receives a notification of the processing of biometric data. [37] A notification of the use of a biometric application with DPA is thus all that is required to get a new biometric application going. Formally, a notification to the data protection authority does not imply a formal 'go'. On the contrary, the notification allows the authority to react is this is needed. In practice, and due to staff constraints, this seldom happens. It is also not required that the processor or controller waits for a 'green light'. The controller can start the processing straight after notification.

The DPA has been very active on the issue of biometrics. In 1999, it already proactively published an extensive report on the privacy aspects of biometrics.[38] It was the result of a study performed jointly by the DPA and the Netherlands Organization for Applied Research- Physics and Electronics Laboratory (TNO-FEL). The report concluded that designers, developers, suppliers and users of products using biometrics for identification, authentication, or exposure of emotions needed to consider ways to protect the privacy of users. The report also provided a checklist with practical directions, for those who want to build a privacy-enhanced product that processes biometrical data. It stated that personal data should be protected with proper PET[39] and referred to crucial decisions in the design phase. In particular, to decisions concerning the question whether to protect data by decentralisation of the template storage and/or verification, or encryption.[40] In the next section of this report, the options for using biometrics as a privacy enhancing technology will be discussed. Here it suffices to observe that the Dutch DPA produced a detailed report in a very early phase, a report that was authoritative and contained conclusions, practical directions and recommendations. To date, it has not been followed up by more detailed guidelines or descriptions of best practice.

The role of the DPA in practice has been to receive notifications, make an administrative check on them and place all notifications on a register accessible through its website.[41] A few organisations have asked the DPA to issue a preliminary opinion, and it has done so. Whilst the 1999 report was very proactive, since then the Dutch DPA activities have been of a more responsive nature. Concerning the semi public or private use of biometric applications, the main supervisory activity of the DPA has been the publication of three preliminary opinions. The first we will discuss is the opinion relating to an access control system through a biometric disco pass. The second is the DPA opinion given on the bill changing the passport legislation in order to introduce biometrics in 2001.[42] The third is a 2003 opinion on the use of face recognition and the use of biometrics for access control to public events, combined with use for police investigations that will not be further discussed here.[43]

In 2001, a producer requested an opinion from the DPA on an access control system named 'VIS 2000' with biometrics intended for use by restaurant owners, sport centres, and similar clubs or

[37] The Dutch Data Protection Authority is the CBP (College Bescherming Persoonsgegevens). See also Hert and Sprokkereef (2008).
[38] Hes et al, 1999.
[39] The report identifies PETs as: different technological elements that can help to improve privacy compliance of systems (p 49).
[40] See pp 58-59 of the report (Hes, 1999).
[41] See www.cbp.nl.
[42] CBP, Wijziging Paspoortwet z2001-1368 (invoering biometrie), 16 October 2001.
[43] CBP, Vragen over de inzet gezichtsherkenning z2003-1529, 3 February 2004.

establishments.[44] The system allowed access control, served marketing and management purposes and keeping a 'black list' of customers who had violated the rules. The VIS 2000 stored the templates of the fingerprint and the face. The templates of the face were stored in a central database, combined with the membership card number and a code for the 'violation of club rules'. The card number would be linked to the personal details of the visitor/members communicated now of the issuance of the card. The biometric data would also be stored on a smart card, and used for membership verification when entering the club. Whilst a person entered the premises, the system performed a check against the black list of banned persons, one of the main purposes of VIS 2000. The biometrics were hence used for the purposes of verification (1:1 check, comparing whether the holders of the membership cards were the owners of the card) and of identification (1:N check, comparing whether the holders were registered on the black list of VIS 2000). In case of incidents, violators could be identified by their biometric characteristics. This involved reverse engineering of the stored templates of the face to images, comparing the images with the images of the violators taken by surveillance camera's, and connecting the templates with the name, address and domicile data if a membership card had been issued. The purposes of VIS 2000 were named as to increase the security of the other visitors and employees at the clubs, to maintain order and to refuse access to unwanted visitors.

The DPA stated in its opinion that the use of biometric data for access control purposes is far-reaching and that it should be evaluated whether the use of biometric data is *in proportion with this purpose*. To this end, the DPA checked the collection and use of the biometric data against several obligations of the Data Protection Act. However, it did not report on investigating whether there were other, less intrusive means to maintain order and to refuse black list individuals to the club at their next visit without storing biometrics in a central database.[45] In this opinion, the DPA explicitly recognizes the possibility of the algorithm used to reconstruct the face of the original scanned facial image from the template. This reverse engineering of the templates was one of the main functionalities of VIS 2000 to identify violators of the rules of the establishments using the system. This technical feature, however, has important consequences. First, it should be noted that the face scan might well contain information about race, which shall not be processed in principle. The Dutch Data Protection Act contains an explicit exception to this prohibition of processing of this information, in particular, when such processing is used for the identification of the person and to the extent such is necessary for this purpose. The DPA considered it inevitable that use is made of templates of the face (containing information about race) for the identification of troublemakers.[46] The DPA continued that the use of personal data for marketing purposes should not include biometric data and that the processing for this purpose should be separated from the other purposes. The DPA concludes its opinion with several recommendations, including with regard to the term of storage and security (requirement for encryption of the templates and membership card numbers) and for the operation of the biometric

[44] Registratiekamer, Biometrisch toegangscontrole systeem (discopas), 19 March 2001. www.cpbweb.nl (last accessed 28 September 2008).

[45] For example, the simple confiscation of the membership card of the person concerned in combination with checking new applications against a central list of suspended individuals. See also, FIDIS deliverable *D3.10 Biometrics in Identity Management,* E. Kindt and L. Müller(eds), www.fidis.net (last accessed on 28 september 2008)

[46] As stated above, the DPA *did not make a proportionality test about the use of biometric data*, and the opinion therefore indicates that a necessity test to use information about race should be regarded as sufficient for the purpose of determining.

system. The DPA also requested that any systems already installed would comply with these requirements.

The divergence of the outcome of this opinion of the Dutch DPA is interesting as compared with the evaluation, comments and conclusion of the Belgian DPA with regard to a similar system. The Belgian DPA reported in its annual report of 2005 that it rendered a negative opinion on a similar system. It considered the use of biometric characteristics for access control for a dancing club not proportionate with such purpose. More particular, the Belgian DPA found the use of biometrics for identification purposes disproportionate and entailing risks for the privacy of the visitors.

Several EU member states planned or started to issue biometric passports in furtherance of the Council Regulation (EC) No 2252/2004 of 13 December 2004.[47] The regulations and the legal aspects of the use of biometrics in ID documents and passports have been analyzed in detail in FIDIS deliverable 3.6. 'Study on ID Documents' of 2006.[48] On 19th September 2001, the Dutch Home Office Minister requested the DPA's advice on some new paragraphs proposed to Article 3 of the passport law. [49] On examination of the provisions the DPA concludes that the law would allow biometric data to be stored in the travel document administration of the appropriate authorities. The DPA points out that it does not find enough arguments to support the necessity of measure. On the basis of the current arguments the DPA rejected the need for such a measure, it also stated that even if these grounds were to be put forward, than the passport law would still need to be based on the purpose limitation principle, whilst in the current wording the purpose was open ended. In a second advice of 30 March 2007, this argument was repeated, and the DPA argued against (de-)central storage, warning for the effect of 'function creep'.[50] It should be noted here databases are not necessary for passport control procedures as the data are to be matched against the reference data on the chip in the passport. It is clear that central databases may prevent citizens from obtaining several identity documents in different names. At the same time, the question is then whether this aim cannot be achieved with other means rather than with the privacy invasive and security sensitive creation of a central, or decentralized, database. A strong opponent of this view is Grijpink who argues that decentralized storage of three (in stead of two) finger prints in the local data base of a Dutch municipality is a very powerful way to prevent large scale identity fraud with biometrics in passports[51]. An illustration that a different approach can be taken is to be found in Germany. In the Federal Republic in contrast, no further purposes beyond those specified in the Regulation are foreseen by the National Passport Act.[52] There are authorizations for respective police, customs, passport and registration authorities, but the new Sec. 16a of the Act states that the use of biometric data shall be absolutely restricted to the verification of the authenticity of the document and the identity of the holder.[53] The National Passport Act expressly outlaws a central database and it will not be permitted to search the data for one specific face. The German approach sounds very privacy protective in the first instance, but it is

[47] Council Regulation (EC) No 2252/2004 of 13 December 2004 for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 385, 29 December 2004.
[48] See www.fidis.net (last accessed 28 September 2008). For a very good analysis: Hornung, 2007.
[49] CBP, Wijziging Paspoortwet z2001-1368 (invoering biometrie), 16 oktober 2001
[50] CBP, Wijziging Paspoortwet advies z2007-00010 (invoering biometrie), 30 maart 2007, 5.
[51] Grijpink 2001 and 2008.
[52] Hornung, 2007-b, p 182.
[53] See Hornung, 2007-a, p257.

extremely privacy invading once an individual's biometrics fall in the wrong hands. Then the system will not be able to prove that the finger scans do not match with the original finger scan and an individual can become faced with the permanent privacy invasion of being the victim of identity fraud. In the absence of a database, the biometrics of an individual who claims to be the victim of identity fraud cannot be checked against original finger scans stored and the perpetrator can easily go undetected. In the case of small scale, private or semi public applications, this argument does not hold, because the impact is not so profound and proportionality becomes a more important issue.

1. 7 Some Observations

There is general agreement that it follows from the European Directive that in most cases[54] the processing of biometric data falls within its scope. However, national differences have occurred in the transposition and interpretation of the general provisions of the Directive. One of the reasons for this is that there is no specific mention of biometric data in the text of the Directive itself. In the Netherlands, no prior authorisation is needed to start using a biometric application. Powers of intervention and the powers to engage in legal procedures against data controllers have hardly been used. The few decisions of the Dutch DPA on the use of biometrics relate to situations where a controller has requested a preliminary opinion on the deployment of a biometric application. Here we see that the proportionality of the measure is not dealt with in the same fashion by other DPAs.

The political debate about the issue whether the biometrics contained in European passports should also be stored on a central database shows that interpretation of the proportionality principle is interpreted differently, depending on national, legal and cultural context. Within the Netherlands itself, the decision-making process surrounding the storing of biometric data of Dutch citizens shows that there is disagreement. What is proportional and how to define the purpose specification of the use of biometric data id interpreted differently by the Dutch DPA and the Government. As an application in the public sector the biometric passport falls outside the scope of this report, however, it the example shows that there can be substantial variations in how the European Directive can be interpreted and/or integrated into the national legal framework. These differences will also show in how national DPAs deal with biometric applications in the semi-public and private sector.

Conclusions and recommendations following from this analysis and the following two chapters can be found at the end of the report. It is now useful to return to the original questions at the beginning of this section. These were concerned with confidentiality, purpose specification, proportionality and individual participation. We will carry the questions on protection of biometric data, sufficient protection against unauthorised use, proportionality between the collection of biometric data and the purpose for which they are collected and maximisation of individual participation to a more technical level. What are the possibilities for biometrics to be used as a privacy enhancing technology? What are the options to maximise the level of privacy of the individual whose biometrics are used? We will first deal with theory in section two and then turn to biometric practice in the Netherlands.

[54] The only exception being the processing of data as a purely personal activity.

Chapter 2 The Privacy Risks of Biometric Data Processing

2.1 Introduction

The use of biometric technologies involves the collection of unique biological and/or behavioural characteristics of a person. Handling or storing these biometric characteristics can produce an invasion of privacy in a variety of ways. The potential (negative) impact of a privacy invasion has to be weighted against the advantages of the use of the biometric application. Thus, factors such as convenience, security and privacy are balanced against each other in the decision-making processes regarding the introduction of the various applications. This is not easy. The concept of privacy in itself already poses some challenges such as what are its boundaries, its core characteristics and how can we determine the economic value of protecting privacy. Chapter one has shown that the privacy risks involved in the handling of biometric data by individuals and institutions can be defined and assessed in legal terms. They can also be considered in a wider societal context of changing perceptions on identity and privacy[55] or in economical terms such as assessing the financial advantages of privacy protection for private business.

