FIDIS

Future of Identity in the Information Society

Title:	"D3.16: Biometrics: PET or PIT?"
Author:	WP3
Editors:	Annemarie Sprokkereef (TILT) Bert-Jaap Koops (TILT)
Reviewers:	Mireille Hildebrandt (VUB) Eleni Kosta (KU Leuven, ICRI)
Identifier:	D3.16
Type:	[Report]
Version:	1.0
Date:	20 August 2009
Status:	[Final]
Class:	[Public]
File:	fidis-WP3-del3.16-biometrics-PET-or-PIT.pdf

Summary

Biometrics plays a vital role in identity management. Biometric data are, however, sensitive and vulnerable, and there is a need to develop biometric applications as a privacy-enhancing technology (PET) rather than a privacy-invasive technology (PIT). Building on earlier FIDIS research, this report studies technical, organizational, and policy decisions in the development of biometrics applications that influence their becoming PETs or PITs. These decisions balance the interests of individuals to have control over their personal data against commercial, societal, and political interests, security, convenience, and efficiency. This report identifies criteria for determining the 'PET' content of technologies and looks at several case studies of decision-making processes in biometrics: biometric pseudonyms and iris recognition, Privacy Impact Assessments, voice recognition, the German ePass, and the Dutch central database of passport biometrics. These case studies suggest a possible gap between expectations and assessments based on technical knowledge and between economic and political expectations of and requirements for biometric applications. Based on this finding, recommendations are given to enhance awareness of privacy-enhancing technologies and to apply value-sensitive design in the development of biometric applications.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

- ***Goethe University Frankfurt*** Germany
- ***Joint Research Centre (JRC)*** Spain
- ***Vrije Universiteit Brussel*** Belgium
- ***Unabhängiges Landeszentrum für Datenschutz*** Germany
- ***Institut Europeen D'Administration Des Affaires (INSEAD)*** France
- ***University of Reading*** United Kingdom
- ***Katholieke Universiteit Leuven*** Belgium
- ***Tilburg University*** Netherlands
- ***Karlstads University*** Sweden
- ***Technische Universität Berlin*** Germany
- ***Technische Universität Dresden*** Germany
- ***Albert-Ludwig-University Freiburg*** Germany
- ***Masarykova universita v Brne*** Czech Republic
- ***VaF Bratislava*** Slovakia
- ***London School of Economics and Political Science*** United Kingdom
- ***Budapest University of Technology and Economics (ISTRI)*** Hungary
- ***IBM Research GmbH*** Switzerland
- ***Institut de recherche criminelle de la Gendarmerie Nationale*** France
- ***Netherlands Forensic Institute*** Netherlands
- ***Virtual Identity and Privacy Research Center*** Switzerland
- ***Europäisches Microsoft Innovations Center GmbH*** Germany
- ***Institute of Communication and Computer Systems (ICCS)*** Greece
- ***AXSionics AG*** Switzerland
- ***SIRRIX AG Security Technologies*** Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	09.03.2009	• template circulated (BJK, AS)
0.2	30.03.2009	• first contributions of all chapters (all)
0.3	09.04.2009	• edited version (AS)
0.4	15.06.2009	• revised chapters (all)
0.5	13.08.2009	• final draft version for internal review (AS, BJK)
1.0	20.08.2009	• final version (BJK, AS)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document.

Executive Summary	Bert-Jaap Koops, Annemarie Sprokkereef (TILT)
1 Introduction	Annemarie Sprokkereef (TILT)
2 Summary of earlier research findings	all authors
3 Concepts and Definitions	Annemarie Sprokkereef (TILT)
4 Technical decisions	
Introduction	Annemarie Sprokkereef (TILT)
4.1 Biometric pseudonyms and iris recognition	B. Anrig, E. Benoist, D.-O. Jaquet-Chiffelle, F. Wenger (VIP)
4.2 Privacy Impact Assessment	Martin Meints (ICPP)
5 Testing-stage decisions	
5.1-5.2 Centre Link and ABN AMRO voice recognition	Vassiliki Andronikou (ICCS), Annemarie Sprokkereef (TILT)
5.3 ePass	Stefan Berthold (TUD)
6 Political decisions	Annemarie Sprokkereef, Bert-Jaap Koops (TILT)
7 Conclusion	Bert-Jaap Koops, Annemarie Sprokkereef (TILT)

Table of Contents

Executive Summary

More and more applications rely on biometrics to authenticate or identify physical persons. Biometric data are intrinsically sensitive and vulnerable. If raw biometric data are misplaced, shared with parties that the owner does not approve of, or straightforwardly stolen, their owners have no choice but to have their biometrics removed from the system to avoid future fraudulent use. They have lost all advantages linked to this biometric in terms of convenience and security and this can not be repaired. Also with more sophisticated forms of biometric templates, revocability remains a major issue.

The use of biometrics in identity-management processes has been extensively studied in research of the FIDIS consortium and many others. Another line of research within FIDIS, as well as by many other groups, has been the study of privacy-enhancing technologies (PETs). This deliverable aims to build on both strands of earlier research, in order to study the precise 'PET content' of biometric applications currently in use or under development. PET in this context refers to a technology that protects personal privacy by minimizing or eliminating the collection and/or handling of identifiable biometric data. PETs can 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. The most far-reaching form of privacy-enhancing biometrics is the system-on-card construction, where biometrics are encapsulated in a personal device and do not leave this device. The second most privacy-enhancing measure is the match-on-card system, where 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. This means that the user still has to trust that the reader and the system do not store any templates.

However, biometrics can also be created in a more privacy-invasive way. We use the term 'privacy-invasive technology' (PIT) when referring to a technology that invades personal privacy by maximizing or creating the collection and/or processing of identifiable biometric data. An obvious example would be the storage of information in a manner where medical or racial information can be inferred; for instance, storing the raw template is privacy invading. This currently only occurs in basic biometric systems that are, except in forensic DNA data-bases, becoming outdated. Equally intrusive however is the use of individuals' biometric data to link their pseudonymity or identity between different applications, domains, and databases. Unnecessary privacy intrusion occurs when a biometric system is used for identification, where verification would already have met the objectives of the application. Finally, the use of biometrics for surveillance purposes seems inherently privacy invasive, since data subjects have no control, and sometimes also no knowledge, over biometric data being processed.

Several types of decisions in the development process of biometrics applications influence their becoming either PETs or PITs. These decisions are taken in the context of a complex process of balancing the interests of individuals to have control over their personal data and a series of other interests such as economic interests, policy and societal interests, security, but also convenience and efficiency interests. All these interests have a bearing on the use of biometrics and its relationship with data protection.

This report identifies a series of possible criteria that can help to determine whether maximization of privacy has been a major factor in decisions on the design and use of

biometric applications. These criteria are: obligatory or voluntary nature of the application, choice of biometric, authentication or verification function, multi-factor system use, personal control, access to biometric data, room for function creep, data quality, and interoperability, linkability and profiling.

With these criteria in mind, a number of case studies investigate the process of decision-making regarding various large-scale as well as small-scale biometrics applications. These case studies concern technical decisions made in biometric pseudonyms and iris recognition, using cryptographic techniques for privacy enhancement; technical and organizational decisions made if a Privacy Impact Assessment is conducted in the development of a biometric application; decisions taken during the test stage of voice-recognition applications and the German ePass; and, finally, political decisions made about the central storage of biometric data outside travel documents.

Together, these case studies show a differentiated picture of biometrics as PETs or PITs. New applications are developed and commercialized that are relatively privacy-enhanced, as the case study on biometric pseudonyms and iris recognition shows. However, as the two e-passport cases show, despite the technical possibilities, many biometric applications are turned into PITs. It is often assumed that the drivers behind PITs are commercial gain as a result of a significant market interest in information collection, or political, often surveillance-related, interests. Although these are major criteria in some contexts, they are by no means decisive reasons in many everyday contexts where biometrics are employed.

One of the questions raised by our research is therefore, why, despite the technical possibilities – such as biometric pseudonyms – so few biometric applications are used as PETs. Technical, organizational, policy, and political decisions turn out to have a major influence on biometrics often becoming PITs. One explanation is that in the information economy as well as in today's socio-political climate, the information-yielding potential of PIT applications seems to offer so many economic or political advantages that privacy arguments and PET alternatives pale in significance. However, another explanation is that there may be a lack of technical knowledge of privacy-preserving technologies at the stage where functional requirements for biometrics applications are specified, resulting in the creation of unnecessarily privacy-invasive biometrics.

The possible gap identified in this report between expectations and assessments based on technical knowledge and between economic and political expectations of and requirements for biometric applications is very relevant for the development of the information society, in which biometrics is playing an increasingly vital role in identity management. It is recommended that further research, encompassing more and different types of case studies, is conducted to refine the tentative finding of the PET/PIT gap between technically-informed and politically-based decisions.

In the meantime, it seems important that both public and private policy-makers become more acquainted with recent technical advances in the field of privacy-enhanced biometrics. Also, technical, organizational, and policy decisions should be more integrated, so that the development of biometric applications takes place according to the notion of 'value-sensitive design'. Increased awareness of the technical possibilities of PETs and the employment of value-sensitive design can lead to better informed and more balanced choices when developing biometric applications, and therewith reverse the trend that is tentatively found in this report of the various types of decisions leading to biometrics becoming PITs rather than PETs.

Abbreviations

AA	Active Authentication
ABN AMRO	Algemene Bank Nederland Banking Consortium
ART 29 WP	Article 29 Data Protection Working Party
BAC	Basic Access Control
BIR	Biometric Information Record
BITKOM	German Association for Information Technology, Telecommunications and the New Media
DoS	Denial of Service
EAC	Extended Access Control
EDPS	European Data Protection Supervisor
EURODAC	Central Database for the comparison of fingerprints (Dublin Convention)
FAR	False Accept Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
FTE	Failure to Enrol
HIDE	Homeland Security, Biometric Identification and Personal Detection Ethics
ICAO	International Civil Aviation Organization
MRTD	Machine-Readable Travel Document
OSEP	On-Line Secure E-Passport Protocol
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PIT	Privacy Invasive Technology
PKI	Public Key Infrastructure
PRIME	Privacy and Identity Management in Europe
PRISE	PRIvacy and SEcurity
RFID	Radio Frequency Identification

1 Introduction

FIDIS research has focused on biometrics in, amongst others, the following deliverables: D3.2. (Study on PKI and biometrics), D4.1 (structured account of approaches on interoperability), D7.10 (multidisciplinary literature selection), D3.10 (biometrics in identity management) and D13.4 (Privacy Legal Framework on Biometrics). In addition, some other European consortia have published recent research that provides useful insights into aspects of biometrics, such as BIOVISION, (especially the Roadmap for Biometrics in Europe to 2010), PRIME (Privacy and Identity Management in Europe), PRISE (PRIvacy and SEcurity) and HIDE (Homeland Security, Biometric Identification and Personal Detection Ethics).

This deliverable builds on all of the above studies and FIDIS reviews of technologies that enhance privacy (such as in *D13.1: identity and impact of privacy enhancing technologies*). Today's use of biometrics makes it very often a privacy-invasive technology (PIT), while there are ample possibilities, such as biometric pseudonyms, through which biometrics could be made into a privacy-enhancing technology (PET). The aim of this deliverable is to make a first assessment of the factors that play a role in policy decisions on biometric technology with privacy-invading and privacy-enhancing implications.

We have therefore studied various cases to assess their PIT or PET content. Biometric applications have been grouped into five categories or types in FIDIS deliverable D3.10, and this categorization has also been used in D.3.14.[1] We will categories individual biometrics applications in accordance with these categories, which we briefly repeat below. Although most biometric applications will belong to one specific group, it may occur that an application falls in two groups, for example the Centre Link and ABN AMRO voice recognition case studies fall in both Type II and Type IVb or IVc.

Type I: Government-controlled ID model

In this group, a public authority will take the initiative to collect the biometric data because of the identity verification or identification ability of the data, and include the data in an ID application, such as in ID cards, social security cards or passports. Control over the data could be central (Type Ia), divided over more than one organization but with appropriate agreements in place (Type Ib) or multilateral (without appropriate agreements for the disclosure or transfer of biometric data) (Type Ic).

Type II: Access control model

In this group, a public or private authority takes the initiative to collect the biometric data to secure the access to a physical place or an online application. Control over the data could be central or divided over more than one organization but with appropriate agreements in place (Type IIa and Type IIb) or divided such that the data subject shares the control (Type IIc).

Type III: Mixed model

In this group, the biometric data collected will be shared or exchanged amongst public and private authorities.

[1] Kindt & Müller 2007; Müller & Kindt 2009.

Type IV: Convenience model

In this group, either the data subject solely takes the decision to use biometrics for exclusive private convenience purposes (secure access to her house for authorized members) (Type IVa) or an organization uses biometrics for simplification of an administrative process with central or divided control (Type IVb and IVc).

Type V: Surveillance model

In this group, a public or private authority takes the initiative to collect and process the biometric data for surveillance purposes.

We will thus use existing FIDIS research to label specific aspects of biometric applications as being PETs or PITs. We start our report with a summary of earlier FIDIS research findings related to biometrics and PETs (Ch. 2), and will then provide a more in-depth analysis of the concepts and definitions at issue (Ch. 3). This lays the groundwork for a number of case studies, which are large-scale and small-scale examples of current biometric applications (Ch. 4-6). The survey of case studies leads to a first and tentative identification of key decision moments and factors in the adoption of biometric technologies in terms of their privacy-enhancing or privacy-invasive impact. We tentatively assess the intended or unintended role of technical and political decisions in determining who controls the biometric systems, their functionalities and their purpose (Ch. 7).