This analysis of the use of biometrics as a privacy enhancing technology is of course an integral part of the wider discussion on privacy enhancing technologies (PETs). We will therefore start with a short analysis of general trends and technologies. As this research project focuses on the private sector, it is also good to take note of some recent research on the use of PETs in business. Within the European PRIME[56] research project, some interesting work has been done on the business case for PET.[57] After four years of research the group concluded that "we still face major obstacles towards a deployment of PET technology at a large scale (...) the part of convincing business to design their business processes in a way such that data minimization can be implemented as envisaged in PRIME will even be harder than has been the technological part".[58] PRIME reports that the central question often is: how much would lack of privacy costs my business? The benefits of investments in PETs are often long term and cannot be presented other than as uncertain. Many companies have never (consciously) experienced a serious privacy breach, and when they have, find it often very difficult to quantify the costs, including the longer term consequences in terms of reputation and so forth.

2.2 Trends and Technologies

Before turning to the concept of PET, a brief description of some general trends in relation to new technologies helps to set the scene. The increased use of biometrics in all kind of settings clearly does not develop in a vacuum. Technological advances in biometric technology open up possibilities, and these are taken up based on a supply and demand that is the result of political and societal developments. The latter affect the introduction of the technology in a range of different settings. Some of the current and relevant trends that can be identified are:

[55] For more details, see the work of FIDIS: www.fidis.net.
[56] PRIME (Privacy and Identity Management in Europe): www. prime.net.
[57] Borking, 2008a.
[58] Camenish et all, 2008, p 127.

- The increasing volume of data that is gathered, processed and exchanged
- Linking of data banks and data sets both by government agencies and by commercial parties
- Increased tendency to keep data on file for possible future use (rather than discard data)
- Development towards more transparency and accountability: open access to documents and data
- Mounting pressure on individuals to disclose personal information and allow data linkage both by government agencies and by business organisations (the latter mainly through internet)
- Growth in the types of hardware that hold large data sets (cd roms, usb sticks, small gadgets and portable computers, data holding phones and so forth:) and pose new security risks.

Biometric applications are seen as useful tools that can play a role in the new systems of data management that result from these trends. In general, expectations placed on biometrics in the short term seem to be high. On the contrary, the expectations of the impact and precise role of biometrics in the long term appear rather vague and not very well documented. To put an image to it: biometrics is the road that we are building whilst we are walking it, and we have no idea where it will take us. [59] As biometric technology is in the roll out phase,[60] the high expectations in the short term will probably be adjusted rather sooner than later.[61]

2.3 The Concept of PET (Privacy Enhancing Technology)

The starting point in thinking about technology and privacy should always be that technology is not privacy neutral per se. Rules for handling information can be enforced, or enhanced, but also be made difficult, be evaded and so forth with technology. In general and without intervention, information sharing and monitoring tend to be promoted more by technology than information shielding. In practice, as a particular information technology evolves, take the development of the internet for example, gradual adaption to possibilities takes place. This then often results in a downgrading of the reasonable expectation of privacy.

At the same time, the desire to shield information may grow once the impact of the new technology on the privacy of individuals or certain groups becomes apparent. The balance that will then have to be found is between the interests of the individual to have control over his/her personal data and a series of other interests such as economic interests, policy/societal interests: security, freedom and so forth. All these have their bearing on the use of biometrics and the relationship with existing data protection legislation.

The combination of the concept of PET (privacy enhancing technology) and the use of biometrics (physical characteristics by which a person can be uniquely identified) could be regarded as a contradiction in terms. When one accepts the notion that a person's biological characteristics form the

[59] This applies arguably to Dutch government policy but certainly, and this is well documented, to EU policies on biometrics. Hornung, 2005.
[60] EBF, 2007.
[61] See Brussee, 2008.

core of a person's fundamental privacy[62] than any use of physical characteristics is privacy invading. In this view, technical measures can at most have a privacy damage limitation capacity but can never have privacy enhancing qualities. Similarly, the concept of PET in combination with the use of biometrics can be regarded as a contradiction in terms from the point of view of public policy and security objectives. In this view, the desirability of the introduction of PETs as tools controlling individual biometric information should be challenged as these PETs are fundamentally at tenterhooks with the use of biometrics as an efficient instrument of public and security policy. Perfect PETs may for example lead to technical and/or security inadequacies and prevent the straightforward track down of terrorists or fraudsters.

Here, however, the point of departure is that the use of physical characteristics in combination with computer systems is in itself not necessarily privacy invading as long as the system offers adequate protection against unjustified or disproportional use of these data. As biometrics are unique and cannot be replaced, unjustified or disproportional use of data as well as theft of biometric data in the private and semi public domain will have a negative effect on the roll out of biometrics in the public domain and *vice versa*. In this context, a relevant question is whether PET is a concept that is taken seriously in the use of biometrics in the private and semi-public domain in the Netherlands. We use the term PET here referring to "a variety of technologies that protect personal privacy by minimizing or eliminating the collection and/or handling of identifiable biometric data".

The above definition can only become practically relevant once the concept of privacy has also been defined.[63] Here it needs to be noted that protecting personal privacy is more than protecting personal identity. The literature on PETs as anonymisation tools on the internet is a good classical example of this. The PET 'encryption' was originally used to protect the content of messages, not the identity of the sender or receiver. The privacy enhancing capacity of the tool was not to anonymise (personal) details of the sender but to make the exchange of information that was taken place invisible for third parties. Another aspect of safeguarding personal privacy is that it covers more than just safeguarding personal information. Safeguarding personal privacy needs to include safeguarding the quality of the information, or the right to correct and/or amend.

The most important distinction always made is that between the goals of identification and verification. This distinction separates biometric systems aimed at bringing about automated identification of a particular person and those aimed at verification of a claim made by a person who presents him or herself. As the identification function requires a one to many comparison whilst the verification function requires a one to one comparison, privacy risks involved in the use of the biometric technology vary considerably from application to application. In principle, the verification function permits the biometric characteristic to be stored locally, even under the full control of the individual, so that the risk that the biometric data are used for other purposes is limited. This does not mean that all biometric systems that could be restricted to serving the verification function have actually been designed to maximise the control of the individual over his or her biological data. From the preliminary inventory made in the

[62] Compare: Van der Ploeg, 1999, 2002 and Alterman, 2002.
[63] Bos, 2006

context of this research, it becomes clear that most biometric applications used in the semi private domain in the Netherlands have been introduced for verification purposes (mainly to grant authorised persons access to physical or digital spaces). Control over personal data in these situations needs to be clarified, and the legal conditions determining the handling of data as well as the enforcement of applicable law are issues that need scrutiny.

The usefulness of the notion of control over biometric data when assessing privacy will be discussed below. What suffices here is to establish that the identification function cannot be performed without the use of a (central or de-centralized) database. Therefore, in the case of biometric identification procedures, privacy-enhancing measures automatically concern the protection of biometric data that no longer are under the strict and full control of the individual. The way in which data are stored centrally of course matters in terms of privacy protection. The use of biometric encryption in combination with the use of a "protected safe" that is only accessible to a small number of people, greatly enhances the privacy protection of individuals enrolled in a system with central storage. The biometric applications using these techniques are still in development or in the early phases of roll out.[64]

It is also important to make a distinction between the protection of biometric data stored within systems and the use of biometrics by operators to safeguard authorised access to other type of data stored in a system. This distinction can be clarified by labelling measures ex-ante and ex-post. Where PET is used as an integrated design into the system, and the owner of the system is responsible for its proper implementation and functioning, PETs can be used as controls. Ex post measures are controls, put in place to check whether the data are effectively protected (biometric operator access to a data bank). To meet high security standards the use of a biometric as an ex post measure should be made in a multi dimensional or multi factor authentication situation (for example the combined used of a biometric and an employee number or even password).

PETs can also be used as a flexible instrument in the hands of a person making use of a system providing this individual with personal and self-determined control over their sensitive information. In the management of privacy, this individual control can take three forms: choice, consent and correction. We can label these as ex ante measures. Ex ante measures create an environment in which data are protected, and the individual can prevent that data are used in a certain way. The most far reaching form of ex ante measures relating to biometrics is the sensor on card system where biometrics encapsulated in a personal device that do not leave this device. [65]

In assessing the exact meaning of the label 'privacy enhancing technology', it is useful to make the distinction between the concept of privacy and justification and the management of privacy. This distinction has first been developed by Tavani and Moore (2001).

[64] See Cavoukian, 2007 and also: Tuijls, 2007.
[65] In a sensor on card system not only the data but alsdo the sensor reading the data is on the card. The second most far measures is the match on card, here the data do not leave the card either but the sensor reading the data is external, and therefore located outside the personal device/or card. See Hornung and also below.

They define the concept of privacy in terms of the protection from intrusion and information gathering. The very absolute objective of privacy enhancing technology would be the simple goal that as little information as possible is gathered, used or stored. Adhering to this concept of privacy results in a strict separation of the use of biometrics in commercial transactions, administrative purposes and law enforcement (sectoral boundaries). An example would be the German decision to refrain from creating databases of the biometric data contained in German passports. In the previous chapter, it has been shown that this might tilt the balance between security and privacy towards the latter in the short term. At the same time in the long term it might create extraordinary problems in the detection of identity theft resulting in individuals experiencing massive invasions of their criminal record protection, and financial and identity privacy.
The concept of control is applied to the use of measures that provide privacy protection and general management of privacy on aspects such as quality of the information, right to correct and so forth. The use of biometric as PET control allows an individual a say in the trade of between privacy and security in any particular circumstance.

2.4 Choice, Consent and Correction

In this project, we have mainly looked at biometric applications used in the private or semi-public domain. Of course, an important element for an assessment of privacy friendliness in the use of biometrics is whether providing biometric samples is obligatory or voluntary for the individual concerned. Of course, by nature applications in the private or semi-public domain are used on a voluntary basis. This means that the individuals asked to provide their characteristic could refuse this and use another facility, for example another swimming pool not using a biometric entry system or the individual can make use of a similar service without the biometric at the same institution (for example voice recognition when managing your bank account). When there is an alternative way to obtain the services offered then the element of choice, consent and control is in the hand of the individual. Here information is a key factor. The users of biometric systems often fail to realise the implications of offering their characteristics for storage on a database, and the loss of individual control over their characteristics once this has happened. Rights, such as the right to correct, are seldom exercised and other ex ante measures remain unused.

When there is no alternative available, and this is the case with most public sector introductions of biometrics such as the biometric passport, the biometric characteristic has to be presented. As the whole point of these systems is to identify individuals and link them to existing data, the use of a database and the possibility to link databases seems unavoidable. Storage of the raw template only occurs in very basic biometric systems the handling of raw data will soon become a relic of the past. New exciting technology have been developed both to improve the possibilities created by encryption and in overcoming the problems of false positives because of noise.[66]

[66] Dutch research and development has been at the forefront of these developments. See for example: www.priv-ID.com.

To integrate PET into the design of the biometrical systems there are two ways: decentralisation of the template storage and verification and/or encryption of template-databases (in case of central storage). By decentralisation of both the template storage and verification process, the biometrical data are processed in an environment controlled by the individual or an environment from which no connection to a central database can be made. In case of central template storage and verification, mathematical manipulation (encryption algorithms or hash-function) can ensure encryption of databases so that it is not possible to relate the biometric data to other data stored in different databases, at different locations.[67] In the case of EURODAC, the PET aspect is the HIT-No HIT facility in the first instance, but of course in the case of a HIT, biometrics are de-encrypted so that they can lead back to the other personal details of the person involved. It has to be noted here that access to EURODAC data by law enforcement agencies such as Europol, also applies to those fingerprints that were provided by those seeking political asylum in the EU before this permission was granted. This is an example of biometric identifier function creep that has been commented on extensively (Standing Committee, 2007). Under Dutch criminal law, also controllers of private applications that store biometric characteristics can be forced to

2.5 Function Creep

Most literature on the European wide introduction of biometric technologies in the public sector clearly agrees on one conclusion: the core problem is that government demand is focusing on surveillance, control and fraud detection instead of on security and risk mitigation. The consensus is that in the public sector, function creep is a logical development when the emphasis is on surveillance and control and therefore on tracking, identifying and controlling individuals. This poses the question whether it is useful to consider PET possibilities of biometric technology as in public information management and law enforcement linking of data will be such an obvious policy goal. IT PET tools such as database privacy gauging, proxies, sticky e-privacy constraints, automatic privacy detection software or even de-identification systems such as anonymisation routines seem to fit in badly with the trends described in section 2.2 above.

Thus, in the absence of a longer term design for the management of information, it is safe to assume that the proliferation of biometrics makes individual biometric data more accessible. It also makes the biometric data more linkable to other personal data, thus making the technology privacy invasive per se. Instances of function creep, such as the use of biometric data collected for immigration purposes used in the context of unrelated criminal investigations[68], might occur in the private sector also. To give examples: biometric applications first introduced with the purpose of fast and efficient entry of employees or customers can be used for time registration or customer profiling at a later stage. Here

[67] The Canadian data commissioner Cavoukian is one of the most pronounced advocates of the use of encryption: see Cavoukian, (2007) who concludes: "While introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns. However, novel biometric encryption techniques have been developed that can overcome many, if not most, of those risks and vulnerabilities, resulting in a win-win, positive-sum scenario. One can only hope that the biometric portion of such systems is done well, and preferably not modelled on a zero-sum paradigm, where there will always be a winner and a loser. A positive-sum model, in the form of biometric encryption, presents distinct advantages to both security AND privacy" (p 31 of the report) " But see also: Tuijls, 2007.

[68] See: an interesting ruling on the use of databases of 18th December 2008: http://www.statewatch.org/news/2008/dec/ecj-databases-huber.pdf

the information given to customers and legal rights to be informed and the right to correct come into play. In addition, some paradigm shifts that are beneficial to privacy protection can also be observed. The most notable is the change in the technology used for access control of the European passport, from the right to access: basic access control (unencrypted face stored) to the privilege to inspect: extended access control (encrypted fingerprint images). This has made skimming of passport details more difficult and has enhanced the privacy of the passport holder compared to the past. To conclude: function creep (as a process by which data are used for different purposes than originally collected for) is a trend that is strengthened by the information exchange interface between new technologies and ICT. This combination has an attraction difficult to resist. The tendency to use data for other purposes than originally collected for[69] can be observed in the public, but also in the semi-public and private domain.

2.6 Using Biometrics as PETs

Based on the literature[70] we will detail some basic notions of what constitute privacy enhancing and potential privacy invasive features of biometric applications.

The one-off use of fingerprints in medical screening is a biometric application that enhances privacy. This makes having to use patient names to match with their diagnostic results unnecessary. There is a double advantage to the one off use of biometrics in this instance: patients can remain anonymous and there is greater reassurance that data are released to the correct person. Another obvious example is the ex post measure already mentioned ***biometric*** authentication to restrict operator use in a database. This use of biometrics makes operators more accountable for any use/misuse of data. A more generic example is the match on card-sensor on card: biometric authentication without the biometric characteristics leaving devices owned by the individual.[71] Biometric cryptography is a privacy enhancing technical solution that integrates an individual's biometric characteristics in a revocable or non-revocable cryptographic key. This method now forms an integral part of all but the cheapest biometric applications on the commercial market. When the key is revocable, this introduces issues relating to function creep and law enforcement. At the same time, there are possibilities for a three-way check to come to an architectural design that restricts the number of people having access to data**.** Than there are applications that offer two-way verification and therefore integrate the "trust and verify" security principle.[72] Another PET possibility would lie in the certification of the privacy compliance of biometrical identification products; this is therefore not a PET but a certification of the biometric application as a PET.

When we concentrate on biometrics as a privacy invading technology an obvious example would be the storage if information in a manner where medical or racial information can be inferred. Equally intrusive is the use of an individual's biometric data to link their pseudonimity/identity between different

[69] Opening up the EURODAC site to police and other law enforcement agencies is the most striking European example of this.

[70] We refer to Hes et all, 1999; BECTA Guidance, 2007; Registratiekamer, 2000; Ministerie van Binnenlandse Zaken, 2004; Andronikou, 2007; Wright, 2007; Grijpink, 2001)

[71] This type of biometric application has been recommended by the FIIDIS consortium: see www.fidis.net deliverable 3.14. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.10.biometrics_in_identity_management.pdf

[72] Many of these privacy-enhancing possibilities were already mentioned in the groundbreaking 1999 study on biometrics by the Registratie Kamer, Hes et al, pp 49-70.

applications/databases. Another example is the use of biometrics for surveillance, where no permission is asked to take (moving) images of people for example of face recognition systems. There are examples abroad but there have also been experiments of this kind in Utrecht and Amsterdam.[73] Then there is central storage of raw biometric data, central storage of biometric templates and so forth aimed at identification, these result, depending on the specifications of the system in possibilities of covert identification systems. Then there are biometric systems aiming for interoperability, maybe even using a biometric as a unique identifiable key (instead of another personal detail such as the name (alphabetical identifier) or a number (numerical identifier). These systems are built on as much identifiabilitiy (thus privacy intrusion) as possible and link data that would otherwise go unconnected. Also very privacy intrusive is a privacy invading choice for biometric identification. To be more precise: the use of a biometric system for identification, where verification would already have met the objectives of the application.

2.7 Some Observations

Privacy enhancing technologies refer to a variety of technologies that protect personal privacy by minimizing or eliminating the collection of identifiable data. PETs can help to give individuals as much control as possible over the processing of their data. PET is broader than just the protection of information, as it also concerns technological possibilities to improve the quality of the information and the technological possibilities to access and correct personal information. The use of biometrics as PET will always have to be balanced against the need to provide security for society but also for the individual concerned. Too much PET may cause an individual another type of invasion of privacy in the long term because he or she cannot be protected against the negative effects of identity fraud. PETs are only useful when integrated into security of system. Using revocable cryptography to store biometric data but leaving access to the database unsecured would be potentially privacy invasive. Management and control of personal data does not stand or fall with using biometrics as a PET where possible. Without security of systems, sectoral boundaries, clear objectives, avoidance of function creep, delineation of the target group and external supervision biometric data become vulnerable to abuse independent from technological possibilities to maximise the privacy of the person providing biometric characteristics. It should therefore be clear that the proliferation of biometrics makes individual biometric data more accessible and more linkable to other personal data in principle. Within this principle constraint, the use of biometrics as PET should be stimulated and enforced. For individuals asked to provide biometrics, options in terms of choice, consent and correction need to be clear and accessible. Those buying biometric applications for use in their daily business ought to be made aware of the PET aspects impact on privacy of the applications available. Above, some of the choices affecting privacy re biometric applications have been listed. No comprehensive checklist is available for semi public or private controllers deciding on the use of a biometric application. So how do these controllers deal with biometrics? How concerned about privacy are those who process biometric information in the private and semi-public sector in the Netherlands? In the next chapter, we will look at some of these issues in detail.

[73] See: https://rejo.zenger.nl/vizier/archives/101.

Chapter 3: Small Scale Use of Biometrics in Practice

One of the aims of the research project was to get a better insight into the PET aspects of biometric applications currently in use in the Netherlands. This was to be achieved by drawing up an inventory of small-scale biometric applications in use in the semi public and private sector and analyzing their technical PET aspects and implementation. It proved difficult to obtain this kind of information via open sources and it turned out that similar efforts of listing biometric projects and their characteristics (for example by the Nederlands Biometrie Forum: www.biometrieforum.nl) also showed very little progress. In addition, once found, information proved hard to check. In all, less than a hundred projects were identified, most of them using technology provided by a handful of producers. All applications but about ten, could be labelled private (or to put it differently: members-only) applications. In many cases, the data holders (when contacted by telephone) did not want to participate in the research.

Is it impossible to make a guess how many applications in the semi public sector have gone unnoticed by the project team. It would be very useful to investigate further, why reliable information about biometric applications in use is so difficult to obtain. Possible future research may take notifications to the CBP as a starting point.[74] After obtaining consent, the projects notified could be followed up by site visits. This method would mean that applications that have not been notified would not be included in the research. Although no figures about failure to notify are available, it should be mentioned here that the ICO (Information Commissioner's Office) in the UK works on the assumption that on top of the 300.000 notifications under the Data Protection Act that have been submitted, about 100.000 instances of data processing that should have been reported, is not notified.[75] Overall, it should be concluded that our information position concerning the use of biometric technology in semi public and private sector in the Netherlands remains weak.

In this report, we have therefore chosen to focus on a small number of anonymous case studies that give a range of insights into current practice. Although these case studies are not necessarily representative, they do show which factors play a role in the implementation of biometric applications and in the choice for their technical specifications. The case studies concern:

3.1 a pilot using obligatory finger scans to gain access to a primary school;

3.2 a system already fully rolled out, using finger scans to prevent known offenders from returning to a public swimming pool;

3.3 a pilot of a supermarket chain using finger scans as a method of payment in a supermarket; and

3.4 a sports club using hand geometry as obligatory access method for its members.

[74] http://www.cbpweb.nl/indexen/ind_reg_meldreg.stm

[75] Information obtained during an interview at the ICO in October 2008.

3.1 Case Study Primary School

A biometric applications producer approached this primary school to conduct a test case for the use of finger scans to gain access to the school building. As the school felt it would be useful to have more control over access to the building it took up the offer. A biometric access system was to be made available to school staff and parent helpers, but also to after school club personnel. The system has been made available free, and it will run for a one year trial period. It started to become operational in March 2008.

3.1.1 Technical Specifications

The system consists of two scanners that have been place next to the two entrances to the school building. The finger scan apparatus scans two fingers only. Through an algorithm, the raw data are converted, compared (and stored) templates in a database. When there is a match, and the particular template is allowed access at that time, the door opens. The templates are held in the database, and directly connected to the personal data of members entered in the database. Both the template database and the computerised personal data are stored in the office of the headmaster. The headmaster can programme the system ahead to a maximum of 20 days. This allows him to determine who can enter the building when in this period. It also allows him to check who has come in when. In some ways, the technical limitations of the system make it less user friendly. For example, someone will have to return in the middle of the summer holidays to reset the system. Failure rate was not perceived as an issue. There have been few instances of authorized persons being refused by the system. Whether unauthorized people have been allowed access is not clear. The system is used one factor instead of multiple factor (or multiple authentications). This means that no other instruments of control such additional passwords or tokens are used.

3.1.2 PET Aspects

The users and controllers of the system that were interviewed were not aware of the PET aspects of biometric technology. The minimisation of the collection and use of personal data was not reported as an issue. Nevertheless, when the school organised an information evening, there was concern reported about privacy aspects (this was at least mentioned in the local newspaper). This concern had apparently petered out as once the system was in use, as the headmaster reports there have not been complaints. Surprisingly, the database now holds the fingers data of the pupils too, although this was originally not the intention. The fact that fingerprints of pupils are collected would allow for the use of the system as a register, but it has so far not been used for these purposes. The database is physically at the same location. The personal data of all users as known by the school are linked to the template stored in the database. If this had not been the case, then the possibility to check who had sought access to the school would not have been possible. Those interviewed did not hold the fact that the templates are based on algorithms and not raw images important. It seems in this case, the raw data remain accessible because the algorithm is revocable. This means that in principle, the template can lead back to the raw data.