2 Summary of earlier FIIDS research findings

This deliverable builds on the findings of previous FIDIS deliverables, in particular the deliverables D3.2 and D3.6. First of all, basic terminology and biometric methods were introduced in the FIDIS deliverable D3.2, A Study on PKI and Biometrics.[2] This deliverable has also analyzed legal principles relevant for the use of biometrics and resulting technical and organizational privacy aspects. In the FIDIS deliverable D3.6, Study on ID Documents, the use of biometrics in the context of Machine Readable Travel Documents (MRTDs) has been analyzed with respect to security and privacy.[3] This work also included a description of ISO standards for biometric raw data and templates concerning machine readable travel documents. Nevertheless, each of the fore-mentioned reports discussed biometrics in a rather specific context, i.e. the use of biometrics in a Public Key Infrastructure and the inclusion of biometrics in MRTDs. Deliverable D3.10 continued on this path and updated the analyzes which have been made in the previous documents, and to place biometrics and its use in a broader context of use of biometrics in public and private applications, from government controlled ID applications to purely private convenience applications.

Biometrics is often used in applications to enhance the authentication and authorization of individuals, for example to obtain a travel document, or to access a building. If we look at the overview of the types of identity management systems as developed in FIDIS report *D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*,[4] we could reasonably say that it is likely that biometrics would most often be used in a *Type 1 IMS for account management* in order to enhance the authentication and authorization. Behavioral biometrics, i.e. the use of behavioral characteristics in biometric systems which may or may not identify a person and which will not be discussed in depth in this deliverable[5] could probably also be used in a *Type 2 IMS for profiling of user data by an organization.* Finally, as the strict borders between the types of IMS are disappearing, it is correct to say that biometrics will also emerge in *Type 3 IMS for user-controlled context-dependent role and pseudonym management*.

As already mentioned, D3.10 analyzed the deployment of biometrics from a technical, legal, security, organizational and forensic point of view in various applications and schemes for the management of identity and individuals in the public and private sector. It highlighted the security and privacy aspects of the use of biometric technologies, but also stressed the advantages which biometrics may offer. The deliverable concluded that the debate about the risks of biometrics should focus on where the control over the biometric system is exercised, and on the functionalities and purposes of the application. Besides that, attention should also concentrate on remaining research issues, such as health-related information in biometric data and revocability of biometrics. The document presented an approach on how to preserve privacy and to enhance security while using biometrics. The technical details of a biometric authentication process were described and illustrated in detail.[6] It was also demonstrated that

[2] Gasson et al. 2005.
[3] Meints & Hansen 2006.
[4] Bauer & Meints 2004.
[5] See for behavioral biometrics, Gasson et al. 2005, p. 82-90, and Hildebrandt 2009.
[6] Kindt & Müller 2007.

biometric data become an increasingly used key for interoperability of databases, without an appropriate regulation. To facilitate the discussion on biometrics, it was further proposed to make a classification of applications models which use biometrics, depending on differences in control, purposes, and functionalities. These application types, already explained in detail above, were the Type I – government controlled ID applications, the Type II – security and access control applications, the Type III – public/private partnership applications, the Type IV Convenience and personalization applications and the Type V – surveillance applications.[7] The distinction of the use of biometrics for verification and identification purposes was stressed and the research also showed that various technical aspects of biometric systems have not been taken into account in the legal treatment of biometrics. This results in a considerable 'margin of appreciation' of national Data Protection Authorities in their opinions on biometric systems, whereby the proportionality principle plays an important role.[8]

Finally, FIDIS deliverable D13.4 contained various country reports which illustrate that biometrics are not only applied in large-scale contexts and gradually entering daily life, but also that these biometric applications are often debated and criticized. Biometric data are in most cases personal data to which article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the data protection legislation apply. This legislation does not mention biometric data explicitly. D3.14 analyzed the gaps in the present legal framework and tackled the issues of the increasing use of biometric data in various identity management systems.[9] In six country reports, the spreading of biometric applications and the applicable legislation has been discussed. The reports – by tackling similar key aspects of biometrics - illustrate how the gaps in the general legal framework are handled and provide useful suggestions for an appropriate legal framework for biometric data processing. Of course, the D13.4 deliverable reviewed the fundamental right to privacy and data protection which shall be assured to individuals as well as Directive 95/46/EC which provides more detailed rules on how to establish protection in the case of biometric data processing. It concluded that the present legal framework does not seem apt to cope with all issues and problems raised by biometric applications. It showed that the limited recent case law of the European Court of Human Rights and the Court of Justice sheds some light on some relevant issues, but does not answer all questions. The analysis of the use of biometric data and the applicable current legal framework in the six countries demonstrated that in many countries position is taken against the central storage of biometric data. The reports show that privacy invading aspects of storage and the various additional risks of such storage are important considerations in decisions made. Although, in some countries the risks of the use of biometric characteristics that leave traces are discussed the deliverable concludes that controllers of biometric applications receive limited clear guidance as to how to implement biometric applications. Conflicting approaches are observed, and the deliverable clearly shows that current legislation does not always provide an adequate answer. It concludes with some specific recommendations to policy makers and the legislator. These recommendations focus on the need for the regulation of central storage of biometric data as well as for transparency of biometric systems.

---

[7] *Ibid.,* p. 60 *et seq.*
[8] *Ibid.,* p. 37 *et seq.*
[9] Only for specific large-scale biometric databases in the European Union, such as Eurodac, VIS, SIS II and the ePass, regulations containing specific but incomplete requirements for biometrics were enacted.

So, as a high-tech identification technology, biometrics has grown in maturity over the past years and is increasingly used for authentication in public and private applications. In general, research on biometrics has concentrated on the improvement of the technology and of the processes to measure the physical or behavioral characteristics of individuals for automated recognition or identification. Previous FIDIS research has not only analyzed these state-of-the-art techniques and their technical strengths and weaknesses but also the privacy and security aspects of biometric applications in use. In the context of the individual deliverables, various and complementary analyzes of the use of biometrics were carried out from a multi-disciplinary perspective. Biometric methodologies and specific technologies were analyzed and described,[10] and the deployment of biometrics in various contexts, such as in a Public-Key Infrastructure (PKI) structure or in Machine Readable Travel Documents have been researched and presented.[11]

This report builds on all the above studies and FIDIS reviews of biometric technologies that enhance privacy. The findings of these deliverables confirm that today's use of biometrics is mostly PIT, while there are possibilities such as biometric pseudonyms through which to create a PET. This deliverable makes a first step into finding out why this is the case. Therefore, a preliminary assessment of the factors that play a role in policy decisions on biometric technology is attempted. A distinction between technical and political decisions is made, and some criteria for assessing PIT or PET qualities are developed.

[10] Gasson *et al*. 2005, p. 62 *et seq*.
[11] Meints & Hansen 2006.

3 Analysis of concepts and definitions

3.1 Introduction

When it comes to the relationship between technology and the law, it appears that technology can enforce or enhance the law, but it can also help to evade legal rules for processing information. When it comes to technology and information management, a rule of the thumb is that without conscious intervention, information sharing and monitoring tend to be promoted more by technology than information shielding.[12]

In practice, as a particular information technology evolves, gradual adaptation to possibilities takes place. This has often resulted in a downgrading of the reasonable expectation of privacy in the past. 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. This may well be the phase in which we currently find ourselves in relation to the handling of biometric data.

Decisions about the use of biometrics as PIT or PET are taken in the context of a complex process of balancing the interests of the individual to have control over her personal data and a series of other interests such as economic interests, policy/societal interests: security, freedom and so forth. All these interests also have a bearing on the use of biometrics and the relationship with existing data protection legislation.

But what exactly do we mean by PET? Definitions of what constitute privacy-enhancing technologies differ considerable. A first important distinction often overlooked is between privacy-enhancing technologies and data security technologies. Data security measures are put in place to keep data safe, regardless of the legitimacy of processing. PETs seek to minimize or eliminate the use of personal data as a matter of principle, giving as much control as possible to the data subject. 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. Likewise, we use the term PIT referring to a variety of technologies that invade personal privacy by maximizing or creating the collection and/or handling of identifiable biometric data.

Herbert Burkert has first developed a typology of different PETs based on whether the subject, the object, the transaction, or the system forms the target of the privacy enhancing technology.[13] Subject oriented concepts seek to eliminate or reduce the capability to personally identify the acting subject. Object oriented concepts try to eliminate or minimize traces left by the objects of interpersonal transactions. Transaction oriented concepts seek to hide the transaction process and system oriented concepts seek to integrate some or all of the above. Charles Raab and Colin Bennett have argued that this classification is insightful but not very useful in assessing empirical examples.[14] Building on Burkert, they distinguish between systematic instruments, collective instruments and instruments of individual empowerment. Systematic instruments arise from intended and unintended decisions of the designers of systems. Collective instruments are created as a result of government policy.

[12] Koops 2009.
[13] Burkert 1997, p. 126-128.
[14] Bennett and Raab 2006, Ch. 7.

They are top-down applications where government or businesses consciously decide to build in privacy (or not). Instruments of individual empowerment are those where individuals can make an explicit choice with regard to their privacy. This classification of Bennett and Raab can be helpful in analyzing the PET or PIT decisions in the empirical biometric case studies in this deliverable.

A complicating factor is that 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) is often regarded as a contradiction in terms. When one accepts the notion that a person's biological characteristics form the core of a person's fundamental identity, then any use of physical characteristics is privacy invading by default. In this view, technical measures (systematic instruments) 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 (collective instruments) and security objectives. In this view, the desirability of the introduction of PETs as tools controlling individual biometric information (instruments of individual empowerment) should be challenged. PETs are regarded as being fundamentally at tenterhooks with the use of biometrics as an efficient instrument of public and security policy. From this perspective, perfect PETs may for example lead to technical and/or security inadequacies and prevent the straightforward track down of terrorists or fraudsters.

In this deliverable, the point of departure is that the use of physical characteristics in combination with IT is in itself not necessarily privacy invading, as long as the system offers adequate protection against unjustified or disproportional use of these data. As already concluded in FIDIS Deliverable D3.10 (concluding remarks) an extended legal, social, economical and technical analysis of both positive and negative effects of biometrics on privacy should always take place. As biometrics are unique, unjustified or disproportional use of data as well as theft of biometric data will have a negative effect on the roll out of biometrics in the longer term. In that sense, there is a strong common interest in using biometrics as PET where possible and at some point privacy and security issues overlap.

The definition used here of biometric PETs as 'biometric technologies that protect personal privacy by minimizing or eliminating the collection and/or handling of identifiable biometric data' can only become practically relevant once the concept of privacy has also been defined. Protecting personal privacy of course covers protecting personal information, but it clearly involves more than that. The literature on PETs as anonymization tools on the internet is a good classical example of this. The PET 'encryption' was set up as a personal privacy protection device. However, originally it was used to protect the content of messages, not the identity of the sender or receiver. Thus, the privacy enhancing capacity of the tool was not to anonymize (personal) details of the sender but to make the exchange of information that was taken place invisible for third parties. The tool was absolutely useless when it came to preventing that a third party could establish how often A was in contact with B. PET can therefore relate to safeguarding personal privacy both in the sense of personal information and personal identity. Of course, safeguarding personal privacy also covers safeguarding the *quality* of the information, such as the right (or the possibility) to correct or amend.

Control is therefore a very important concept in the assessment of levels of privacy achieved. As the biometric identification function cannot be performed without the use of a (central or de-centralized) database, 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.

It is also crucial to make a distinction between the protection of biometric data stored within systems and the use of biometrics by operators to safeguard authorized access to other types of data stored in a system. 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 (for example biometric operator access to a data bank). A further protection measure of this control function would be the use of a biometric in a multi dimensional or multi factor authentication situation.

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 (Bennett and Raab's notion of an instrument of individual empowerment). In the management of privacy, this individual control can take three forms: choice, consent and correction. The measure of individual control creates 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 this type of measures relating to biometrics is the system-on-card construction, where biometrics encapsulated in a personal device do not leave this device. As discussed in FIDIS deliverable D3.10,[15] performance may be an issue, and this biometric privacy enhancing architecture is currently an option for fingerprint and signature verification only. This is a totally self-containing system, keeping the reference and sample template on card as well as the matching process. There is therefore no opportunity to intervene with the card, except in the communication between the card and the card reader after matching. The second most far-reaching measure is the match-on-card construction. 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. This means that the user still has to trust that the reader and the system do not store any templates.

In assessing the exact meaning of the label 'privacy enhancing technology', and its relationship with control by the individual, it is helpful to make the distinction between the two concepts of 'privacy' and the 'management of privacy'. This distinction has first been developed by Tavani and Moore.[16] 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 (collective instrument in Bennett's and Raab's terminology) to refrain from creating databases of the biometric data contained in German passports. 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 biometrics as a control mechanism (PET) allows an individual a say in the trade-off between privacy and security in any particular circumstance (this corresponds with Bennett's and Raab's instruments of individual empowerment).

As a basis for an analysis of the privacy problems of biometrics problems of biometric

[15] Kindt & Müller 2007, section 6.2.2.
[16] Tavani & Moor 2001.

systems, earlier FIDIS deliverables (especially D3.2 and D3.10) have started from the issues which were described in the authoritative opinion of the Article 29 Data Protection Working Party (Article 29 WP) on biometrics.[17] The privacy problems identified have been subjected to further analysis in FIDIS report *D3.2: A study on PKI and biometrics*.[18] The overview of the privacy problems given in that 2003 working document of the Article 29 Working Party were presented in a useful schematic overview in Deliverable D3.10.