3.1.3 Other Aspects of the Implementation of this Biometric System

The school has not sought permission from parents to collect biometric data from their children nor from the parents or the staff required to give provide their biometric data. This is technically not required for all processing of data according to the *Wet Persoonsgegevens*. Whilst consent is not required, schools can be expected to involve pupils and their parents in their decisions to use biometric technologies as it would with other decisions made regarding the pupils at the school. In this case, the school has met this requirement because it has organised an information evening on the subject. It seems however, that it was stated at the time that finger scans of pupils would be not be taken.

The maintainer of the database does not have an official policy on deleting data after a certain period, such as deleting the data after pupils have left the school. In line with data protection principles data should be kept no longer than necessary. The impression gained at this school is that the templates based on pupil's biometrics will stay on file after a pupil has left the school. According to the information obtained in the interviews, the application has not been notified to the Dutch data protection authority.

Finally, as stated above the system uses a one-factor authentication. The question that can be asked is whether in a semi public institution such as a school, there should not be a preference for multi dimensional systems to increase individual and system security.

3.1.4 Main Issues Arising from Case Study One

Active Marketing Approach by Industry

This is an interesting case of a supply lead application of a biometric system. The school was approached with the biometric product by its producer and decided it was an interesting option worth trying out. For this reason, it would be relevant to see whether this school will continue to use the system after the trial period, and on which factors any decision will be based.

Lack of Guidelines

From the interviews, it is clear that al participants (school management, School Board, data controller at the school, other parties such as parents) have played the situation by ear. There was no evidence that a clear procedure had been followed to assess technical possibilities (including PETs), legal consequences, social implications and so forth. This case shows clearly that information and guidance is lacking, or does not reach the right audiences. This school would have benefitted from guidelines such as those provided by the UK Information Commissioner (http://www.ico.gov.uk) or BECTA (www.becta.org.uk).

Obligatory participation and Policy Against Theft or Abuse

There is no fall back procedure at the school for staff members, parents or pupils. This means that it is not possible to refuse to provide finger scans. There is no procedure in place for those who refuse to participate. Also at first sight, the data are not kept very secure as data and templates are linked and kept on a PC in the head master's office.

Function Creep

Originally, the idea was to use fingers as key to gain entrance to the building. In that respect only fingers of personnel and helper parents would be scanned. However, soon after implementation started, the decision was made to scan pupils' fingers too. Pupils had never had a key to the school before. The school states that there is no intention of using the system as a register, but the fingers could be used for control purposes. This is simply a matter of possibility creating an action. Again, here, it cannot be predicted whether over time, the fact that the technical possibility is there, will result in a digital register informed based on finger scans or other surveillance type data processing being introduced. As long as this school does not deviate from the use of the biometric data so far, it need not be concerned about the DPA's requirements as laid down in the decision on VIS2000 (Chapter 1). Were the producers to offer a replacement product with more possibilities, the circumstances of the case point towards further function creep. This reinforces the need for detailed guidelines and legal advice.

3.2 Case Study Swimming Pool

In this case too, a company approached the swimming pool concerned with their products. The system was made available free. As a result, a biometric application was introduced. First as an access control test case for some months, and later on it was operationalized on a permanent basis.

In contrast to the primary school case, the swimming pool concerned reports to have already felt a need to be able to enforce a ban on swimming pool entrance for certain persons who had shown disruptive behaviour. Introducing an efficient application that would allow the singling out of known offenders could become the corner stone of a security policy. This policy was aimed at creating a sense of security in the swimming pool. In addition, to enhance the quality of visits for the public at large. Thus, the objective was to enhance security of swimming pool customers by preventing undesired behaviour by a small group of customers already identified and banned from the swimming pool. The background to this objective was a rise in criminal behaviour in the swimming pool during the past 8-10 years (e.g. thefts, drunkenness, drugs abuse, vandalism or aggressive behaviour versus other customers, etc.). The introduction of finger print-based biometric technology in this swimming pool took place simultaneously with three other swimming pools in the same council area.

After implementation of the system in the swimming pool in July 2007, it became obligatory for all visitors to have a single finger scan taken, this scan is then crosschecked against the list of banned customers on database.

3.2.1 Technical Specifications

The system consists of a scanner that takes scan picture of the index finger of each customer. These digital finger scans are not stored but are encrypted into a template. The template is used to crosscheck against finger scans from those individuals who have been found acting in breach of the rules and regulations while they were in the swimming pool and have been banned consequently (people placed on a black list).
The templates are not stored and are not processed further unless there is a match with the templates of banned customers in the database. The database of the finger scans from the registered individuals is only accessible centrally, by less than five authorised people who maintain the biometric system. They use a password access system, which is known only by the maintainers. The system has been introduced in cooperation with the town council and local police.
All those on the black list of the swimming pool are asked to provide 10 finger scans by the maintained of the system. These prints are provided on a voluntary basis in the presence of a police officer. The data collected can only be used by the swimming pool for the process of comparison of the scans with those of visitors entering the swimming pool. However, one of the five persons authorised to maintain the system explicitly mentioned that the swimming pool could be asked by the police to provide the

fingerprints of the registered person for different forensic purposes. This has not yet happened in practice and has remained unclear on what legal basis police would ask for this information. The last aspect to be mentioned here is that the swimming pool has chosen not to use the system on a continuous basis. At busy times, the biometric application was used at the discretion of the person behind the till, based on criteria that have not been disclosed. In practice, this means that some people in the queue are scanned and others are not. In addition, the swimming pool will switch to a lower threshold when it is busy. This means that people will pass quicker through the system, but the negative failure rate is higher.

3.2.2 PET Aspects

The swimming pool visitor does not need to show an identification document to prove that he or she is not a person on the database. They provide a finger scan, which is encrypted into a template and then anonymously checked against the database and deleted after that. The privacy of the visitor is thus protected because no identification is shown and no record is kept of his or her visit to the swimming pool.

3.2.3 Other Aspects of the Implementation of this Biometric System

In this case, the limits of the purpose of the application seem to have been very loosely set. The impression remains that there is a second objective of comparing data kept by the swimming pool with those kept by the police in the future. This impression is reinforced by the situation that finger scans are taken from those who have shown disruptive behaviour in the swimming pool on what is regarded a voluntary basis. How voluntary this is, in view of the presence of a police officer, can be contested. Ideally, further clarification by a court or the data protection agency should be sought. Another interesting aspect of this case is the way this system has been implemented. When it is busy in the swimming pool visitors do not all have to provide a finger scan. In practice, the system is in fact used at the discretion of the person behind the till. It has not been possible to establish to what extent the use of the system is used on a discriminatory basis. The fall back procedure in case of technical failure is clear: the gates are just simply opened and people let through on the traditional method of facial recognition. There is no fall back procedure in case of a person refusing to provide finger scans. The swimming pool reports that it has adequately informed visitors through posters and brochures, and after initial critical queries the system is now uncontested. No information is available on whether the system has acted as a deterrent. In addition, it is not known whether potential visitors have been put off by the use of system and have sought their swimming pleasures elsewhere.

3.2.4 Issues Arising From Case Study Two

Use of Biometric Technology for Marketing Purposes

It is understood that the application of the biometric identification system was introduced in the swimming pool in order to be able to enforce the ban on a small group of people. Certainly, such an approach serves an underlying marketing purpose, to convince potential customers of the idea that it is guaranteed that their stay will remain undisturbed. It turns out that in practice the system causes delays at peak hours and personnel reverts to the more traditional photo black list method. The finding of this case study give indications that biometric technology here is used more as a 'Pet' technology, a new gadget that will impress the public, rather than that it can achieve objectives that cannot be reached in other ways.

S*ocial and Ethical Aspects*

The voluntary finger print taking from individuals that is taking place could also be regarded as semi-obligatory. The swimming pool authorities oblige those who have been disruptive to provide a sample in the presence of a law enforcement authority: a police officer. The swimming pool and the police then seem to be subsequently sharing this information. Two issues emerge here: the fact that the swimming pool authorities hold that there needs to be no legal basis for taking the samples (10) and the fact that personal information on the disruptive youngsters is stored, albeit with a high security level, also with a view to disclosing the data to police when so requested. The swimming pool cannot use this information for any other purposes than denying access to the swimming pool. It seems however, that the secondary objective is that they can pass on this information to police based on a legal request. This raises fundamental questions about rights of those who provide finger scans after being disruptive in the swimming pool.

Compliance with Dutch Data Protection

This same system is in operation in at least three more swimming pools in the Netherlands. At one other swimming pool, the biometric system uses both fingerprints and iris scans. First, as not all-necessary information has been made available it is impossible to determine whether this project complies with data protection legislation. Secondly, if it does, the question should be asked whether it would be important to assess the impact of this situation. Do the individuals concerned need more protection against function creep? Could the Dutch data protection Agency (CBP) provide a solution by issuing detailed guidelines or a categorisation of biometric applications?

3.3 Case Study Supermarket

A Dutch supermarket chain launched an experiment in June 2008 whereby customers at one branch only could opt for paying with their finger. The pay method involves authorisation of a payment from their account by authentication through placing their fingertip on a fingerprint scanner. The chain is treating this experiment as a six-month trial called the Tip2Pay project and is working with Equens, a fingerprint payment processor from Germany. The supermarket and Equens are conducting the pilot in consultation with IT-Werke, a German company that specialises in integrating biometric technology in retail and consumer applications. A German supermarket chain has already successfully tested the IT-Werke fingerprint scanner called digiPROOF. The Gewrman chain now offers fingerprint payment services at 120 of its stores.

The six-month Tip2Pay project is the first of its kind in The Netherlands. With this project, the supermarket chain aims to investigate the potential of this technology as a new payment method. The emphasis is very much on the question whether this method of payment will be received positively by its consumers. The supermarket chain has announced that after the trail period a continuation of the payment method may be considered the feedback is positive and the system proves reliable and secure in practice.

3.3.1 Technical Specifications

The digiPROOF system is connected to the cash register through a standard interface and communicates with the cashier over TCP/IP protocol. Before a costumer can use digiPROOF, he must sign up and provide his personal details, a debit card and a customer loyalty card if they have one, along with the initial scanning of their fingerprint. The scanning of the fingerprint will result in the creation of a template that will be encrypted to a unique code. It is then stored in a database registered with the Dutch DPA (College Bescherming Persoonsgegevens). Databases are backed-up and secured according to newest state-of-the-art technologies. All user interfaces are designed in such a way, that a mix of user data and templates is excluded.

Of importance in this whole process, a reliable recognition identification is highly dependent of good image data. The acquisition hardware has to provide a maximum quality raw image. To guarantee this, IT-Werke uses single fingerprint scanners, conform to FBI standards ANSI/NIST. To ensure desired quality, saving a digiPROOF template is designed as a multi step procedure. First three raw images are acquired and image quality is assessed. If predetermined thresholds are not obtained, the whole process has to be redone. Raw data are than aggregated and a template is written into a temporary database. Already in the acquisition process a 1:n identification takes place. This step reveals overall image quality and reliability of later identifications. DigiPROOF uses 24 typical reference points of the fingerprint that will be used to identify the finger later. If quality standards and benchmarks are not met, the process has to be redone. According the advantage of obtain good quality templates in this way is considerable as it avoids time-consuming capture of two fingers or complicated verification of complementary data (two-factor authentication) like phone or pin numbers. The disadvantage obviously, is that one-factor identification is always weak from a security point of view. The weakness of the system is thus its reliance on one factor authentication. Many security

experts feel that one-factor systems are only safe in private situations with a very small number of people using the system. In terms of prevention of fraud or abuse of the system, the use of a second factor (such as a pin code (something you know) or a customer loyalty card (something you have) or a second biometric (something you are) would decrease the security risks involved.

3.3.2 PET Aspects

The scan of a fingerprint is not be stored as a raw image, but as template obtained through a calculation (unique number). From this number it is impossible to derive the original fingerprint. The fact that the templates are based on irrevocable algorithms instead of raw images, leads to privacy enhancement.