Privacy Risk	**Storage**	**Qualifying factors**	**Data Protection principle**	**Suggested remedy in Art 29 WP working document to counter risk**
Identification	Central storage	Size of database Type of biometrics used	Proportionality Art. 7	
Biometrics contain sensitive information (health, race)	Central (or local) storage		Prohibition to process sensitive data Art 8 Data minimization Art. 7	No images Use of templates which exclude such information
Secret capture and/or surveillance	Central storage	Especially vulnerable are low-level intrusiveness biometrics (e.g., face, voice), but also fingerprint, …	Fair collection and processing Art. 6 (a)	Local storage under control of data subject
Incompatible re-use (‘function creep’)	Central storage		Special risks to rights and freedoms Art. 20	Prior checking with DPA
Theft	Central (or local) storage		Appropriate technical and organizational security measures Art. 17	Appropriate security measures Including revocability of templates and impossibility to reconstruct biometric raw data from template
Use as unique identifier for connecting databases	Central storage	Use by governments	Conditions to be determined Art. 8 § 7 Right to object	Mathematical manipulations

[17] Article 29 Data Protection Working Party, Working Document on Biometrics, 1 August 2003.
[18] Gasson et al. 2005.

			Art. 14 (a)	
FAR/FRR	Central or local storage	Type of biometrics used	Prohibition of automated decisions Art. 15	Re affirmation of outcome, appropriate back-up procedures

Table 1. Overview of privacy risks of biometrics based on Art 29 WP Working document

Almost all of the privacy concerns in the table above, in fact relate to biometric Type I , II and III models as described in FIDIS Deliverable D3.10. The risks also relate most often to the place of storage of the biometrics: when biometric characteristics are stored in a central place, privacy risks increase dramatically. Despite warnings of the Art 29 Working Party in another (2005) working document[19] that setting up a centralized database containing personal data and in particular biometric data of all (European) citizens could infringe the proportionality principle, central storage developments can be detected. The arguments and privacy implications will be assessed in the case studies on the German and Dutch passport in this deliverable.

Based on the literature,[20] we will detail some basic notions of what constitute privacy enhancing and potential privacy invasive features of biometric applications here.

To integrate PET into the design of the biometrical systems there are basically two ways: decentralization of the template storage and verification and/or encryption of template-databases (in case of central storage). By decentralization 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.[21] In the case of EURODAC,[22] the PET aspect is the HIT-No HIT facility, where no information is exchanged except the mere fact whether or not there was a hit; however, in the case of a hit, biometrics are subsequently de-encrypted so that they can lead back to the other personal details of the person involved. As the whole point of these systems is to identify individuals

[19] Article 29 Data Protection Working Party, *Opinion on Implementing the Council Regulation (EC) N° 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 30 September 2005.

[20] Hes, Hooghiemstra & Borking 1999; Hes 2000; BECTA 2007; Koorn et al. 2004; Andronikou, Demetis & Varvarigou 2007; Wright 2007; Grijpink 2006.

[21] 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).

[22] On EURODAC, see http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33081_en.htm; see also Van der Ploeg 1999.

and link them to existing data, the use of a database and the possibility to link databases seems unavoidable.

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 in 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 already mentioned measure of 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.[23] Biometric cryptography is a privacy enhancing technical solution that integrates an individual's biometric characteristics in a one way or two way cryptographic key. The two way method now forms an integral part of all but the cheapest biometric applications on the commercial market. When the key is two way, 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**.** There are also applications that offer two-way verification and therefore integrate the 'trust and verify' security principle.[24] 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 of information in a manner where medical or racial information can be inferred. Storage of the raw template is privacy invading and only occurs in very basic biometric systems. The handling of raw data will soon become a relic of the past. New technologies have been developed both to improve the possibilities created by encryption and in overcoming the problems of false positives because of noise.[25] Equally intrusive is the use of an individual's biometric data to link their pseudonymity or identity between different applications or 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. Systems with central storage of raw biometric data or of templates can, depending on the specifications of the system, turn into 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 identifiability (thus privacy intrusion) as possible and they 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.

[23] This type of biometric application has been recommended by the FIIDIS consortium in report D3.14, see Müller & Kindt 2009.
[24] Many of these privacy-enhancing possibilities were already mentioned in the groundbreaking 1999 study on biometrics by the Registratiekamer, see Hes et al. 1999, p. 49-70.
[25] See, for example, www.priv-ID.com, and the iris case study in this deliverable.

3.2 A set of criteria to assess privacy-enhancing features

On the basis of these examples and the earlier FIDIS work, in this section we will describe a series of possible criteria that can help determine whether maximization of privacy has been a major determinator in decisions on the use of biometric applications. They are in a non-preferential order: obligatory or voluntary nature of the application, choice of biometric, authentication or verification function, Multi-factor system use, personal control, access to biometric data, room for function creep, data quality, and finally, interoperability, linkability and profiling.

3.2.1 Obligatory or voluntary nature

An important element in any assessment of privacy aspects of the use of biometrics is whether providing biometric samples is obligatory or voluntary for the individual concerned. If it is voluntary, 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, the use of a call center and passwords as an alternative to 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 realize 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 remain unused. In Type 1 government-controlled ID models involving biometrics in electronic documents, participation is more or less obligatory and individual consent and choice cannot play a role.[26] Theoretically, in the case of a biometric passports, there is of course the option of choosing not to apply for one, but this is not a serious alternative as the harm of not enrolling is substantial (in this case: not being able to travel outside the EU). When there is no real alternative to the use of a biometric apart from (social) exclusion, and this is the case with most public sector introductions of biometrics, the biometric characteristic has to be presented.

3.2.2 Choice of biometric to be presented

The second of the defining criteria is the choice of the biometric to be presented. The impact on privacy of the main biometrics used in commercial applications is diverse. This is summed up in Tables 2 and 3.

[26] See Introna and Nissenbaum 2009, p. 47, on the notion of meaningful consent.

Table 1. **Biometric summary table**

Biometric	Accuracy	Ease of use	User acceptance	Stability	Cost	Trans-parency[1]	Typical applications	Suitability for	
								1:1	1:N
Finger-scanning	High, possibly Very High	High	Medium Low	High	* to ***	Overt	Traveller clearance, driver's license, welfare	Yes	Yes
Hand geometry	High	High	Medium High	Medium High	***	Overt	Access control, traveller clearance, day care	Yes	No
Facial recognition	Medium High[2]	Medium High	High	Medium Low	***	Covert	Casino, traveller clearance	Yes	Potentially[3]
Iris scanning	Very High	Medium Low	Medium High	High	*****	Covert	Prisons, access control, traveller clearance	Yes	Yes
Retinal scanning	Very High	Low	Low	High	****	Overt	Access control, traveller clearance	Yes	Yes
Finger geometry	Medium	High	Medium High	Medium High	***	Overt	Access control, amusement park ticket holder	Yes	No
Voice recognition	Medium	High	High	Medium Low	*	Covert	Low security applications, telephone authentication	Yes	No
Signature verification	Medium	High	Medium High	Medium Low	**	Overt	Low security applications, applications with existing 'signature'	Yes	No

Table 2. Characteristics of different biometrics. Source: OECD 2004

Table 2. **Candidates and preferred technologies**

	Facial recognition	Fingerprint	Iris scan
Advantages	Public acceptability Ease of use Use of passport photo Useful for watch list	Mature technology High accuracy Stable over time Large extant database	High accuracy Stable over time
Disadvantages	Accuracy controversial Questions as to effects of aging over time	Low public acceptability	Very new technology Single vendor issues Not yet user friendly

Table 3. Advantages and disadvantages. Source: OECD 2004

As the FIDIS study on PKI and biometrics has shown,[27] from a technological and economic perspective, biometric applications chosen for authentication and verification depend on the following factors: quality (low false acceptance rates (FAR), tamper resistance and privacy compliance), Convenience (easy and quick enrolment, use and maintenance, low false rejection rate (FRR) and costs for the infrastructure needed. The study concluded that many questions with respect to the implementation of privacy criteria are still open from the perspective of currently available commercial solutions. To what extent biometrics collected now may yield privacy critical information in future, for example concerning health still

[27] Gasson et al. 2005.

needs a considerable research effort of which only economic gain or social government priorities can be the driver. The FIDIS PKI study has also made clear that the 'magic' triangle defined by (1) quality, (2) convenience and (3) costs is always a compromise with focus on one, or at best two factors, with the remaining factor(s) showing considerable weaknesses. As to the choice of biometrics, and international standards applying, such as fingerprinting, biometric methods and data used for forensic purposes have been highly standardized. Others suffer from lack of standardization such as face recognition and hand geometry. If quality is important in the choice of biometric, then one of the criteria to determine quality is privacy. Some technical features protecting privacy such as algorithms or templates formats may be subject to patents or copyrights, the privacy and convenience aspects and costs of using the iris for example, have been competing values.

3.2.3 Authentication or verification

Whether a biometric application is used for identification or verification is very relevant for an assessment of privacy enhancing options available. 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 maximize the control of the individual over her biological data. Most private biometric applications been introduced for verification purposes (mainly to grant authorized 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 integration of biometrics in electronic documents issued by the government, which is an application of the government controlled ID model (Type 1), presents privacy issues relating to the verification and authentication function. If biometrics are stored in central database, it is very likely that this database will be attacked at some point. The larger the database, the more attractive it will be for hackers and/or thieves to break into. Such attacks may have several purposes, one of them obviously identity theft. A second aspect to a central database is the possibility of function creep, which will be discussed below.

The use and storage of templates is only a very partial solution as templates can also be stolen, and once stolen, they could still be used by an impostor. Therefore, the use of biometrics to secure and authenticate in a reliable way through the use of uniquely encrypted templates has made so much progress. Once stolen, encrypted templates can be revoked and replaced. Although this does solve the storage problem of reference tokens, it does not solve the problem of leakage in the biometric processing from the capture to the comparison component. Decentralization of critical data, user control and encapsulation of the whole processing into a tamper resistant device are all technical measures that can be taken to minimize the risk.

To assess the place awarded to privacy in decision-making, an obvious method is to evaluate

the proportionality of the use and the used functionality of the biometric data. Biometrics will in general be used to enhance the security of an application. However, because of the risks associated with biometrics as explained above, in particular also in relation with the type of control that is exercised over the biometric system (central, divided, multilateral), the use of biometric data shall be carefully designed and biometric data will only be used in cases where no other means are available to guarantee the same level of security. Furthermore, for most applications, the verification function of a biometric system will do.

3.2.4 Personal Control

The advantages of biometrics are sometimes assumed known rather than spelled out. Obviously, biometrics remain an undeniably unique tool to link an individual to documents or claims and as such further technological development and efficient use of this new technology provide exciting options. The concept of encapsulated biometrics is often introduced as a method to make use of the advantages whilst minimizing privacy and security risks. According to this concept, the biometric data remain under the control of the data subject, and the data subject has increased decision powers as to when and for what purposes its biometrics are going to be used. To what extent does the individual retain control over their biometrics? By perfect use of biometrics in this sense, an environment is created in which data can be protected by the individual, including the possibility to prevent that data are used in a certain way, thus exercising powers of control, consent or even correction. This requires the sensor-on-card construction, where biometrics encapsulated in a personal device do not leave this device. To achieve this not only the data but also the sensor reading the data remains on the card. A match-on-card system is already less perfect, as although the data do not leave the card, the sensor reading the data is external, and therefore located outside the personal device or card, leaving more possibilities for data transfer outside the control of the individual.

In terms of individual control, the revocability of biometrics is important for all biometric models mentioned above, but it is clear that it is most crucial in the Type I government controlled ID model, where the use of the biometric identifier is mandatory for individuals in ID related documents. It is also important in the Type II a and b Access model and the Type III Mixed model, as the biometric can be used in different kinds of documents and tokens in relations with the government and/or private organizations for access purposes, e.g., to e-government services or commercial banking. If the biometric has been compromised and it cannot be revoked, the relations of the individual with the government and other concerned organizations will become severely damaged, if not impossible. Revocability is less of an issue for the Type IVa Convenience model, as an individual could in that case still choose to no longer use the biometric application (e.g., for access to the house, etc) or, in case the template is compromised, and cannot be replaced, change to another method for authentication. If the biometric system is compromised, the user may eliminate it from the authentication process. Revocability is intrinsically realized in Type IIc models ('encapsulated biometrics'), where the biometric template data is never accessible to persons other than the owner. A lost or out of date device incorporating such data cannot be abused as the data can technically not leave the device. Once a device that carries an 'encapsulated biometric' system is out of service, the stored biometric data is lost and thus revoked.

3.2.5 Multi factor system

Identity theft with the use of biometric information, especially of fingerprints, can take place

in many ways such as gaining access to a databank, theft of traces unknowingly left. In fact, biometric data cannot be used to secure or to authenticate because they can be intercepted easily. The strength of biometrics could be based on the fact that it provides a convenient piece of unique information that someone always has. However, as it will always remain subject to a risk of misappropriation, it should in a particular system be combined with other authentication information (such as a secret knowledge of an access number), as multiple authentication will render the system more secure and attack proof. The strengthening of the authentication procedure rather than the creation of an alternative and more reliable procedure should in fact be considered as a main purpose of use of biometric characteristics in private applications. As a solution to this problem, the use of biometrics in combination with additional, revocable factors of authentication such as possession or knowledge have been suggested in the late 1990s foremost by Cavoukian,[28] but it has since been taken up by other authors [13] and is held up as a relevant measure [14]. Nevertheless, many of today's systems do not implement biometrics in a revocable way. One example of this is the European passport.[17] The reason seems to be that currently no standardized and cost efficient solution is available that can be easily integrated into the various biometric systems.

3.2.6 Access to biometric data stored on RFID chip

The intended usage of the documents often determines their structure and limits their potential for including biometrics. Nowadays, travel documents are often no more than a paper booklet containing an integrated RFID chip with limited functionality; while the majority of the European national eID cards are smart cards with extended computational capabilities; e.g., many eID cards can be used to generate electronic signatures for strong authentication or to create legally binding signatures. Tamperproof smart cards offer more flexibility to include biometrics in a secure and privacy-friendly way than RFID chips.