As aforementioned, the database is backed-up and secured. All user interfaces are designed in such a way, that a mix of user data and templates is excluded. The database has been registered with the Dutch data protection authority. It remains unclear to the researchers what the physical location is of the database, and how authorised to a data controllers only has been secured. The impression was gained that because the system did not work with raw images, it was not perceived very important to restrict the number of individuals having access to the database. When asked the users and controllers of the systems were not aware of the PET aspects of biometric technology. The use of personal data however, was felt by them to be a privacy issue. It was put forward that there are concerns that costumers have to give too much personal information away to a commercial organization. In this case, the controller links the biometric data to the customer loyalty card. The company already uses this card for marketing purposes. In the existing situation without biometrics, the supermarket cannot ascertain whether the customer in whose name the card is, is actually using the card. With the biometric authentication, this is certain. This means that the data have become more reliable for marketing purposes. Large-scale use of the biometric paying system in this pilot could lead to a situation where the supermarket has very accurate and valuable data on shopping patterns, interests and spending power of millions of customers.

3.3.3 Main issues arising from Case Study Three

Cracking the IT-Werke system; A Need for Multiple Authentications?

Within two weeks of its introduction, a security researcher cracked the IT-Werke fingerprint payment system at the branch. The researcher succeeded by successfully constructing a copy of a fingerprint out of rubber that was accepted by the digiPROOF. Staff members of the store failed to detect the fraud. The method is easy to copy: Typically, a fingerprint left on a glass is sufficient to create a usable copy. A spokesperson for the supermarket chain stated, when prompted, that the hack did not demonstrate a genuine security threat, because a registered user of the payment system voluntarily provided his fingerprint to the hacker. The company argues that therefore the hack compares to cloning an ATM (automated teller machine) card. As the system has a daily spending limit and will compensates consumers in case of fraud, the risk is minimal. It has not been made public whether there have been other detections of identity fraud since the system has come into operation. It is obvious that all pay methods result in illegal use or fraud. The issue for the supermarket of course is,

whether the percentage of illegal transactions is smaller or larger than traditional methods of payment. Even if the number of illegal transactions was slightly higher, effects such as a pro-technology and modern image may still be worth the small financial loss. For the customer in good faith (the registered user in the security breach above was of course in bad faith) it is important that there are good fall back procedures and the supermarket chain can be held responsible for any financial losses.

Many companies maintain that secure authentication through fingerscasn technology requires additional security measures, especially when it comes to banking transactions. These companies opt for a plural or multiple authentications, e.g. a bankcard and a PIN code instead of only one-factor authentication like in the case of this supermarket. In this case, as discussed above, it is a one-factor system only, and the supermarket tries to obviate this risk by giving the costumer only a few attempts to scan a fingerprint, while the cashier overlooks him or her.

Absence of Reactive Security

A costumer notices when he looses his bankcard, and the first step he will take is to block his bankcard. This reactive security is not possible with a costumer who leaves his fingerprints behind everywhere, without ever knowing if criminals will copy them. Only after the first fraud has occurred, the registered user will be know of the theft and be able to block the account. Of course, it is not possible to issue a new fingerprint. To what extent it is possible to issue a new code through encryption is not clear. In any event, as the supermarket branch does not use multiple (or plural) authentication, the risk of the system being cracked is considerable. Although it has been published in the public domain that the system was cracked by one hacker within weeks, the chain does not want to disclose whether any more abuses of the system have been detected.[76]

High Thresholds and Comfort of Use Factor

Due to the high-predetermined thresholds, persons with worn out fingerprint (e.g. senior people) have problems with scanning their fingerprint successfully. There is no solution to this problem, as these high thresholds are needed in order for the fingerprint scanner to recognize the correct person. Despite the fact that older people sometimes have to scan a few times, it turns out that five months into the project, they are reported to be the most satisfied customers.[77] Shopping with their finger, without running the risk of being pick pocketed or otherwise assaulted, is what they find attractive in shopping at the branch that is conducting the pilot. The informal reports are that a high percentage of the customers are very satisfied with the system. The majority would like to continue using it. To what extent these customers are aware of other consequences of the system than comfort of use for them is unclear. It would be interesting to establish:

a. whether customers are aware of the increased profiling possibilities for the supermarket itself and the legal duty of the supermarket chain to provide the biometric data to police and judicial authorities when asked to do so in the context of criminal procedures and
b. whether the awareness of the possibilities under a. would change customers' wishes to keep using the system.

[76] Telphone Interview December 2008
[77] Telephone interview October 2008.

3.4 Case Study Hand Geometry Reader at a Private Sports Club

This sport club started using the Hand key in 2005. There was no trail period. The system consisting of a hand geometry reader and the hand as key (Hand key) is used at a number of similar clubs in the same chain all across the Netherlands. However, the Hand key systems of the clubs cannot be mutually consulted. In other words, the Hand key and corresponding personal data are only integrated in the local network of the sport gym. The owner and maintainer of the Hand key is Dewi B.V. Various manufacturers are bringing the Hand key on the market. Two well-known manufacturers of the Hand key are Ingersoll Rand and Honeywell. Dewi B.V. however, can access the data for maintenance and administration purposes.
The first ever pilot for the Hand key was conducted in 1993 at the Department of Energy in the US. The results were positive as the Hand key proved to have an excellent acceptance and high maintainability. Since then more than 100000 Hand keys have been sold around the world.

3.4.1 Technical specifications

The club concerned has installed the Hand key on a tourniquet that in combination serves as an access control system for gym members. Each new member has to be enrolled for the first time. The member would put their hand into the Hand key three times so that a CCD camera records a 3D image of the hand. The Hand Key reader utilizes field proven hand geometry technology that maps and verifies the size and shape of a person's hand all in less than one second. The Hand Key captures a three-dimensional image (older version used two-dimensional image) of the hand using a 32,000-pixel image array. The 90 measurements including the lengths, widths, thickness and surface area of the fingers and hand are taken. The algorithm converts these images into one mathematical value (template). The generated template is a nine-byte hand template, which ensures fast enrolment with minimum data coverage. This template is then matched with a unique ID-code of four numbers. The club stores the template and other personal data from the member in a central computer. These stored templates will then be used every time a member punches in or out, i.e. the stored template will be matched with the new generated template and the ID-code will be checked. If there is a match and the ID-code is correct, the tourniquet will provide access. Besides storing the template on a computer, there is also the possibility to store the template in the reader or on a card. Dirt, cuts, jewellery and abrasions on the hand are reported by the producer to have no impact on accuracy. Finally, it is important to note that the Hand key error rates at default threshold setting are extremely low. False Accept Rate (FAR) and False Reject Rate (FRR) are both 0.1%, the lowest of any biometric device.

3.4.2 PET Aspects

The gym manager was not aware of the PET aspects of biometric technology. The gym manager did not report the use of personal data as an issue. Neither the gym members showed any resistance against the Hand key and the collection of personal data. The main PET is the use of templates. The system does not work with raw data as an algorithm is used to convert the hand images into one mathematical value (template). The database used to store the templates and other personal data however, seems not very security proof. The manager reported that the database containing the templates and member data is approachable for every person employed by the club without any authentication/identification process taken beforehand. Furthermore, it is also approachable – at a distance- by Dewi for maintenance and administration purposes. The central computer containing the database is physically located in a room of the club.

The hand geometry technology used by the Hand key cannot be reverse-engineered to identify people. It does not store the image of the hand, but instead stores a 9-byte template, which is a mathematical representation of the hand image. This mathematical value is meaningless to other devices. In addition, no fingerprint or palm print information is gathered. Thus, it can be considered as a privacy enhancing technology.

Another PET possible is the notion that no law enforcement agency or other governmental institution keeps a database of hand templates whilst fingerprints and facial geometry templates are used in law enforcement. Therefore, in this case, the choice for hand geometry is more privacy enhancing than a choice for finger scans or face scans.

This also prevent the use of the data for surveillance purposes: facial recognition applications “scan the crowd” to identify known criminals. With hand geometry, a user cannot be identified without their knowledge and consent.

To ensure system integrity, a tamper switch is built into the Hand key reader. Tamper alarms and other conditions such as verification refused, lock out and duress can be monitored by the panel directly or through one of the Hand key's two auxiliary outputs.

Finally, the gym manager was not aware of the privacy enhancing possibility to store the templates on a card (instead of the computer as is the case now) resulting in the protection of cardholder privacy and eliminating the need to store and update cardholder databases.

3.4.3 Main Issues Arising from Case Study Four

Assessment of Technical Claims Made

Regarding the advantages of hand key over other forms of biometric identification, the low failure rates claimed by manufacturers seem to be questionable. Even though the manufacturers of the Hand key are advertising that, the Hand key has no problems with cuts, plaster and other inconveniences during scan process, the gym manager does state in the interview that sometimes scanning is difficult if afore-said circumstances are present. The problem here is, that just as in the case of PRIVIUM at Schiphol, figures are not released or are unknown (negative failure rates) and assessment of claims of producers is difficult.

Easy Approachable Hand Geometry Database Encompasses Risks

Another issue rising from this case study is the fact that the database containing privacy sensitive information and templates is easy to access and not well protected. The lack of a security enhancing protocol while entering the database contains risks, and the number of people that can access the database within the organisation is unrestricted. There is certainly no all-encompassing prevention policy to prevent theft or abuse of biometrics of the individuals concerned in place. In this case this can partly be explained by the belief that hand geometry, in contrast to other biometrics that are used by central governments or for example in banking, is not very suitable for further criminal activity such as various forms of identity fraud. As stated above, hand geometry is also not very useful for purposes of surveillance.

Absence of Detailed Knowledge on PET Aspects or Data Protection Legislation

It is interesting to see that this Club as the user of the Hand key and the affiliated database is unaware of any rules and regulations involved when using personal and biometrics data. The gym manager could not tell whether the Hand key and the used database are conform legislation and if the status quo should be registered with the data protection authority. Here again, there seems to be a need to be informed. Public guidelines covering the use of biometrics in all four application domains (large-scale public, large-scale private, small-scale private/semi-public, and individual small scale) would provide the information needed for any organisation to make sure that its controllers stay within the law

3.5 Some Observations on the difficulty of Drawing up an Inventory

The project team has gathered information through the internet, following it up with phone calls and interviews. This process has been slow and frustrating and the number of projects and applications on which reliable and complete information could be obtained has stayed relatively low. A project count did not reach beyond hundred (see Annex) and we have looked at about twenty private and semi public biometric applications in detail. A few public applications that have semi-public aspects have been included in the inventory (see Annex to this report), but none of them have been selected for further study. Other studies carried out by the Tilburg Institute for Law, Technology and Society have concerned some public or semi-public projects that include the use of biometrics. Examples are the new Dutch passport (public use of face scan and fingers can, obligatory) and the PRIVIUM facility at Schiphol Airport (semi-public use of iris scans for fast airport passage, voluntary).[78]

Some of the projects in the private or private sector were found to have a 'pet project'[79] character, and many others were still in a pilot phase. We traced a number that had been set up and then "petered out" for all kind of practical reasons. If not enough publicly available information could be found, we

[78] Brussee et al, 2008. Oomen (2007) on Privium: "Identification and anonymity of citizens in the governmental provision of services":
http://www.fidis.net/resources/deliverables/forensic-implications/d54-anonymity-in-electronic-government-a-case-study-analysis-of-governments-identity-knowledge/doc/8/.

[79] With 'pet project' we refer to another meaning of 'pet': the 'new gadget' aspect of biometrics. Here we see the introduction of biometrics because it is a "cool" play thing. Subsequently, and in the longer term however, the application is not that much fun and for practical reasons users return to old procedures or, in case of a pilot, the use of the application is discontinued.

have left projects out of the inventory. Often, in case of small projects in the private or semi-private domain, the exact reasons for discontinuing the use of biometrics could not be found in documents. It also often proved difficult to find individuals prepared to give information in (telephone) interviews. In one large-scale case, a pilot project with voice verification, the reasons behind the decision not to roll out after a pilot phase could be established.

This is the voice verification in telephone banking at ABN AMRO, put on hold in 2008 after a take over by Fortis, Royal Bank of Scotland and Banco Satander. For ABN AMRO, the proposed use of voice verification was one development in a wider strategy to use speech technology in the provision of bank services.[80] The ABN AMRO bank had carried out a telephone pilot to assess whether voice recognition was a worth while alternative for TIN code (Telephone Identification Number) in a stand alone system with more than 1300 (employee) participants and over 30.000 calls.[81] This project was technically very successful and as competitors were not at all in a position to introduce voice recognition within the near future, the bank seemed on course to gain 'a first mover competitor advantage'.[82] Because of the take over in 2007, a changing company strategy and a wider need of re-assessment of the cost of the overall project portfolio has put the project on hold. From the documents available it becomes clear that the take over has probably only caused a serious delay in the full roll out of a system using biometrics. The bank is still aiming for an optimal use of different speech (including voice) technologies in bank services. This can be explained as follows: like iris recognition, voice recognition is less likely to be used for other (e.g. forensic) purposes than the application in hand. In trials, the technology an equal error rate of below 1% has been achieved, exceeding security and performance criteria, even without factoring the additional security of a second factor such as a security question. In addition, from an end user point of view, speech it is an intuitive and natural technology. Voice or speech recognition only uses spoken words, and it is generally regarded less intrusive than systems that rely on scanners or other devices.

More than ten of the projects we looked at in more detail could be said to be demand led: this means that the initiative to consider starting to use a biometric application had come from the producer. A clear example of a "demand led" example is the use of biometrics at the primary school detailed above. In these cases, often the user of the application relied completely on the information of the producer, including the producer's guidance on data protection. Here we observed two important trends. Firstly, a top down approach could be identified in many cases. Here we noticed a 'dropping' of the biometric application through the producer, via the management, down to the controller and user, results in a situation where de facto controllers and users of the applications are unwire of important aspects or PET possibilities of the applications they are using. An unease and lack in confidence of the controllers could be identified. There is clearly a need for independent information concerning biometric applications, their impact on privacy and data protection. Secondly, there is a serious risk of vendor lock in (see section below).

[80] For example: the bank uses another form of speech technology: the use of speech navigation in customers' telephone contact with the bank (replacing complicated touch-tone menus).

[81] For details see: http://www.findbiometrics.com/Pages/voice%20articles/vvabn.pdf

[82] For the factors determining the choice for voice recognition and the full strategy and short, medium and long-term outlook of the bank, see the report by Frost and Sullivan: Leading European Financial Institution Implements Voice Verification Biometrics to Enrich Customer Experience, July 2006.

Many PET features listed above have a low adoption rate when we examine the projects that we identified. This might be explained by that the PET features usually lack ease of use, sometimes their benefits are not perceived as high priority or are not known, and they almost without exception add to the cost of the biometric technology application.

Where there seems to be a need for biometrics to provide convenience and service in most applications in the private or semi-public sector that we find in our inventory, privacy has hardly been a consideration. There are some exceptions such as PRIVIUM at Schiphol. It is obvious that the investments made in the technology made for business travellers at an airport[83] cannot be equalled in down town cafes selling soft drugs or in schools striving to control entry of all members of a school community. In most semi public applications however, privacy and PETs seem to have been low on the agenda and the controllers of the system were unable to answer questions about privacy and possible PETs. Anonymisation and pseudonymisation processes were found to be rare, and reversible templates linked to other personal data such as name, address and date of birth used.

In some of these privacy-enhancing possibilities for the use of biometrics, the introduction of privacy protection would have reduced the convenience of use, or have increased the costs disproportionately. The cost factor was important in this respect but also the dependence of the buyers of the biometric applications on the producers selling them.

3.6 Some Observations on the Four Case Studies Detailed Above

As already has become clear from the section above, an active marketing approach of industry is observed to be an important factor in the development of the use of biometric applications. The four case studies show a picture of relative dependence on the products. In addition, a dependence on the information and knowledge of the biometric application producers can be detected. This also applies to the PET aspects of the technologies used. At least in the case studies presented here it turns out that the people dealing with the applications on a day to day basis, do not have a clear idea about the choices that have been made and how this relate to privacy enhancing possibilities and data protection legislation. In none of the case studies for example, biometrics are used as an ex post measure to provide an extra layer of security against data theft. It is reassuring to find that the applications examined refrain from the use and storage of raw data. At the same time, the persons actually running these applications did admit that they were not aware of the difference between the two. In addition, few of those interviewed showed an insight into the relationship between data security and one-dimensional and multi dimensional systems. The absence of reactive security was also not considered an issue. Possibilities for storing on card rather than on database were not considered or, at least not known to have been considered. The importance of protecting access to a database to prevent identity fraud and theft, or illegal processing of data did not appear to be a priority for most of the people interviewed.

We therefore identify a clear need for government guidelines destined at those who choose, implement and run a biometric application. As far as some guidelines already exist, they do not seem to have been communicated to such extent that they have reached the audience intended. Especially

[83] The PRIVIUM facility will now be extended beyond the original target group of frequent business travellers: http://tweakers.net/nieuws/54633/schiphol-gaat-irisscan-voor-iedereen-beschikbaar-maken.html

where it concerns semi-public institutions such as the school in our case study, clear guidelines need to be made available to any school board or management deciding on the use of biometrics in their school. In none of the case studies were participation was (semi) obligatory (three) there was a procedure for those objecting to provide biometrics, nor were there adequate fall back procedures for someone was unwilling to participate or an occurring instance of failure of technology. We have not paid too much attention to technical issues such as high thresholds or engaged in an assessment of claims made about biometric systems. To some extent, this has already been done elsewhere and it would be too ambitious in the context of this study.[84] Some of the issues identified in these studies; such as function creep, use of biometric technology for marketing purposes, social and ethical aspects of the use of biometrics all showed up in our four cases studies too. What we want to note here is that privacy enhancing aspects of biometrics should also be seen in the light of society's interest in minimising the possibility of identity theft. The less is known about you, the lesser options there are for stealing some of your personal details or even your identity. The main PET issues remain storage on database and protection of biometric data. The storing of biometric data on a database or the unsafe storage of biometric data should be minimised and prevented where possible. The above case studies show without doubt that current practice is not informed enough to make PET choices or to explain them to the public. A more stringent monitoring of the practical implementation of biometric applications is long over due. Now the over stretched DPA is the only body that could exercise some control over individual biometric applications. The Dutch DPA does not have the French powers of having to grant an authorization before the start of the processing of biometric data. Nevertheless, there is scope for following up notifications and assessing them based on data protection principles. Are the biometric data fair and lawfully processed for a limited purpose, are the data adequate, relevant and not excessive and accurate. Are data no longer kept than necessary, secure and processed in accordance with the data subject's rights? Formally, a notification to the data protection authority does not imply a 'go'. On the contrary, the notification allows the authority to react is this is needed. In practice, and due to staff constraints, this seldom happens. It is also not required that the processor or controller waits for a confirmation that processing can start. The controller can commence processing once he has submitted notification. As the DPA does not have the staff capacity to go out and assess notifications, nor the possibility to engage in a fully-fledged information policy, the question is whether a separate government body should be appointed to deal with the approval of biometric applications in semi public and private applications. Storage of biometric information could then be notified to this designated body with power of control that would also have to be informed in case of abuse of biometric data. A set of detailed and easily obtainable guidelines for all situations would certainly help to make the use of biometric applications in the Netherlands more privacy enhancing and more secure. The guidelines may be complemented with a categorisation of biometric application and techniques, that could make it easier to find the best possible solution using biometrics in any particular circumstances. Some efforts have already been made to initiate such a categorisation.[85] Of course, to avoid duplication, a European wide voluntary code with a

[84] Gasson, 2007; Cavoukian, 2008; all FIDIS work on biometrics: www.fidis.net.
[85] Albrecht, 2003; European Biometrics Forum, 2007; Kindt and Dumortier, 2008.

categorisation[86] of biometric applications with corresponding data protection and security guidelines would make sense.

[86] Kindt and Dumortier(2008).

Chapter IV: Conclusions and Recommendations

Conclusions

In this project, we have assessed the PET aspects of biometric applications currently in use in the private and semi-public sector in the Netherlands. As defined above, privacy enhancing technologies refer to a variety of technologies that protect personal privacy by minimizing or eliminating the collection of identifiable data. We have looked at the legal framework for using biometrics in the EU and the Netherlands and at privacy enhancing characteristics of current biometric technologies. We have observed that whilst the biometric applications can introduce many benefits, they can also cause new privacy and security risks and vulnerabilities. Decisions that determine how (and which) biometrics will be used in any particular system set the standard. The security of the system that the biometric application will become part of is equally crucial. In one of the earlier articles on biometrics Grijpink stated some basic rules for the use of biometrics: sectoral boundaries[87], clear, recognizable and permissible objective, proportionality, subsidiarity, precise delineation of the target group, security and external supervision. [88] We have seen that some of these principles have come under considerable pressure since 2001.

Our fieldwork shows that especially external supervision on the use of biometrics in the Netherlands is lacking. Due to staff shortage and lack of powers, the Dutch DPA has not been able to develop an active policy on the stimulation of good practice in the use of biometrics. At the same time, the DPA cannot possibly be expected to provide informed steering of the approach to biometrics alone.[89] What is needed is a multi-layered approach, with a policy role for all tiers of government and an active role of the Dutch parliament in calling the government to account. So far, the introduction of biometrics in the private sector seems to escape the attention of government, parliament and the data protection community. Guidelines on the use of biometrics such as those issued in the UK[90] would be one way of providing a lead and improving the information position of data subjects. No new legal powers are necessary for the DPA to issue detailed guidelines.

Of course increased powers for the DPA, more in line with the French approach, for example a system whereby prior approval of a certain biometric application is needed, could be considered. Certification of biometric applications would require a separate regulation on biometric applications. A regulation on biometrics might for example consist of an explicit legal prohibition to process raw images, an obligation to encrypt biometric data used for processing and an obligation to use multiple authentications.[91] The question is of course whether in practice these goals cannot be achieved with

[87] Grijpink (2001) stated: "one of the fundaments of the protection of privacy is that data from a certain sector cannot automatically be sued in another sector. The use of biometrics should therefore not automatically be permitted to exceed the sectoral boundaries that have come about in practice and have been sanctioned by law. The sectors in question include banking, health care, education, and in the public sector taxes or civil affairs" p 158. Compare this to current developments in Persoonsinformatie of Identiteit? Identiteitvaststelling en Elektronische Dossiers in het Licht van Maatschappelijke en Technologische Ontwikkelingen, Brussee et al, 2008.

[88] Grijpink, 2001, p 158-159.

[89] On the role of the DPA and the development towards a second generation of supervisory authorities see: De Hert, 2009 38-40.

[90] www.ico.co.uk

[91] See De Hert and Sprokkereef, 2008, 302.

other means such as information provision, broadening of administrative powers[92], extensive use of opinions and effective enforcement through increased consultation. Categorisation of different biometric applications and their impact on privacy as described at the end of section 3.2, would be a mid way house. It could also take the form of a voluntary code of conduct. An obligation to notify any loss or abuse of data to the DPA or another designated body has also been suggested.[93] Although experts agree that privacy enhancing measures are technically sound and obvious, those making decisions about the use of biometrics and the public at large are often unaware of the issues. More proactive policies stimulating best practices and more community involvement in the enforcement of data protection legislation can make amends for the latter.