Biometrics add security to applications because they provide a stronger link between the card and the card holder, thus between the physical and the electronic identity. Biometric data that are stored on a contactless chip need to be sufficiently secured in order to prevent unwanted disclosure of the data contained therein. FIDIS and other authors have strongly advocated the use of appropriate security measures to avoid tracking and eavesdropping of the personal biometric data stored on media which involve new technologies such as RFID.[29] This issue has become very important, because the use of a contactless chip has been agreed for the issue of the so-called e-passports, following the ICAO specification for Machine Readable Travel Documents in May 2004, and confirmed and mandated in the 2252/2004 Regulation. The vulnerability of the biometric data stored on the RFID chip has been proven by documented attacks on the e-passport in several countries, including Germany, the Netherlands, the United Kingdom and Belgium.[30]

---

[28] In several papers, Cavoukian held that the most important step to achieve privacy protection was to encrypt all biometric data, and to destroy all original biometric data, see for example, Cavoukian 1999.
[29] FIDIS, *Budapest Declaration on Machine Readable Travel Documents (MRTDs)*, Future of Identity in the Information Society, 2006, available on http://www.fidis.net. (Unless otherwise noted, all URLs in this report were last accessed on 10 July 2009.)
[30] For the first overview, see Meints & Hansen 2006.

3.2.7 Room for function creep

This brings us to the third criterion, the possibilities for function creep. The example of EURODAC illustrates the relevance of this criterion. Access to EURODAC, which serves as a system for comparing fingerprints of asylum seekers and illegal immigrants, has now been opened to law-enforcement agencies such as Europol. This permission also applies to those fingerprints that were provided by those seeking political asylum in the EU before this access for law-enforcement agencies was granted. This is an example of biometric identifier function creep. In many countries, controllers of private applications that store biometric characteristics can be forced to disclose biometric data when requested to do so by the appropriate legal authorities under criminal law. Existing literature on the European wide introduction of biometric technologies in the public sector shows that the core problem is that government demand is focusing on surveillance, control and fraud detection instead of security and risk mitigation. The general 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 when in public information management and law enforcement linking of data will be such an obvious policy goal.

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. Political or management decisions can be made regarding the use of biometric data to use the technology in a privacy invasive manner. Instances of function creep, such as the above mentioned example of the use of biometric data collected for immigration purposes used in the context of unrelated criminal investigations[31], 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 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 that for governments is difficult to resist. However, the tendency to use data for other purposes than they were originally collected for[32] can be observed in the public, but also in the semi-public and private domain. Strict legislation can make it more difficult for function creep to occur, but can never completely prevent it.

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

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

3.2.8 Data quality

One of the basic principles of the data protection legislation as set forth in Directive 95/46/EC on the protection of personal data is the data quality. The principle requires that the personal data must be '*accurate*, and, where necessary, kept up to date'; furthermore, 'every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified'.[33]

This legal requirement with regard to the data quality poses a problem for specific forms of biometric data which relate to a human characteristic that changes over time, for example, if the individual grows older. The reference biometric data relating to hand geometry or the face of younger persons, for example pupils of a school, at a certain point may not be of good quality anymore, as the characteristics change and these changes are not reflected in the reference data. This problem has been recognized in relation to the use of the facial image of children for the use of identity documents in a study performed for the Ministry of the Interior in the Netherlands in 2005. The report stated that 'it is very likely that facial recognition of children of twelve years or younger, on the basis of a reference image that is some years old, is problematic. The reason is the significant changes in the proportions of the characteristic points in the face during growth. These changes take place after a complex process that is to a large extent determined by the sex and genetic background'.[34] The data quality of the reference biometric data of younger persons (for example, under eighteen) is therefore a concern, not only from a practical point of view, but also under the data protection legislation, which imposes requirements for the quality of the data, in particular that the data shall be accurate. In some European countries, biometric applications have been promoted in schools or other environments involving children, for convenience and other purposes (for example the lending of books)[35]. Under some circumstances, reference data will need to be replaced at regular intervals with new reference data by a new enrolment of the data subject. If this would not be possible, the data shall not be used any longer and is to be erased. According to FIDIS Deliverable D3.14 the administrative and operational requirements for such replacement and the consequences of this principle is most important for the biometric Type I government controlled ID model; the importance remains but decreases in the biometric Type II Access model, the Type III mixed model and the Type IV convenience model.

Various privacy problems in relation to the quality of biometrics can also occur, such as the difficulties in achieving sufficient data quality or the fact that not only captured biometric samples but also the biometric templates may contain sensitive information about someone's health. There still is a lack of overview of biometric methods and related information about someone's health condition in captured biometric samples. One of the privacy problems that needs further investigating is the data quality of specific biometric data, such as face scan and hand geometry, for specific groups of people. It may well be that certain groups carry a higher risk of having inaccurate or outdated biometric data processed about them.

---

[33] Article 6.1 (d) of the Data Protection Directive 95/46/EC.
[34] BZK 2005.
[35] See, for example, the debate about the use of biometrics in schools in the United Kingdom, Müller & Kindt 2009 (country study UK).

3.2.9 Right to object

If biometrics are used by a private owner for access control purposes, e.g., to a place open to the public such as a health club or swimming pool, the public interest (securing (public) order) is often invoked, or the interests of the controller, outweighing the interests of the individuals.[36] Directive 95/46/EC states that especially if the processing is based on these grounds, the data subjects should have the right to '*object at any time on compelling legitimate grounds relating to his particular situation'* to the processing, unless the national legislation states otherwise.[37] Legitimate grounds could be the contention that biometric data include sensitive data, difficulties to enroll, or also religious belief.

The right to object, the principle of the right of individuals to object to the processing of data, shall be taken into account in the discussions about biometrics in the way that alternatives for use of a biometric system will always have to be provided. This will be especially true for the biometric Type II access models operated by a private organization. For biometric Type II access models operated by a government, e.g., for e-government services, the use of alternatives is feasible, though complicated and will cause inefficiency. The use of alternative means for biometric Type I government controlled ID models, will be more difficult still. It has to be accepted that biometric systems will never include all individuals to whom it might be directed, privacy enhancing applications will take account of this observation. Appropriate specifications as to when somebody is entitled to object to become enrolled in a biometric system can form part of a package of PET measures.

3.2.10 Direct identification ability, interoperability, linkability and profiling

In addition to the privacy threats and ethical concerns described above, biometrics might also raise concerns of linkability, disclosure of additional health information and unobserved verification or identification.

Templates, which are used for a specific application and stored on a local or central place, are often linked with other personal data such as name and address. In most cases, an individual is even unable to influence her biometric characteristics without harming herself. It is therefore difficult to deny or to hide biometric properties. For governments and identity management system operators, biometrics offer the unique possibility to authenticate individuals that are uncooperative and even to prove to an impostor her true identity (negative authentication). Biometrics is the only authentication concept with this quality. In a world where identity theft becomes a serious threat for whole populations, biometric properties become the crucial factor for secure authentication. The potential use of biometrics in this way inherently holds risks for the privacy and the social life of a user. The lifetime of a typical identity credential should be shorter or at least not exceed the lifetime of a typical identity record in an IMS of a biometric system. For biometric templates used as identity credentials, this is clearly not the case. Most biometric characteristics remain identical for a long time and some of the characteristics even remain unchanged for a full lifetime of a person. In addition, individuals have to use the same biometric characteristic as a biometric credential in many different authentication situations. A corrupted biometric credential can severely harm a person. There is naturally no revocation list for corrupted or out of date biometric characteristic and

[36] See Article 7(e) and (f) of Directive 95/46/EC.
[37] Article 14(a) of Directive 95/46/EC.

properties. Therefore biometric data should never run the risk of corruption or disclosure to non-authorized entities. As already discussed above, states and large organizations collect and store huge amounts of biometric data from their citizens or members in large databases. Nobody can guarantee that such data can be fully protected against attack. A further drawback of centralized databases is the limitation on scalability. Depending on the technology, biometric template databases have collisions between individual templates already with a few hundred or thousands of Biometric Information Records (BIRs). This can lead to confusion of persons with potentially dramatic consequences for innocent people. The choice whether or not to store centrally and to opt for technical possibilities for interoperability, linkability, profiling, sharing of data all have a bearing on whether biometric will actually be used as a PIT or PET.

3.3 Conclusion

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 other interests. This interest can be the need to provide security for society but also security or convenience of the individual concerned. Too much PET may cause an individual another type of invasion of privacy in the long term because she cannot be protected against the negative effects of identity fraud. PETs are only useful when integrated into the security of a system. Using revocable cryptography to store biometric data but leaving access to the database unsecured would be potentially privacy invasive. Proliferation of biometrics makes individual biometric data more accessible and more linkable to other personal data in principle. Responsible management and control of personal data does therefore not only stand or fall with using biometrics as a PET where possible. Without security of systems, sectoral boundaries, clear objectives, exclusion of function creep, delineation of the target group and external supervision, biometric data become vulnerable to abuse. These factors are therefore as important as the possible technical measures that maximize the privacy of the person providing biometric characteristics. Within the relevant constraints, the use of biometrics as PET can be stimulated and enforced. Some of the criteria affecting the potential of the use of biometrics as PIT or PET affecting privacy in biometric applications have been listed. In the following chapters, we will look at some concrete cases and decisions in more detail.

4 Early-stage decisions

4.1 Technical decisions: biometric pseudonyms and iris recognition

More and more applications rely on biometrics to authenticate or identify physical persons. Biometric data are intrinsically sensitive and vulnerable in today's applications:[38] if they are stolen, their owners have currently no choice but to revoke them (where possible) to avoid future fraudulent use. In doing so, they lose all advantages linked to this biometric in terms of convenience and security.

We present the general ideas of biometric pseudonyms, followed by a short presentation of the basic ideas of a technique which allows developing biometric pseudonyms – using the example of iris recognition – in order to overcome major threats for security, privacy and convenience in today's use of biometrics. The present approach has been studied in the BioCrypt project, which led to a patent in 2009.[39]

The project BioCrypt focused on deriving biometric pseudonyms from iris recognition images. A proof of concept has been implemented. Note however, that the main ideas developed and patented are general enough to be used for other biometric data as well, e.g. fingerprint.

In a similar direction, the EU project TURBINE[40] (TrUsted Revocable Biometric IdeNtitiEs) focuses on fingerprints and 'will hence provide the assurance that:

1. the data used for the authentication, generated from the fingerprint, cannot be used to restore the original fingerprint sample
2. the individual will be able to create different 'pseudo-identities' for different applications with the same fingerprint, whilst ensuring that these different identities (and hence the related personal data) cannot be linked to each other, and
3. the individual is enabled to revoke an identity for a given application in case it should not be used anymore.'[41]

These three points are also satisfied by our approach, as discussed below.

The central point is the creation of *biometric pseudonyms*. This first section, after reconsidering some general concepts of biometrics, describes what such pseudonyms are and why they are needed. The second section focuses on how they can be created, for example in the case of the iris. We consider the implications of this technology from the user's perspective. It also explains how our innovation seeks to offer all the benefits of iris recognition in terms of security and convenience while ensuring the privacy of biometric data and its related personal information.

---

[38] See also Gasson et al. 2005 on possible threats and attacks.
[39] Patent submission for European patent n. 08169061.2. For more information on BioCrypt, see http://labs.hti.bfh.ch/biocrypt.
[40] http://www.turbine-project.eu/.
[41] From http://www.turbine-project.eu/.

4.1.1 Biometrics and pseudonyms

4.1.1.1 Advantages and disadvantages of biometrics

There is little need to present here the complete list of advantages and of problems arising with the use of biometrics like for example iris recognition, as the main issues have already been discussed in the FIDIS project.[42] Biometrics enable the automatic recognition of human beings with speed and reliability. Applications as means of authorization are numerous, from physical access to buildings and rooms to logical access to services and computer resources. In the context of the information society, it makes the secure remote identification of citizens over a network possible.

Moreover, biometrics offer much convenience to its users. Passwords and PINs are easily forgotten or disclosed; keys, cards and tokens can be lost or stolen. Biometric traits, unlike secrets and possessions, accompany us wherever we go. We do not need to remember nor maintain them.[43]

Biometric technologies can facilitate life in many ways. For instance, you could go jogging with nothing more than your clothes on, buy some refreshment that you pay thanks to your fingerprint, then go back home and unlock your door through retina scan. Or, if you are a frequent flyer, you could save lots of time by bypassing immigration control and passport presentation if you are registered in a system for automated border-crossing using iris recognition.[44]

Yet, no biometric technology is perfect, i.e. achieves exactly 0% error rates. Every biometric system is only as strong as its enrolment process and can be the target of many attacks.[45] However, we will focus on how the use of biometrics can affect our privacy. This takes us to the next section.

4.1.1.2 Unlinkability of personal information

To understand the impact of biometrics on the protection of our private life, we have to realize how our personal digital information is collected and processed. The figure below depicts our identity as a set of attributes that characterizes us. Partial identities are subsets of these attributes that are known about us in different contexts (at work, when shopping, during leisure time, and so on). Some of this information is stored in a digital form in various databases.

[42] See especially Gasson et al. 2005 and Kindt & Müller 2007. See also *supra*, Ch. 2.
[43] Besides a few behavioral biometrics, e.g. signature or gait.
[44] This application is taken from Daugman's webpage at http://www.cl.cam.ac.uk/~jgd1000/.
[45] See e.g. http://www.iris-recognition.org/counterfeit.htm on the secureness of biometric systems.

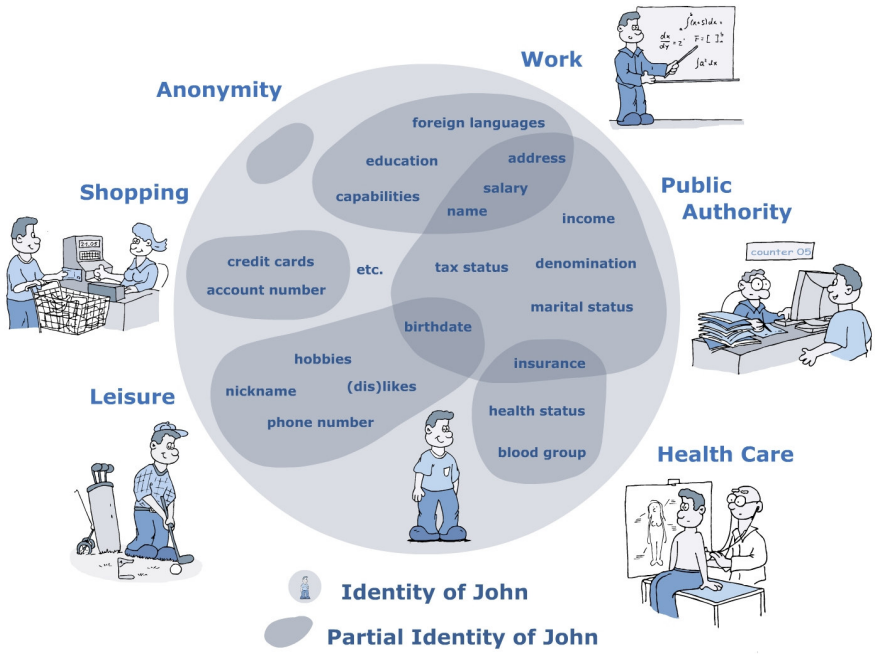

Figure 1. Identities and partial identities

Source: tutorial of the PRIME (Privacy and Identity Management for Europe) project, available at http://www.prime-project.eu/.

The key to privacy is choosing what personal data to disclose depending on the context[46] and knowing who knows what about us.[47] An important threat to privacy is the linking of some or all of our identity-related information without our consent or knowledge. As we can see in the figure above, most partial identities have one or more attributes in common. Mathematically speaking, linking grossly corresponds to the union of non-disjoint partial identities on condition that the elements at the intersection of these sets match.

Now some types of attributes can be more or less distinctive within a given group of persons, making it more or less difficult to link partial identities. For instance, our full name may unequivocally identify us within our family and company, but usually not within our country of residence, let alone the whole world. This is where biometrics come into play.

A biometric trait such as the iris can be potentially used like a globally unique identifier. This means that if we use the same biometric, say the right iris, in different contexts, then our corresponding partial identities could be univocally linked from a technical perspective.[48] This is possible because our iris is so discriminatory that it distinguishes us from the rest of mankind.

[46] Typically, a good strategy would be to reveal only what is strictly necessary in such a context.
[47] Cf. M. Hansen, "User-controlled identity management: The future of privacy", in Jaquet-Chiffelle et al. 2006.
[48] Of course, this depends on the interoperability of the possibly distinct implementations of all these applications. Note that we consider here only the technical feasibility, not the real likelihood.

4.1.1.3 Data protection and revocability

Another drawback of current iris recognition technology is related to data protection. Biometric templates that specify our iris structure patterns are vulnerable data. Unlike DNA, they do not reveal information about our genetic predispositions or, contrary to the belief of iridology,[49] our health status.[50] However, if they are stolen, their owner has currently no choice but to revoke them (when possible) to avoid future fraudulent use. In doing so, he loses all advantages linked to this biometric in terms of convenience and security. In general, '[t]here is the additional risk with biometrics that whereas other pseudonyms can be replaced from time to time which can make linkage more difficult, biometric ones are inherently associated with a physical person (thus cannot be changed) and once compromised can never be anonymised.'[51]

We can change password as many times as desired, but most people have only two irises and ten fingerprints. Once we have revoked both our irises, we are unable to use iris recognition anymore. It does not matter whether biometric templates are kept in a common database[52] or on separate smart cards.[53] Of course, local storage is preferable to centralized storage from a privacy point of view. But in both cases, sensitive personal data is stored somewhere and subject to theft.

Regardless, biometrics remain an attractive process due to its many advantages. So how can we turn for example iris recognition from a privacy-invasive technology (PIT) to a privacy-enhancing technology (PET)? Our solution based on pseudonyms solves all the above-mentioned problems.

4.1.1.4 Biometric pseudonyms

Etymologically speaking, a *pseudonym* is a 'false name' or an alias. For example, authors may use one or several pen names instead of their real name. However, a given pen name plays the role of a mask for its subjects[54]. The virtual person 'Ann Onymous' may be used by one physical person or shared by many different persons, or it could conceal a computer program.

The concept of *biometric pseudonym* takes back the idea of multiple aliases but it creates a strong link between the owner of some biometric trait and her pseudonyms. Thus, we can be confident that only one single physical person hides behind any biometric pseudonym. For instance, a particular iris may be linked to many pseudonyms but no biometric pseudonym

---

[49] Cf. the definition from Wikipedia, http://en.wikipedia.org/wiki/Iridology: "Iridology (also known as iridodiagnosis) is an alternative medicine technique whose proponents believe that patterns, colors, and other characteristics of the iris can be examined to determine information about a patient's systemic health. Practitioners match their observations to iris charts which divide the iris into zones which they correspond to specific parts of the human body" . But note also: "Iridology is not supported by any published studies and is considered pseudoscience to most medical practitioners" (ibid.).

[50] For a detailed discussion see Kindt & Müller 2007.

[51] Michison et al. 2004.

[52] Take for instance the screening database (watch list) of *persona non grata* on the territory of the United Arab Emirates.

[53] Like those of the eye-scan program for frequent flyers at JFK airport.

[54] See Jaquet-Chiffelle et al. 2006.

can be related to two physical persons. As enumerated in the previous section, iris biometric pseudonyms have to:

- Store no sensitive biometric data. We achieve this by using a one-way function for the computation of pseudonyms from the original template.
- Be as numerous as desired. Once we know how to produce one pseudonym, the process can easily be extended to create many distinct instances by the addition of a parameter. To each pseudonym, we associate a value such as a PIN or a service-dependent number.
- Be unlinkable to each other. There is no direct link between two pseudonyms of the same person: the only existing link is through the original iris. This is made possible by the parameterized one-way function, which means that brute force is the only possible attack, under the assumption that the one-way function is strong from a cryptographic perspective.
- Be revocable. As biometric pseudonyms are non-sensitive data, they can be simply revoked by adding them to a black list. A new pseudonym can then easily be constructed using a different parameter (e.g. a different PIN).

Note that these four points are just fully compatible with the three points of the EU project TURBINE mentioned above.

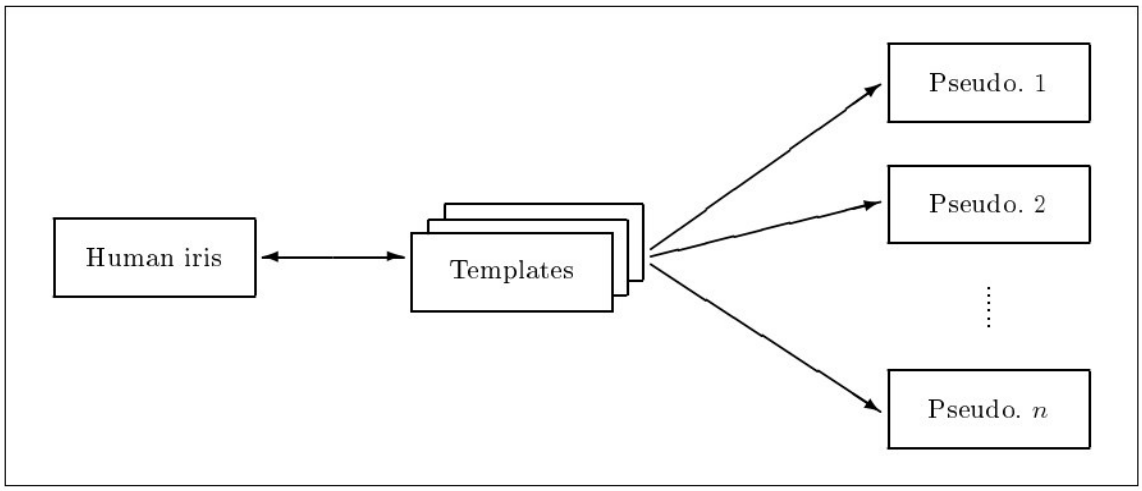

Figure 2. Biometric pseudonyms

As shown in Figure 2 , there are one-way links from a person's templates to its pseudonyms. The main difficulty is that, due to the imaging process, the same iris (and similarly all other biometrics) yields a different template every time (we have drawn three of them in Figure 2). In spite of this intra-class variation, we want to get constant pseudonyms. This is the big challenge.

On the other side, the interclass variation, i.e. the variation of pseudonyms which belong to different human iris, must be large enough to be separated from the intra-class variation mentioned above.

4.1.2 BioCrypt – Biometric Pseudonyms in the Example of Iris Data

The general processing steps of a biometric system have extensively been described for example in FIDIS deliverable D3.10 – see Figure 3.

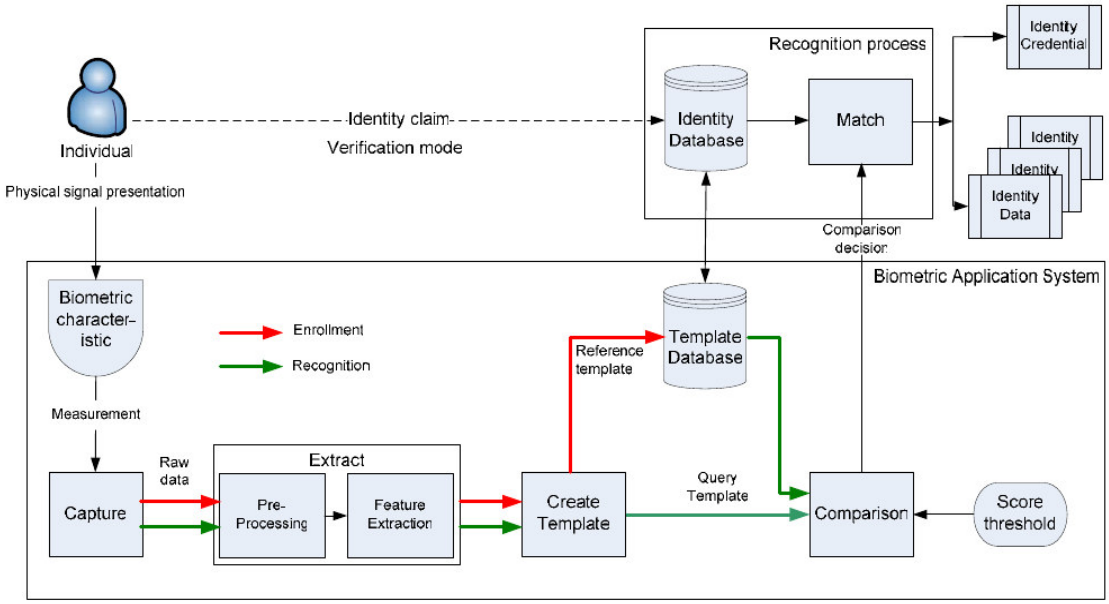

Figure 3. Overview of steps for a biometric system. Source: Kindt & Müller 2007.

In the following section, we will have a look at the image acquisition, i.e., how the physical appearance of the human (or other biometrically measurable entity) is done, followed by the template production and analysis, template matching as has been studied in the BioCrypt project (http://labs.hti.bfh.ch/biocrypt). We present the ideas only as a brief overview. The interested reader will find more information and additional links on the website mentioned.

4.1.2.1 Image Acquisition

In the process of image acquisition, there is no difference to the 'standard' approach, i.e., in fact all we need is an image of the iris, in a quite good quality, mostly done in near infra-red illumination 650-900 nm band. In our approach, we restricted ourselves to the use of available databases of iris images in order to avoid the administrative and technical problems of live image acquisition.

4.1.2.2 Template Production and Analysis

As in the 'standard' approach, we have to

- localize the iris ring within the eye, i.e. find the pupil and the outer limit of the iris,
- stretch the resulting image into a rectangle of normalized size which is done by transformation of polar coordinated into polar ones,
- apply 2D Gabor wavelets transform to extract the biometric features.[55]

An example with these three steps is shown in the next figure.

[55] See the project BioCrypt, http://labs.hti.bfh.ch/biocrypt, for a more detailed description.

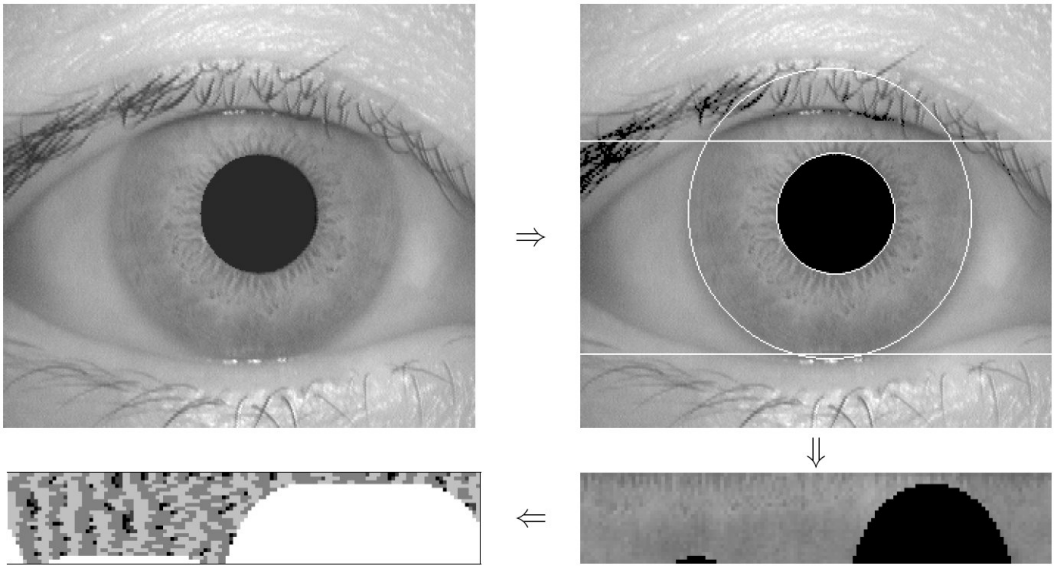

Figure 4: Template production

The challenge in this process is the determination of the valid parts of the image, i.e. the parts that really contain information about the iris and not the surrounding parts like parts of the eyelid or eyelashes. In actual live image acquisition, this problem can to some extent be eased by repeating the process until an image (or several) of acceptable quality is available. However in many cases no 'perfect' image of the iris is available and the further processing *must* be capable of dealing with invalid portions of the image. The simplest idea clearly is to consider only the intersection of the valid parts of the templates, yet one has to pay attention that enough information persists in this intersection.