In our analysis, we have focussed on control of users of biometric technology over their own data. From the literature can be concluded that in large-scale applications the adequacy of PETs at this roll out stage of current biometric applications can be challenged in terms of their technological effectiveness. [94] However, effective individual PET measures may seem in themselves, when their overall system design is not geared towards the same protection criteria, privacy can be protected at one end of the system and invaded at the other.[95] More importantly, the security and public policy implications of the large scale use of biometric data as PETs are still uncertain.The diversity of the results of current assessments becomes clear from the different solutions preferred by EU member states when deciding on centralized and/or de-centralized storage of biometric data contained in the new EU passports[96]. In the end, PETs that offer (semi) anonymity potentially endanger national or individual security because the prevention, investigation or prosecution of identity fraud cases will be hampered. These aspects have not received further attention in this study because our findings concern the use of PETs in small-scale applications in the private and semi-public domain.

Clearly, the use of PETs is broader than just the protection of information, as it also concerns technological possibilities to improve the quality of the information and the technological possibilities to access and correct personal information. If this can be achieved through biometric technologies, biometrics can be applied as a data protection enhancing mechanism. To return to the issues of control, consent and correction, the information aspect of using biometrics as PET is crucial. From the case study section, we conclude that information about biometrics as PET is lacking. Alternative uses of biometrics are not clear to those who are in a position to make decisions about the use of alternative biometric applications. It appears that many consumers of biometric applications and the persons whose biometrics are enrolled in their applications make relatively uninformed decisions about the disclosure of data. Following chapter two, what we did expect to find would be informed decisions and clear information about: decentralised storage; encryption; verification on a token or match on card; emphasis on security of systems and so forth. This was not the case.

The conclusion from our preliminary inventory and detailed case studies is that privacy implications of biometric applications are not that well understood, even not by those involved in their implementation. For most project managers, the absence of a negative reaction following notification of a project to the

[92] De Hert, 2009, 39.
[93] This is a proposed in the UK now (and the idea has been endorsed by the UK information Commissioner).
[94] EBF, 2007; Adronikou, 2007; also www.fidis.net.
[95] For example because the number of agents having access to the data is unlimited, or can be increased through processes of function creep.
[96] Grijpink, 2008.

Dutch Data Protection Authority constitutes an endorsement of compliance with data protection. The need to introduce biometric technology as privacy enhancing as possible under the circumstances was not very strongly felt.
The growing interest in PETs is justified. The development of PETs, also in electronic government, is still ongoing. In view of the fact that biometric applications are expected to take a flight in the near future, the stimulation of best practice and clear government guidance should become a priority. Government guidelines and information campaigns on best practice are already in place in some other EU countries. Clearly, PETs can be solutions in part problems and practical situations. However, the stimulation of PETs in biometric applications can only be supportive of a thorough general policy on data protection and the use of biometrics. Given the complexity of the assessment of the technical possibilities of biometrics, detailed legislation on the use of biometrics might make compliance more likely. However, no other European country has gone down the road of separate regulation of biometrics (see chapter one). As this study has shown, in the Netherlands there is still scope for a more effective enforcement of existing legislation through the instruments mentioned above. Therefore, this is the more obvious route.
However, the findings of this study do support the arguments for strengthening the DPA. Increased, tougher powers of the Dutch Data Protection Authority would help to achieve enforcement that is more effective and better control over breaches of security, data abuse and data losses. In view of the fact that the DPA is an agency with a broad mandate that is already overstretched other options could be considered. Entrusting enforcement in the field of biometrics to an agency other than the DPA might be an option at a later stage when biometric practices have become more firmly established. At the present time, a DPA categorisation of applications according to their objectives and technical specifications could help those responsible in the private and semi-public domain make the best decisions to protect the privacy of those required to provide their biometrics for processing.

Recommendations

As biometric technologies have also become part and parcel of public policy, there rests a serious responsibility on the government to ensure that the introduction of this technology will prove an asset.

An update of the 1999 Rekenkamer report is long overdue. As biometric technology has moved on, if not matured, stock should be taken of developments in the use of the technology in the public and in the private sector. The new report could provide input for future government policy.

The findings in this study indicate a clear need for information provision on the PET aspects of biometrics and guidelines for private businesses and semi-public organisations considering the use of biometrics. Our research has also highlighted a lack of external supervision. If the update of the 1999 report confirms the findings in this small-scale study, the following recommendations should be seriously considered:

- more effective use of some existing instruments (especially of the right to request DPA opinions)

- the adoption of a new instruments (such as detailed guidelines, categorisation of biometric applications or a new form of prior approval)
- a broadening and strengthening of the administrative powers of the Dutch DPA
- entrusting some aspects of enforcement of data protection in the case of biometric applications to a separate agency

REFERENCES

ADAMS, C. (2006). "A Classification for Privacy Technologies." 35-52.

ALBRECHT, A. (2003). "BIOVISION: D 7.4, Privacy Best Practices in Deployment of Biometric Systems (Final Report).

ALTERMAN, A. (2003). ""A piece of yourself": Ethical issues in biometric identification." Ethics and Information Technology (Kluwer publisher) Vol. 5.: 139-150.

ANDRONIKOU, V. D., D. S.; VARVARIGOU, T. (2005). "Biometric Implementations and the Implications for Security and Privacy." Journal of the Future of Identity in the Information Society Vol. 1.(Issue 1.): 20.

ARTZ, S and VAN BLARKOM (2002). "Beveiliging van persoonsgegevens: de WPB. Privacy en Biometrie: een technisch vraagstuk?" Jaarboek Fraudebestrijding.

ASHBOURN, J. (2005). The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies Background paper for the Euroscience Open Forum ESOF (2006) in Munich. Available from: http://www.statewatch.org/news/2006/jul/biometrics-and-identity-management.pdf

BECTA, B. E. C. a. T. A. (2007). "Becta guidance on biometric technologies in schools." 1-10. Avaliable from: http://schools.becta.org.uk/upload-dir/downloads/becta_guidance_on_biometric_technologies_in_schools.pdf

BENOLIEL, D. "Law, Geography and Cyberspace: The case of Territorial Privacy ".

BORKING, J. (2008a). Organizational Motives for Adopting Privacy Enhancing Technologies

BORKING, J. (2008b). The Business Case for PET and the EuroPrise Seal. Europrise deliverable.

BOS, T. (2007) "Privacy-Enhancing Technologies: Theorie en Praktijk bij de Overheid".ego Vol. 6, no 2, 26-28. http://www.sbit.nl/ego/bestanden/EKSBIT1.pdf

BRAY, E. (2004). "Ethical Aspects of Facial Recognition Systems in Public Places." Info, Comm and Ethics in Society (2004) 2: 97-109.

BRUSSEE, R., Heerink, R. Leenes, S. Nouwt, M. Pekarek, A. Sprokkereef and W. Teeuw (2008). Persoonsinformatie of Identiteit? Identiteitsvaststelling en Elektronische Dossiers in het Licht van Maatschappelijke en Technologische Ontwikkelingen. Telematica Instituut. Report TI/RS/2008/034:1-98.

CAMENISH, J. and R. Leenes and D. Sommer (2008). PRIME deliverable The PRIME Architecture, Brussels, February 2008.

CAVOUKIAN, A. and A. Stoianov (2007). Biometric Encryption:A Positive-Sum technology that Achieves Strong Authentication, Security And Privacy. Infromation and Privacy Commissioner's Office, Ontario.

CHO, A. (2008). "University Hackers Test the Right to Expose Security Concerns" Science Magazine Vol 322, 28 November 2008, pp 1322-23.

CROMPTON, M. F. P. C. (2002). "Biometrics and Privacy - The End of The World as We Know It or The White Knight of Privacy?" Not Journal: Conference Paper - Biometrics – Security and Authentication - Biometrics Institute Conference: 1-17.

DIMITRIADIS, C. K. (2004). "Biometrics - Risks and Controls." Information Systems Control Journal Vol. 4.

DONOS, V. Z. a. P. (2004). "On biometrics-based authentication from a privacy-protection perspective - Deriving privacy-enhancing requirements." Information Management and Computer Security vol 12: 125.

EUROPEAN BIOMETRICS FORUM (2007): Security and Privacy in Large Scale Biometric Systems commissioned by the EC: JRC/ITPS. Avaliable on: http://is.jrc.es/documents/SecurityPrivacyFinalReport.pdf

EUROPEAN COMMISSION (2007). A Fine Balance 2007: Privacy Enhacing Technologies; How to Create a Trusted Information Society. Conference Summary.

FREEMAN, E. (2003). "Biometrics, Evidence and Personal Privacy." Information System Security. July/August.

GASSON M. et al (2007) (eds.) *Fidis deliverable D.3.2. : A study on PKI and Biometrics*, www.fidis.net

GONZALES FUSTER, G. and S. Gutwirth (2008). “”Workingpaper series REFGOV-FR-19 at http://refgov.cpdr.ucl.ac.be/?go=publications.

GRIJPINK, J. (2008). “Biometrie, Veiligheid en Privacy”. Privacy en Informatie. vol 11: 10-14.

GRIJPINK, J. (2005). “Two Barriers to Realizing the Benefits of Biometrics”. Computer Law and Security Report 21(3) 249-256.

GRIJPINK, J. (2001). "Biometrics and Privacy." Computer Law and Security Report Vol. 17(No. 3): 154-160.

HAMMOND, R. J. H., Jr. (2003). "Identity Theft: How to Protect Your Most Valuable Asset." 224.

HERT, P. (2009). Citizens’ Data and Technology: An Optimistic Perspective. The Hague: Dutch Data Protection Authority.

HERT, P. and A. Sprokkereef (2008). “Biometrie en Recht in Nederland”. Computerrecht. 301-302.

HERT, de P. W. Scheurs and E. Brouwer (2007). "Machine-readable identity Documents with Biometric Data in the EU - part III - Overview of the Legal Framework." Keesing Journal of Documents and Identity (No. 22): 23-26.

HERT, de P. and A. Sprokkereef (2006). "An Assessment of the Proposed Uniform Format for Residence Permits." Directorate-General Internal Policies Policy Department Citizens Rights and Constitutional Affairs: 1-16.

HES, R. (2000). Privacy-Enhancing technologies: The Path to Anonymity Registratiekamer Achtergrond Studies en Verkenningen 11 (Revised Edition): 1-60.

HES, R., T. F. M.Hooghiemstra and J.J. Borking (1999). At Face Value, On Biometrical Identification and Privacy Registratiekamer Achtergrond Studies en Verkenningen 15, September 1999, 1-70.

HOPKINS, R. (1999). "An introduction to Biometrics and Large Scale Civilian Identification." International Journal of law Computers and Technology 13(3): 27.

HORNUNG, G. (2005) Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren. Reihe „Der elektronische Rechtsverkehr“, Prof. Dr. Alexander Roßnagel (ed) and TeleTrusT Deutschland e.V., Vol 10, Nomos Verlagsgesellschaft, Baden-Baden

HORNUNG, G. (2007). "The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards." SCRIPT ED Vol 4(3) September, 246-262.

JOINT RESEARCH CENTRE (February 2005). "Biometrics at the Frontiers: Assessing the Impact on Society." Technical Report Series; Institute for Prospective Technological Studies (IPTS): Seville.

KINDT, E and J. Dumortier (2008). “Biometrie als Herkenning- of Identificatie Middel” Computerrecht 2008 132 ff.

KINDT, E. (2007). "Biometric Applications and the Data Protection Legislation (The legal Review and the Proportionality Test)." Datenschutz and Datensicherheit (DuD) 31: 166-170.

KINDT, E. (2007 December 28). "FIDIS (Future of Identity in the Information Society) Deliverable 3.10: Biometrics in Identity Management."

Surveillance Studies Network ((2006). A Report on the Surveillance Society - For the Information Commissioner by the Surveillance Studies Network (Full Report): Kristie Ball, D. L., David Murakami Wood, Clive Norris, Charles Raab. To be found at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

LARSSON, M. P., L. Nancy and H. Stattin (2007). "Associations between Iris Characteristics and Personality in adulthood." ELSEVIER; BIOLOGICAL PSYCHOLOGY (online publication)): 1-11.

LEVI, M. et al (2004). "Technologies , Security, and Privacy in the Post-9/11 European Information Society." Journal of Law and Society Vol. 31, No. 2.(4th June 2004): pp 194-200.