Here, we do not distinguish between the enrolment phase and the recognition phase (cf. also Figure 3, where the paths in the figure are identical up to the template production). The typical difference between the two phases is only in the quality and eventually the number of the images taken, which is of minor interest here.

4.1.2.3 Template matching (verification vs. identification)

In verification, there are two (or more) templates available, and the algorithm determines whether the templates match or not. In identification, we look for the one template in a set of templates which matches best the template provided. In both cases, there is a matching algorithm which must compute distances between pairs of templates. Here for the discussion of our approach, we do not distinguish between verification and identification because all we are interested in for the moment is the matching algorithm.

Such a matching algorithm can clearly not test on equality of the templates only because different influences (from the environment) may augment the variation of the image of the iris, like different equipment (camera), rotation of the iris, eyes more or less closed (hence different validity zones), etc. Typically, the Hamming distance is used for computing the bitwise difference of two templates, but this is clearly dependant on the size, position and rotation of the iris.[56] In the simplest case, rotation can to some extent be circumvented by

[56] For a general discussion of how to recognize irises of different sizes, positions or orientations, see Daugman 2004.

adding some shifting to the templates.

4.1.2.4 Iris biometric pseudonyms

Consider a simple pseudonymization algorithm first. As mentioned, iris recognition relies on a measure of *similarity* derived from the Hamming distance. Two biometric templates are claimed to describe the same iris if their Hamming distance is sufficiently small, i.e. if they are similar enough.

Now let us consider a simple algorithm for pseudonyms generation involving the SHA-256[57] hash function. Instead of storing whole templates, we save only 256 bit hash codes. We can create as many pseudonyms as needed by appending some parameter, like a PIN, to a template before hashing it.[58]

This promising algorithm enables both pseudonymization and privacy protection. Yet, we have two problems to solve:

- Due to the avalanche effect, if one bit of the input flips, about half of the output bits flip. This means that, in order to obtain the same hash code, we should have absolutely identical templates, which is practically never the case. We have to find a prior transformation that turns same-class instances into a unique class archetype.
- We have to deal with the varying proportion and location of valid biometric data inside a template. Invalid areas cannot be compared or equated to valid information. Therefore, instead of replacing the Hamming distance similarity measure with a single *equality* check, we suggest to run multiple equality tests on various valid parts of the template.

For dealing with the first problem, we focus on error-correcting codes (ECC) which are designed to deal with the errors that can happen during the transmission or storage of data. Their basic idea is to add redundancy to data before sending it over a communications channel or saving it on a storage medium.

When the data is subsequently received or read, it is possible to detect whether some errors have occurred or not. In the case of transmission, the receiver can either restore the original message by correcting these errors or request the transmitter to resend the data.

In the case of storage, a simple example would be the tenth and last digit of the ISBN-10 number which is computed from the first nine digits. This check digit enables detection when a symbol has been altered or two adjacent symbols have been inverted; strictly speaking this is an error-detecting code which can only detect but not correct the error(s). Likewise, redundancy checks can be performed through parity bits, checksums or CRCs.

Error-correcting codes have numerous applications for storage on high density media (e.g. CDs, DVDs), and communication over noisy channels or with limited power resources (e.g. GSM, space probe). Note that their performances are restricted: errors of some type can always be corrected while other errors can only be detected. Finally, a third kind of errors cannot be detected at all.

---

[57] See http://en.wikipedia.org/wiki/SHA1. Note that in principle, any reliable hash function can be considered for this application.

[58] Similarly, this can be done using Message Authentication Codes MAC, see http://de.wikipedia.org/wiki/Message_Authentication_Code.

So here in the context of biometric pseudonyms, we have the problem caused by intra-class variation, also called biometric fuzziness: how can we extract a constant string out of the variable template of a given iris? On the other hand, the problem of error correction is to find back a codeword by removing the noise that has affected it.

The fundamental idea of applying ECC to biometrics is that these two problems are similar. Instead of developing a new technique to solve the first problem, we choose to reuse the solution to the second one. However, this solution needs to be slightly adapted.

We can see ECC decoding as a kind of geometric projection in a discrete space whose points are the strings of some length. The codewords of a given code are a subset of these points. Each codeword has its own decoding region which contains all the points that are always decoded as – projected onto – this codeword. In the case of nearest neighbor decoding, the decoding regions are centered at their respective codeword.

Thus, decoding a so-called received word consists in finding what decoding region contains it and projecting onto its center codeword. The received word is always accurately corrected if the codeword is affected by an error of weight smaller than half the minimum distance between distinct codewords.

Traditional ECC decoding works because any sent word is a codeword and is therefore at the center of a decoding region. Now what happens if we try to decode biometric data? The result will be unsatisfactory because sent words will not necessarily be codewords anymore. For this reason, the decoding process must be adapted.

Each time we measure a biometric trait, we get a different template. The collection of all possible templates for a given iris can be viewed as a cluster of points whose center is a random point in some space. The problem is that the cluster points are spread in different decoding regions. This means that they will be decoded as different values, whereas we want to get always – or, at least, most of the time – the same value for a given class.

If we could find the cluster center, we could perform a simple translation in order to center the cluster around some codeword. But as we know only a few points of the cluster at the time of enrolment, we can merely compute an imprecise estimate of the cluster center. Yet, we have no other option.[59]

For application to biometrics, a further question is then which ECC should be chosen? Different requirements from its application to biometrics, like the code, length, dimension, distance, transmission rate and especially the error correcting rate impose that the 'right' ECC is a matter of compromise.

For the second problem mentioned above, namely that we have to deal with the varying proportion and location of valid biometric data inside a template, we no longer use the whole template as is, but zones selected from it. We call zones the portions of biometric data used for the recognition of iris templates. For convenience, we decide to use rectangular shapes within the (horizontally) circular template domain. Zones can loop horizontally, but not vertically, inside the stretched iris ring. A zone is hence a (non empty) rectangle in the template space. Figure 5 below shows the template domain and two zones (A, B) along with the definition of the axes and the zone parameters. Notice the location of zone B which loops horizontally. These zones will be the regions of interest instead of considering the whole

[59] See the project BioCrypt, http://labs.hti.bfh.ch/biocrypt, for a more detailed description.

template.

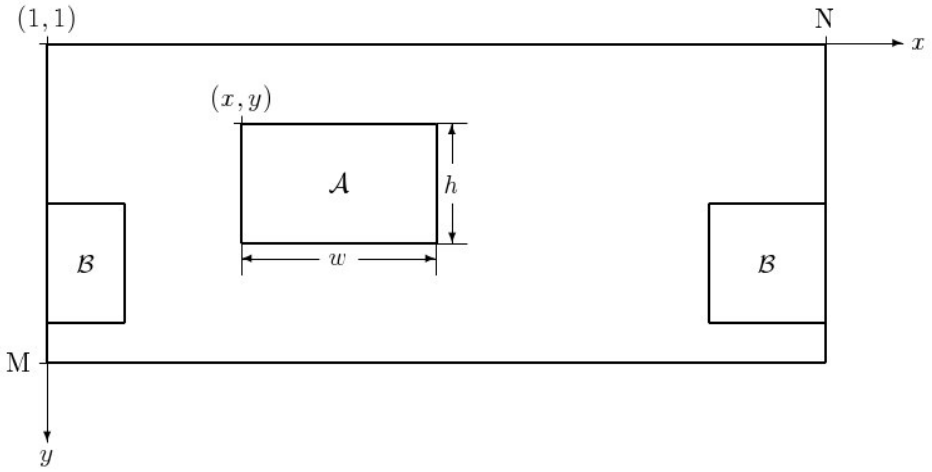

Figure 5. Template domain

A major question, then, is which zones should be considered and how to compare different templates using these zones. Without getting into too much detail, all we do is select a (sufficiently big) number of zones of 'good' size in the enrolment phase and compare them then in the verification phase with zones of same size in the presented template. This is to be combined with the process of using error-correcting codes mentioned above. Clearly, this induces some computational overhead, which can be limited to a reasonable extent in an acceptable way.

So finally, all that needs to be stored for each enrolment is a set of data items which are the result of zones of the templates having been first processed using error-correcting codes, then combined with some PIN and finally hashed. The combination of these techniques allows to satisfy all requirements we have mentioned above, hence biometric pseudonyms are available.

4.1.3 Conclusion

The presented approaches do not solve all problems of biometrics, but address especially the concerns raised in FIDIS deliverable *D3.10: Biometrics in identity management*, how templates 'could be rendered unique by encryption in such way that if the (uniquely) encrypted biometric template is stolen, it could be rendered useless (much like revocation of a PIN).'[60] The presented approach using error-correcting codes together with zones of templates is one possibility for successfully providing this, as our a proof of concept implementation has shown.

To our knowledge, there is no commercial product implementing privacy-enhancing iris recognition. But two companies offer similar products based on fingerprints: Philips priv-ID[61], and GenKey[62] that coined the term 'biocryptics'. The solution made by priv-ID creates anonymous and revocable biometric identifiers that can be e.g. printed as barcodes or stored in RFID chips, which implies a verification scenario. Further, as already mentioned, the EU project TURBINE focuses on fingerprints as well.

---

[60] Kindt & Müller 2007.
[61] http://www.priv-id.com/.
[62] http://www.genkey.no/.

4.2 Organizational and technical decisions: Privacy Impact Assessment

4.2.1 Introduction

For the evaluation of the impact of biometrics on privacy and data protection internationally two methods are established:

1. the Privacy Impact Assessment (PIA) and
2. a Data Protection compliance check.

Both methods result in a list of suggested or required technical and organizational measures. In this chapter the lists resulting from the application of both methods will be compared. The result of this comparison is of interest especially for vendors that have an interest to sale a biometric system on the international market.

4.2.2 Privacy vs. data protection

First of all when comparing different methods one needs to clarify their targets. The term 'privacy' is referring to at least four different types of privacy:[63]

- *information privacy* referring to the way private or governmental institutions handle Personal Identifiable Information (PII),[64]
- *privacy of communications* including e.g. the privacy of correspondence,
- *physical or bodily privacy* referring to the way under which conditions and how a body search may be carried out or body samples (e.g. DNA) may be used, and
- *privacy of personal behavior* referring to the freedom of action as long as freedoms of others are not touched or restricted.

Data Protection is focused on the protection of *personal data*, a concept defined in Art. 2(a) of the Data Protection Directive 95/46/EC[65] and recently further clarified by the Art. 29 Data Protection Working Party in the Working Paper 136.[66] In short, there is not much difference between the concepts of PII and personal data. European data protection legislation is focused on information privacy and partly covers privacy of communications.

As in the context of this study the European perspective is of most interest, we will focus on the types of privacy mapping with the targets of the European Data Protection legislation.

4.2.3 PIA – Background and Methodology

The PIA is a formalized privacy risk assessment method that was developed in the mid-1990s. Early descriptions of the method and guidelines for its application date back to 1998.[67] Since the early 2000s the method is adapted by the authorities responsible for privacy protection (in

[63] See e.g. the Privacy and Personal Information Protection Act of 1998 from the state of New South Wales in Australia, http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/pnsw_03_ppipact.
[64] In this context Personal Identifiable Information (PII) is understood as defined in the OECD *Guidelines on Protection of Privacy and Transborder Flows of Personal Data* from 1980, http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
[65] Accessible via http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.
[66] See http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.
[67] Clarke 1998.

many cases the Privacy Commissioners) in a number of countries, among them Australia[68], Canada[69], New Zealand[70] and the United States[71]. Typically the national implementations of PIA come along with a guideline or handbook, referring especially to the national privacy protection legislation and varying in concreteness with regard to the privacy risks to be covered. One of the most detailed descriptions and guidelines for the application of the methodology is provided by the Federal Privacy Commissioner of Australia.[72] The description of PIA in the following section is based on the Australian guideline.

All handbooks and guidelines investigated agree in the phase of the life cycle of procedures and products (plan, build, run or operate) the PIA best is applied: The application in the planning phase is recommended in general.

4.2.3.1 PIA – Description of the methodology

The PIA results in a privacy impact report, a document that can be compared in its structure with a security concept. In this report the results of the steps one needs to run through in the context of PIA are documented. In this way the reports show always the same structure. The five steps to be documented are:

1. Project description (description of governmental and business procedures including the ICT used);
2. Mapping the information flow (description of the data flows focused on PII);
3. Privacy impact analysis (core step, documenting the results of the privacy risk assessment);
4. Privacy management (analysis whether the procedures from a privacy point of view could be improved);
5. Recommendations (list with technical and organizational privacy protection measures).

For the core step 3 a standardized questionnaire is provided. It includes a list of relevant privacy risk related and explained questions:[73]

- Is compliance to privacy legislation given?
- Do individuals have to give up control of information about themselves to any degree?
- Will the project require, or is it likely to result in, individuals changing their behavior (e.g., having to present identification in more circumstances), or incurring costs?
- Will the project impact disproportionately on individuals or groups without identity documentation?
- Will decisions that have consequences for individuals be made on the basis of the personal information handled in the project (e.g., decisions about services or benefits)?
- Does the project deliver the right amount of accurate and relevant information to adequately inform these decisions?

---

[68] See e.g. http://www.privacy.gov.au/publications/pia06/mod-f.html and http://www.cic.gc.ca/english/DEPARTMENT/atip/pia.asp.
[69] See e.g. http://www.privcom.gc.ca/pia-efvp/index_e.asp.
[70] See e.g. http://www.privacy.org.nz/privacy-impact-assessment-handbook/.
[71] See e.g. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf.
[72] See http://www.privacy.gov.au/publications/pia06/index.html.
[73] Cf. http://www.privacy.gov.au/publications/pia06/mod-f.html and http://www.cic.gc.ca/english/DEPARTMENT/atip/pia.asp.

- Is there provision for complaint-handling mechanisms, in the event that privacy breaches eventuate?
- Have emergency procedures been devised in the event that the system fails?
- Is there provision for audit and oversight mechanisms, including emergency procedures in the event that the system fails?
- Does the project include the potential for function creep (e.g., might there be an interest in using the personal information collected for the project, for other purposes) or other unplanned consequences?
- Assess the value of the information to unauthorized users (e.g., is it information that others would pay money or expend effort to gain access to)?
- Is any intrusion (physical or on property) or surveillance (whether covert or overt) fully justified and proportional to the outcome?
- Is it the only way of achieving the aims of the project?
- Is it done in the least intrusive manner?
- Is it subject to legislative or judicial authority?
- How consistent is the project with community values about privacy (e.g., does it involve new ways of identifying individuals, the creation of significant databases or the use of genetic material or information)?
- How has privacy been factored in the project's cost-benefit analysis, and the analysis of the project's return on investment?

The PIA is generally applicable within as well as outside Europe – the first question in the privacy risk assessment provides the connection to national or regional legal requirements. This may include European data protection legislation. Differences in legal regime concerning data or privacy protection, for example the sectoral approach of privacy protection legislation outside Europe vs. a broad applicability of data protection legislation in Europe can be addressed by PIA this way.

4.2.3.2 Application of PIA in the context of biometrics

Since the late 1990s and early 2000s PIA has been applied to biometrics by various authors, among them the Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian,[74] the Federal Privacy Commissioner of Australia, Malcolm Crompton,[75] Roger Clarke,[76] and consultancy companies.[77] Recent updates concerning the results of the privacy risk assessment, especially recommendations, are available.[78]

The recommendations by the authors for a privacy aware or privacy compliant application show a certain variety, as the evaluation of the same set of risks leads to different conclusions. This has quite a number of reasons of which the following seem to be the most important:

- Differences in the legal grounds concerning privacy protection.
- Differences in the results of the evaluation for different biometric methods such as fingerprint recognition, face recognition or genetic fingerprinting.

---

[74] See Cavoukian 1999b.
[75] See http://www.privacy.gov.au/news/speeches/sp80notes.doc.
[76] See http://www.rogerclarke.com/DV/Biometrics.html.
[77] See for example the International Biometrics Groupe, LLC, New York, with the BioPrivacy Initiative, a PIA based consultancy approach, http://www.bioprivacy.org/.
[78] See e.g. Cavoukian & Stoianov 2007 and Curtis 2006.

- Progress in research concerning threats and vulnerabilities of biometric systems as well as progress in privacy protection measures.

4.2.4 Comparison of PIA with a Data Protection Compliance Check

As already explained the recommendations resulting from the application of PIA show a certain variety. This is also true for the results of the data protection compliance check. In addition to the reasons mentioned for PIA, considerations concerning proportionality are important.[79] A comprehensive comparison on the recommendations level would lead to highly case-specific results. However, a more general comparison concerning the coverage of both methods concerning specific privacy / data protection risks can be carried out relatively easy, based on the references cited above in section 4.2.3.2. In addition, selected, mostly general and not case-specific recommendations are used to make the comparison more concrete. Concerning data protection compliance, the recommendations are taken from various documents.[80] The results are summarized in Table 4 below (with our comments in brackets).

Privacy Risk related Question	Data Protection Principle	Coverage	PIA-based Recommendations	Data Protection Recommendations / requirements
Do individuals have to give up control of information about themselves to any degree?	Legitimacy principle (including fairness, and appropriate legal grounds) National concept of informational self-determination	The legitimacy principle includes to a large extent the control issue. In some European member countries the aspect of control is covered more explicitly, e.g. in the context of the fundamental right to informational self-determination.	Decentralized storage of reference data recommended. Mechanisms for anonymous enrolment and de-enrolment should be provided. Use encapsulated biometrics where possible.	Legal grounds such as legislation or effective consent required. Decentralized storage of reference data recommended. As a consequence verification is preferred over identification. Use encapsulated biometrics where possible.
Will it require, or is it likely to result in, individuals changing their behavior (e.g., having to present identification in more circumstances), or	Integral idea behind the principle of informational self-determination. (Data subjects should not need to change	Behavioral control is not directly covered by data protection. In most European member countries specific	Biometrics should not be used hidden and for surveillance purposes.	Biometrics should not be used in surveillance scenarios unless allowed by specific legislation.

[79] See e.g. Müller & Kindt 2009.
[80] Gasson et al. 2005; Kindt 2007; Meints 2007; the Working Paper 80 of the the Art. 29 Data Protection Working Party (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf); and the WhitePaper *Datenschutz in der Biometrie* issued by TeleTrust e.V. (http://www.teletrust.org/uploads/media/Datenschutz-in-der-Biometrie-080521.pdf).

Privacy Risk related Question	Data Protection Principle	Coverage	PIA-based Recommendations	Data Protection Recommendations / requirements
incurring costs?	behavior due to fear of surveillance or tracking.)	legislation exists, covering behavioral control e.g. at the workplace.		
Will the project impact disproportionately on individuals or groups without identity documentation?	Proportionality considerations, transparency principle	Full mapping	Disclosure policies[81]	
Will decisions that have consequences for individuals be made on the basis of the personal information handled in the project (e.g., decisions about services or benefits)?	Regulation on automated individual decision making Legitimacy principle: For each step of processing (collection, decision making) permission by law or consent is necessary.	Partly mapping; as semi-automated individual decisions are legally possible unless not restricted by other legislation; data protection offers no privacy risk assessment in these cases.	Biometrics need to be used responsibly in policing.	Automated individual decisions are prohibited. Legitimacy principle: For each step of processing (collection, decision making) permission by law or consent is necessary.
Does the project deliver the right amount of accurate and relevant information to adequately inform these decisions?	Transparency principle	Full mapping; however when personal data is used, the processing needs to be transparent for the data subject.		Art. 29 DPWP, Working Paper 100 and national data protection legislation
Is there provision for complaint-handling mechanisms, in the event that privacy breaches eventuate?	Data subjects rights Security safeguards	Data protection exceeds complaint handling suggested in PIA as the data subject has the right for request handling in any case, not only	Security incident handling, and breach notification in certain cases	Process and management for the handling of requests of data subjects required, security incident handling implicitly required (state-of-the-art in security)

[81] BioPrivacy Application Impact Framework, accessible via http://www.bioprivacy.org/.

Privacy Risk related Question	Data Protection Principle	Coverage	PIA-based Recommendations	Data Protection Recommendations / requirements
		case, not only cases of privacy breaches.		
Have emergency procedures been devised in the event that the system fails?	Security safeguards	Full coverage, though security safeguards are not very specific concerning availability. National legislation may be more specific compared to the Data Protection Directive 95/46/EC.	[No specific guidance for biometric systems.]	[No specific guidance for biometric systems.]
Is there provision for audit and oversight mechanisms, including emergency procedures in the event that the system fails?	Security safeguards, Data protection control mechanisms on a national level	Mapping is quite complete.	Internal audits, third party audits, Privacy Commissions / authorities Security incident handling	Internal audits e.g. to be carried out by data protection officers Data Protection Commissions / authorities Security incident handling
Does the project include the potential for function creep (e.g., might there be an interest in using the personal information collected for the project, for other purposes) or other unplanned consequences?	Finality principle (purpose binding principle) Data minimization	Mapping, though in countries outside Europe a certain degree of function creep might be acceptable.	Check for unplanned consequences including function creep. The scope of the biometric system should be limited and published. Biometric reference data should not be used as unique identifier. A privacy risk rating covering commonly used biometrics is available.[82]	Legal prohibition, e.g. to use additional information included in biometric reference data.

[82] BioPrivacy Application Impact Framework, accessible via http://www.bioprivacy.org/.

Privacy Risk related Question	Data Protection Principle	Coverage	PIA-based Recommendations	Data Protection Recommendations / requirements
Assess the value of the information to unauthorized users (e.g., is it information that others would pay money or expend effort to gain access to)?	Technical and organizational measures to enforce finality, PET, data minimization	Full mapping; though methods to assess the privacy / data protection risk may vary, the results are quite comparable.	Biometric reference data must not be used as identifier (early requirement). Templates should be used instead of biometric raw data. Mechanisms for template protection, e.g. Biometric Encryption	Use of templates instead of biometric raw data Mechanisms for template protection, e.g. Biometric Encryption
Is any intrusion (physical or on property) or surveillance (whether covert or overt) fully justified and proportional to the outcome?	Covered in other legislation outside data protection, e.g. the protection of the home and communication (E.C.H.R.)	Physical privacy is not covered by data protection	Rules how biometric samples, e.g. DNA, should be taken, rules on surveillance in homes.	Rules how biometric samples, e.g. DNA, should be taken, rules on surveillance at workplaces and in homes [both rules not based on data protection].
How consistent is the project with community values about privacy (e.g., does it involve new ways of identifying individuals, the creation of significant databases or the use of genetic material or information)?	Proportionality: Is the processing of personal data proportionate in relation to the purpose?	Proportionality considerations seem to cover community values about privacy largely.	[See examples above.]	[See examples above.]
How has privacy been factored in the project's cost-benefit analysis, and the analysis of the project's return on investment?		Economic considerations concerning privacy are not directly included in European data protection legislation. However, data protection seals[83] are available on a	The BioPrivacy Application Impact Framework[85] provides concrete guidance how privacy could be factored, based on (qualitative) technology acceptance considerations.	Economic considerations with respect to data protection are not covered in a mandatory way by data protection legislation.

[83] See e.g. https://www.datenschutzzentrum.de/guetesiegel/index.htm.

Privacy Risk related Question	Data Protection Principle	Coverage	PIA-based Recommendations	Data Protection Recommendations / requirements
		available on a national and European[84] level.		

Table 4. Comparison of PIA with a Data Protection Compliance Check

4.2.5 Summary and conclusion

The result of the comparison between PIA and a data protection compliance check shows that there are not many differences in the resulting general recommendations or requirements concerning privacy and data protection of biometric systems.

Data protection provides a binding legal framework for the application of biometric systems where data protection legislation is applicable. Flexible evaluations are possible based on proportionality considerations.

PIA uses a qualitative privacy risk assessment method that is similar to the qualitative method for information security risk assessment described in ISO/IEC 27005. The privacy risks to be covered can be described in standardized questionnaires, covering relevant classes of privacy risks. PIA covers a larger area of risks for individuals, as certain aspects of privacy in communication, bodily privacy and behavioral privacy are not covered by data protection legislation. Flexible evaluations are possible by assessing the possible impact and the likeliness of occurrence of a privacy incident for specific application scenarios of biometric systems. Recommendations generated using PIA are binding only in cases where legal grounds require the implementation of privacy protecting technical and organizational measures.

PIA can be used to include European data protection legislation in the compliance requirements. A qualitative risk assessment using PIA may also generate indications concerning proportionality considerations in the context of a data protection compliance check.

In any case, a PIA carried out for a specific application scenario of biometric systems provides a valuable ground for a data protection compliance check in European member countries. However, to comply with European data protection legislation, specific and mainly organizational requirements such as prior checking, reporting requirements etc. need to be taken into consideration in addition. That PIA assesses a larger area of risks for individuals not covered by European data protection legislation may result in various welcome additional recommendations, even if are as a matter of course these are not based on binding rules.

[84] See http://www.european-privacy-seal.eu/.
[85] Available via http://www.bioprivacy.org/.

5 Testing-stage decisions

5.1 Centre Link voice recognition

Centre Link conducts a pilot project aimed at testing replacing the client number and password system with a voice recognition system. Centrelink is an Australian Government agency within the Human Services portfolio that offers services such as job search assistance, childcare and social security benefits including unemployment payments, pensions and family assistance packages, whereas it oversees international pension payments.[86] This agency offers its services to more than 8 million customers. Access to Centrelink is provided through:

- 401 Centrelink offices around Australia;
- a Web site, which currently processes 1.6 million enquiries a year;
- a central call center, which receives approximately 28 million calls a year;
- mobile and remote-link services based in rural areas and the regions, including social workers, farm support and financial information.

The demand on Centrelink call centers has been increasing over the past years, posing a strict need for new measures to be taken for the reduction of the call waiting of citizens as well as demand on front counter staff and improve the quality of services offered, including fast and convenient access to Centrelink services. Moreover, given the nature of the services provided, identity and authentication comprise critical issues. Towards this direction Centrelink introduced the Interactive Voice Recognition (IVR) phone services.

Centrelink has been investigating the incorporation of voice authentication since 2002, but was quite reluctant to introduce this technology into their systems due to its immaturity, its non-readiness for large-scale deployment and the great effort required to enable the handling of the agency's strict security protocols. However, given the recent advancements in the biometric technologies and voice authentication techniques in particular and after a long close cooperation with the telecommunications provider Telstra, it has developed a voice authentication system which will be used for the authentication of the Centrelink customers over the phone via their voiceprint, replacing this way the client number and password. Currently this system is on active trial including 10 Centrelink employees in order to evaluate and ensure its stability, robustness and performance according to the system requirements. However, the agency is planning to extend the trials involving general public for larger-scale evaluation and more accurate refinement.