LEEUW, de E. (2007). "Biometrie en Nationaal Identiteitsmanagement." Privacy and Informatie Vol. 2 (No. 10): 50-56.

MINISTERIE VAN BINNENLANDSE ZAKEN, (2004). Privacy Enhancing Technologies. Witboek Voor Beslissers. R. Koorn et al. The Hague.

NETKWESTIES (2008) "Biometrie voor Discotoegang: Fun Kost Privacy." Netkwesties (Online Magazine: over Vrijheid, Rechten en Regels op Internet) (22/07/2008): 4.

NEUWIRT, K. Report on the Protection of Personal Data with Regard to the Use of Smart Cards. Council of Europe.

NICHOLAS M. P. Orlans and J. D. Woodward (2002). "Biometrics."

PHILIPS, D. (2004). “Privacy Policy and PETs” New Media and Society Vol 6 (6) 691-706.

PETERMANN, Th and A. Sauter, (2002) Biometrische Identifikationssysteme Sachstandsbericht, TAB Working report nr 76: http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

PLOEG van der, I. (2003). "Biometrics and Privacy A Note on the Politics of Theorizing Technology." Information, Communication & Society 6(1): 19ff.

PLOEG, van der I. e. D. L. (2002). "Biometrics and the Body as Information, Normative issues of the Socio-Technical Coding of the Body (chapter 3), in: Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination Routledge: New York.). 57-73.

PLOEG van der, I. (1999). "The Illegal Body: 'Eurodac' and the Politics of Biometric Identification." Ethics and Information Technology.

PRINS, C. (1998). "Making our Body Identify for Us: Legal Implications of Biometric Technologies " Biometric Technology Law - Computer Law and Security Report Vol. 14. no. 3 1998.

RIBBERS, P. (2008). Privacy Risks, Benefits and Costs, Deliverable F3 of WP0301 PRIME Consortium, 15th february 2008.

RUNDLE, M. C., Chris (2007). "Ethical Implications of Emerging Technologies: A Survey (UNESCO, Information for All - IFAP)." UNESCO, Communication and Information Sector: 1-90.

SPROKKEREEF, A. (2008) “Data Protection and the Use of Biometric Data in the EU”; in IFIP International Federation for Information Processing, Volume 262: The Future of Identity in the Information Society; Simone Fischer Huebner, Penny Duquenoy, Abin Zaccato, Leonardo Martucci; (Boston Springer), pp 277-284.

STATEWATCH (30/11/2004). "An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents" European Digital Rights.

TAVANI, H and J. Moor (2001). “Privacy Protection, Control of information, and Privacy-Enhancing Technologies” Computers and Society March 6-11.

TURLE, M. (2007). “Freedom of Information and Data Protection Law: a Conflict or a Reconciliation?” Computer Law and Security Report 23: 514-522.

TUYLS, P, B. Skoric and T. Keevenaar (eds) 2007) On Private Biometrics, Secure Key Storage and Anti-Counterfeiting (Springer).

WRIGHT, T. (2007). "Promoting Data Protection by Privacy Enhancing Technologies." C. T. L. R. 2007: 6.

Annex: Inventory of businesses using biometric applications as found and investigated by the project team in 2008

Project/onderzoek	Soort biometrie	Website
20 Kinderdagverblijven in Groningen	Vingerafdrukherkenning	http://endtimes.punt.nl/index.php?r=1&id=478479&tbl_archief=0
Abonnement bij Dierenpark	gezichtsherkenning	http://www.dierenpark-emmen.nl/nl/praktischeinfo/abonnementen_nieuw_systeem.htm
Betalen supermarkt (proef)	vingerafdrukherkenning	http://www.persberichten.com/persbericht.aspx?id=48892
Bemiddelingsbureau	vingerafdrukherkenning	www.suprema.nl
Basisscholen in Limburg	vingerafdrukherkenning (twee vingerafdrukken nodig)	http://www.identysoft.nl/pers.php
Bedrijvencentrum in Zuid Holland	vingerafdrukherkenning	www.suprema.nl
Benzinepomp in het zuiden van het land	vingerafdrukherkenning	www.suprema.nl
Bepaalde diensten van een NL bank	stemherkenning	http://www.security.nl/article/16035/1
Groot bedrijf	vingerafdrukherkenning	http://www.ingenieur-job.stepstone.be/content/be/bnl/HR_Magazine_Toegangscontrole_en_tijdsregistratie.cfm
Beveiligingssysteem (BCA systems)	vingerafdrukherkenning	http://www.bca-systems.com/beveiliging/index.html
Beveiligingssysteem (Biot)	vingerafdrukherkenning	http://www.biot.nl/content/view/39/76/lang,nl/
Bezoekers controle systeem marketing bedrijf	gezichts-, vingerafdruk en stemherkenning	http://nl.itsmportal.net/gotosection/leverancier/160.xml
Café in Brabant	Vingerafdrukherkenning	http://www.waarmaarraar.nl/pages/re/16520/Cafe_neemt_vingerafdruk_van_bezoekers.html
Cargocard Nederlandse haven	Handgeometrie	http://www.secure-logistics.nl/cargocard/index.php
Cashferium	gezichts- en vingerafdrukherkenning (meerdere vingerscans)	http://www.sa-road.com/
Chippas van vliegmaatschappij	vingerafdrukherkenning	http://www.dft.nl/bedrijven/airfrance-klm/2112111/Chippas_moet_vliegen_eenvoudiger_en_sneller_maken.html?cid=rss
Coffeeshops in Noord Holland	vingerafdrukherkenning	http://www.koffieshopbirdy.nl/main/index.php?option=com_content&task=blogsection&id=10&Itemid=37
Coffeeshops in Zuid Holland	vingerafdrukherkenning	www.suprema.nl
Coffeeshops in Limburg	gezichts- en vingerafdrukherkenning	http://www.nieuws.nl/464461
Datacenter in Noord Holland	gezichts- en vingerafdrukherkenning	http://www.sa-road.com/

Data Info Centrum	vingerafdrukherkenning	http://www.bioxs.nl/physicalxs
DCG Amsterdam	vingerafdrukherkenning	http://www.nxs.nl/content/nxsinternet/datacenters/dcg_amsterdam/
Discotheek in Zuid Holland.	gezichts- en vingerafdrukherkenning	www.alcazar.nl
Een uitzendbureau in het midden van het land	vingerafdrukherkenning	www.suprema.nl
Een van de grootste deurenleveranciers van Nederland	vingerafdrukherkenning	www.suprema.nl
Electronica groothandel	vingerafdrukherkenning	www.suprema.nl
F!tness centrum Zuid Holland	Vingerafdrukherkenning	http://fitness.moonfield.nl/algemene-voorwaarden
Aantal fitnesscentra in Gelderland	vingerafdrukherkenning	http://www.sa-road.com/
Gokhallen (5) (pilot voor 250 amusementscentra)	vingerafdrukherkenning	http://www.ad.nl/binnenland/2847299/Gokverslaafde_geweerd_met_vingerafdruk.html
Gemeentes in het zuiden en midden van het land	vingerafdrukherkenning	www.suprema.nl
Gemeentehuis in de Veluwe	vingerafdrukherkenning	http://www.easysecure.nl/ingebruikbijDetail.php?id=8
Gloeilampfabrikant in het zuiden van het land	vingerafdrukherkenning	www.suprema.nl
Grote verzekeraar in Friesland	vingerafdrukherkenning	www.suprema.nl
HOROMECA	vingerafdrukherkenning	http://www.horomeca.com/toegangscontrole-biometrisch.html
Nationale Verslavingszorg	Handgeometrie en vingerafdrukherkenning	http://www.kennislink.nl/web/show?id=89849
Internetcatalogus universiteit	Vingerafdrukherkenning	http://cms2.tudelft.nl/live/pagina.jsp?id=6270f7b0-d981-4c42-9a78-aef01004430c&lang=nl
Kinderdagverblijven in Deventer e.o.	Vingerafdrukherkenning	http://www.destentor.nl/regio/deventer/deventer/3766657/Vingerscan-doet-intrede-in-Deventer.ece
Milieufederatie	vingerafdrukherkenning	www.suprema.nl
Ministerie van Justitie - rechterlijke organisatie	vingerafdrukherkenning	www.precisebiometrics.com en webwereld.nl/articles/4147/justitie-stapt-over-op-vingerafdrukidentificatie.html
Mode shows	vingerafdrukherkenning	www.moniquecollignon.com
Nederlandse bank met het hoofdkantoor in het midden van het land	vingerafdrukherkenning	www.suprema.nl
Notariskantoor in Zuid Holland	vingerafdrukherkenning	www.suprema.nl
Perfect school	vingerafdrukherkenning	http://www.gonen.nl/products/perfectschool/nlperfectschool.htm

	irisscan	http://www.schiphol.nl/layouts/print_page.jsp;jsessionid=GWZ0fd02J33Ng8szZ14kx1KlP!1133093664!1180064116245?PORTLET%3C%3Ecnt_id=10134198673765538&FOLDER%3C%3Efolder_id=2534374302572265&ASSORTMENT%3C%3East_id=1408474395729234&VIRTUAL_TEMPLATE%3C%3Evt_id=10134198673763216&bmUID=1180064116328&bmLocale=nl#24
Progis	vingerafdrukherkenning	www.management-centrum.com/referenties/lz/
Kliniek Nijmegen	badgesysteem	http://www.sa-road.com/
Sportclub in Zuid Holland	Handgeometrie	http://www.sportaccent.nl/fitness.htm
Stichting Myosotis	Vingerafdrukherkenning	http://www.amdas.nl/docs/Procedures%20van%20het%20AMDAS.doc
Supermarkt in het midden van het land	vingerafdrukherkenning	www.suprema.nl
Technische hogeschool in het noorden van het land	vingerafdrukherkenning	www.suprema.nl
TICA	vingerafdrukherkenning	http://www.sa-road.com/website/new/download/tica_web_pdf.pdf
Tikkloksysteem (winprik)	vingerafdrukherkenning	http://www.winprik.be/NL/default.htm
Kinderdagverblijven Noord Brabant	vingerafdrukherkenning	http://www.kdv-dino.nl/
Toegang tot Evoswitch	gezichts- en vingerafdrukherkenning	http://www.evoswitch.com/nl/home
Verhuur autos	vingerafdrukherkenning	http://www.ad.nl/autowereld/2615276/Auto_huren_Vingerafdruk_afgeven.html
Video uitleen bedrijven	vingerafdrukherkenning	http://www.imp-media.nl/product_6.html
Voetbalstadions (pilot)	gezichtsherkenning	http://www.adodenhaag.nl/adodenhaag/nl/html/algemeen/kaartverkoop/huisregels/huisregels.pshe
Voetzoolherkenning Zwembaden	voetzoolherkenning	http://www.laupro.nl/dev/biometrie/zwembad/
Winkelcentrum Zuid Holland	gezichtsherkenning	http://www.unisys.nl/about__unisys/news_a_events/2005190801.htm en http://www.frankwatching.com/archive/2008/06/18/mobiel-rfid-nfc-bluetooth-biometrie-contact-op-maat/
Winkeldiefstal Amsterdam (proef)	gezichtsherkenning	http://www.loket.amsterdam.nl/loket/centralestad/product/71860;jsessionid=HP7gQ2wqZNGLfyLvJvLfbLzVvQyp0ywyQ2pH2hsLfS49c3QtKWSG!-1414646
Zorginstelling in het oosten van het land	vingerafdrukherkenning	www.suprema.nl

Zwembad Zuid Holland	gezichts- en vingerafdrukherkenning	http://www.de-fakkel.nl/index.php?content=website/news/news&id=47
Zwembaden Noord Brabant	vingerafdrukherkenning	http://spitsnet.nl/nieuws.php/1/3823/online/Bioscan_bij_vijf_zwembaden.html