This speaker verification system is built for semi-complex two-factor authentication (to Australian Government Authentication Framework standards).[87] Based on this system the user is requested to answer to one or two pre-recorded secrets in order to offer to them access to the system and their account. Thus, every customer must have her identity verified through the voice authentication system before being granted with the permission to access her personal accounts. Through the Centrelink services every two weeks 200,000 customers provide their earnings mainly through the communication with a live operator. The incorporation of voice authentication into the Centrelink system aims at improving the

[86] http://www.centrelink.gov.au/.
[87] http://www.w3.org/2008/08/siv/Papers/Centrelink/w3c-sv_multi-vendor.pdf.

workload management within the system by offering faster customer serving. However, it should be noted that the incorporation of speaker verification functionalities into the Centrelink system mainly focuses on the enhancement of the security aspects of the system (authentication) and not of the user interface.

5.2 ABN AMRO voice recognition

Voice verification in telephone banking was selected by the ABN AMRO bank as one of its areas of investment and development in the early 2000s. 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.[88] The biometric application falls under Type IV: Convenience model. It is a combination of the data subject solely taking the decision to use biometrics for exclusive private convenience purposes (easy banking when there is an alternative available) (Type IVa) and the ABN AMRO bank using biometrics for simplification and increased security of an administrative process with central or divided control (Type IVb and IVc).

The ABN AMRO bank carried out an extensive 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.[89] This project was technically very successful and as competitors were not at all in a position to introduce voice recognition within the near future, so the bank seemed on course to gain 'a first mover competitor advantage'.[90]

Nevertheless, the project was put on hold in 2008 after a takeover by Fortis, Royal Bank of Scotland and Banco Santander. Official statements stated that a changing company strategy and a wider need of re-assessment of the cost of the overall project portfolio formed the background to this decision. The decision had nothing to do with a re-assessment of the benefits and advantages of the project. 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 is 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, an equal error rate of below 1% has been achieved, exceeding security and performance criteria, even without the additional security of a second factor such as a security question. In addition, from an end user point of view, speech is an intuitive and natural technology. The bank was attracted to the notion that voice or speech recognition only uses spoken words, and it is generally regarded less intrusive than systems that rely on scanners or other devices. Despite considerable costs, the system chosen would also allow for alternative arrangements, leaving the choice whether or not to participate in voice recognition to the individual bank customer. Therefore, the voice recognition fitted into the bank's wider strategy to been seen to generate and maintain high levels of customer trust and protection of customer privacy.

Analyzing the factors that played a role in the decision whether or not to proceed with voice

---

[88] 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).
[89] For details, see http://www.findbiometrics.com/Pages/voice%20articles/vvabn.pdf.
[90] For the factors determining the choice for voice recognition and the full strategy and short, medium and long-term outlook of the bank, see Frost & Sullivan 2006.

recognition in the magic triangle scheme:

- The project scored high on quality and convenience and the cost factor seem not to prevent the project from becoming fully operational. The privacy and security advantages of voice recognition were regarded as being so high, that no alternative biometric applications were regarded a viable alternative.
- Then after the takeover, the cost of the project suddenly halted the project for the time being, despite the fact that the quality and convenience factors both scored high.

In conclusion, this case study about the decision-making process regarding the use of an biometric application in a commercial environment provides some interesting data. If we were to ask the question whether organizations have some inherent interest in privacy, we find a few answers here. Drivers to protect privacy can be found, for example, in fear of reputational damage and increased business awareness of the strong link between protecting privacy and protecting security. Another driver to protect privacy in this case study is clearly the need to generate trust with (potential) customers and to show good corporate practice as being an innovative and modern bank. In the short term, privacy considerations may have been given so much weight, that, due to the changing circumstances at the bank, the chosen system invested in could not be put into operation. Cheaper, less privacy enhancing solutions, probably also carrying higher security risks, were not adopted as viable alternatives. The choice to allow other forms of telebanking to continue (voluntary nature of the application), the choice of biometric (voice), opting for multi-factor system use (two-factor authentication), insistence on data quality investment (expensive procedure to make sure that enrollment quality was maximal) and even the very limited options to use the biometric data for profiling, all added to the cost of the voice recognition application. All in all, this resulted in the roll-out of voice recognition being put on ice.

5.3 The ePass

Privacy and security features of the German ePass have been discussed in previous FIDIS deliverables. *D3.6: Study on ID Documents*[91] contains a study with focus on the recommendations of the International Civil Aviation Organization (ICAO)[92] and on the first generation of security features of the ePass, such as Basic Access Control (BAC). The deliverable particularly outlines threats of tracking citizens by means of weak authentication, static IDs, and passive biometrics. It also outlines threats of data leakage because of an inappropriate choice of key parameters for encryption and thus for confidentiality.

Measures for mitigating these shortcomings have been proposed in part in the ICAO recommendations, for instance Faraday cages to suppress unwitting communication, but have not or rarely been adapted by identity document issuers.

D3.10: Biometrics in identity management[93] complements the study by an analysis focused on biometrics and security features of the second generation, such as Extended Access Control (EAC). The deliverable particularly outlines threats arising from biometrics stored in central databases and summarizes alternative solutions, such as template-based authentication where the actual biometric data is (stored or acquired and) evaluated on a trusted device, such as a

[91] Meints & Hansen 2006.
[92] See http://www.icao.int/.
[93] Kindt & Müller 2007.

smart card. Deliverable D3.10 also refers to biometrics as a measure to ensure privacy when used in an authorization framework. This, however, requires that authorization by means of biometrics can be done without raising new privacy threats just from using biometrics. In most cases, this requirement is not fulfilled.

In addition, with the Budapest Declaration on Machine Readable Travel Documents (MRTDs), the FIDIS network released a review of the ICAO recommendations for MRTDs.[94] The ICAO recommendations have been adapted to electronic ID documents in the EU. The Budapest declaration contains a set of recommendations for short-term, mid-term, and long-term actions to be taken in order to improve MRTDs in the future. These recommendations most prominently include the limitation of the purpose to borderline control.

Electronic ID documents (or MRTDs) are more and more entering into the live of European citizens. The German government recently decided to introduce electronic identity cards starting from 2010.[95] It will contain a set of biometric images and templates, similar to the European passport.[96] In contrast to the recommendations in the Budapest declarations, the electronic identity card will not be limited to the purpose of borderline control, but deliberately open to a range of purposes; explicitly mentioned are eGovernment and eBusiness.[97]

At the same time, the current security measures such as BAC and EAC are better understood due to formal verification,[98] and new security measures are proposed and implemented[99] in order to overcome the weaknesses discovered in the current protocols. A comprehensive security analysis of these new protocols will be subject of future research.

In this case study, we will abstain from repeating the work in the previous deliverables and instead briefly survey recent work that appeared since 2008, i.e., since Deliverable D3.10 was published. We summaries findings about formal security analysis, recent protocols developments for new documents such as the German identity card, and their security evaluation.

5.3.1 Terrorist detection and the change in identity documents

The motivation for introducing MRTDs can be understood as the approach to address the gaps in current border control procedures that were made obvious during recent terrorist attacks. Apart from the question of whether expectations to secure the authentication by means of biometrics can be satisfied or not, a change in border control procedures has been performed. While the threats arising from the introduction of MRTDs have been recognized in scientific publications as well as in public media, the nature of the change is often blurred in the arguments.

---

[94] FIDIS, *Budapest Declaration on Machine Readable Travel Documents (MRTDs)*, Future of Identity in the Information Society, 2006, available at http://www.fidis.net; ICAO 2008.
[95] Gesetzesbeschluss des Deutschen Bundestages: Gesetz über Personalausweise und denelektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften. Deutscher Bundestag, Drucksache 32/09 vom 23.01.2009, http://dip21.bundestag.de/dip21/brd/2009/0032-09.pdf.
[96] Reisen 2008.
[97] Bender et al. 2008; Reisen 2008.
[98] Pasupathinathan et al. 2008a.
[99] Bender et al. 2008.

Koc-Menard analyzes the nature of the change and identifies three trends:

1. 'a move away from evidence-based detection to rule-based discovery'
2. 'a move away from observation of actual human behavior to the analysis of electronic traits', and
3. 'a move away from national discovery systems to multinational structures.'[100]

The first trend is the reason for building up of large knowledge bases, from which indicators of terrorist activity can be derived. Then, instead of interpreting actually committed activities of citizens, the indicators are matched against personal data in order to quantify the threat that is arising from the data subject. Rule-based detection systems, however, have a serious drawback, they may fail with false positives and false negatives. This can be compared with a human that is guessing and improves by time and observation. The systems need to learn from their mistakes as well to improve the rules, i.e., making the rules match the reality better. However, rule-based systems will never reach the perfect set of rules, since the reality dynamically changes over time and the systems, thus, need to adapt all the time.

The second trend makes it necessary to make as much personal information electronically available as possible. The identity is not longer determined by what you are, but rather by what you show. This raises the question of how easy it would be to show a different identity, pretend to be someone else, and thus the entire question of identity fraud. For automatic detection of terrorists, people need to be stuck to their identities. That is why biometrics is included in modern MRTDs.

The third trend most nobly supports the interconnection and collaboration in terror prevention across countries and beyond political borders. The back side of the medal is, however, that this is a fail-safe way to implicitly trade legislation whenever not explicitly regulated, for instance all those countries that do not definitely export their data protection regulations will implicitly import a mixture of the most liberal regulations of the other countries. At the end of his analysis of the current trends, Koc-Menard raises the question whether rule-based terror prevention systems would be the end of privacy. He concludes that this is not the case, since it would be possible as well to apply rule-based terror prevention to small sets of personal data and good guesses, just as it currently is with the human-driven border controls. The challenge would be to find a set of appropriate size and meaning.

5.3.2 Formal Analysis of MRTD Security Measures

Pasupathinathan et al. have published a formal security analysis of BAC, ActiveAuthentication (AA), and EAC.[101] As to BAC, the result is (not surprisingly) a formal verification of known shortcomings. In particular, the man-in-the-middle attack was successfully verified by means of model checking. The AA protocol, in contrast, works perfectly as expected and secure, but only as long as BAC can be assumed to work securely. The model checker shows that AA can be compromised, once the weakness against replay attacks of BAC is exploited. Then, an attacker can gain possession of the session key and decrypt the transferred data. Besides, an attacker would be able to authenticate to the reader as a genuine passport. By combining the weaknesses of both, BAC and AA, it is even possible to create a copy of the

[100] Koc-Menard 2009.
[101] Pasupathinathan et al. 2008a.

passport. This would indeed be a considerable step towards identity fraud. It is also possible, to masquerade as a genuine reader by exploiting the knowledge of the session keys. This way, it is possible to make the chip authenticate an arbitrary reader. Pasupathinathan et al. also point out that random nonces are necessary for the BAC and AA to work properly. Nonces without enough entropy[102] enable the attacker to perform cipher-text with known partial plain-text attacks. In the long run, that might lead to the disclosure of the session key. This is particularly an issue, since key freshness and key integrity cannot be assured (as outlined in the previous paragraph) and MRTDs use to have a relatively long validity compared to the time frame in which the attacks can be performed. In addition, it is not very likely that a device of so limited resources like an RFID chip may be capable of generating high-quality nonces. Thus, the reader might be the only source of appropriate entropy, whereas the reader is not authenticated and thus not a trustworthy device in the stage when the nonces are required. This opens up the entire bandwidth of skimming and snooping attacks.

After that, the same authors have provided an informal security analysis of EAC.[103] EAC makes use of certificates for assuring integrity of the reader. The main criticism is the use of a Public Key Infrastructure (PKI) for the certificate management and the time management for deciding when a certificate is outdated and thus the corresponding reader not trustworthy anymore. The Entropy can be understood as a quality measure for randomness. The more entropy a nonce generator provides the less is it predictable. PKI is a tree-shaped data structure where the root certificate must be trusted and consequently all certificates which are signed with the root certificate are trusted as well. Any trusted certificate can serve as a root certificate in a subtree. Thus, the path from the trusted root certificate to a certificate which is used for the reader authentication can be arbitrarily long. In order to verify the certificate, it is necessary to verify all certificates in the certification path to the trusted root certificate. Thus, the entire path must be available in the MRTD chip which raises two questions, (a) how will the MRTD get all required certificates, and (b) how much time is needed to verify the entire path? As to the first question, there is a simple solution in EAC, that is they have to be transmitted. This, allows indeed to transmit arbitrary certificates in order to perform a Denial of Service (DoS) attack. The solution of the second question can be used for an attack on the limited resources of the MRTD. If it takes too long to verify the path of certificates (perhaps because of limited computing power), it will not be tolerated by neither of the parties, the citizens and the border control officers. The problem with an accurate time management is closely related to the problems with the PKI. Due to the lack of an internal clock in MRTDs, the current time can only be estimated. This is a problem, since the less accurate the time is the worse can outdated certificates be identified and rejected. The time in MRTDs is estimated from timestamps of recently evaluated certificates. However, if the MRTD is rarely used, the internal time estimation of the MRTD would be 'stepping behind' the real time. Thus, actually outdated certificates can be accepted as long as the MRTD does not receive a certificate with an up-to-date timestamp.

5.3.3 German electronic identity card

The German electronic identity card will be issued starting from 2010. Like the electronic passport, the identity card will contain a Radio Frequency Identification (RFID) chip with

[102] Entropy can be understood as a quality measure for randomness. The more entropy a nonce generator provides the less is it predictable.
[103] Pasupathinathan et al. 2008b.

biometric data stored on it. Thus, the identity card will be capable of serving the same functionality as the electronic passport, unfortunately without any new security measures. This makes the identity card a fully featured MRTD, but the passport application is only one among others. The identity card will contain additional applications for eGovernment and eBusiness,[104] which will be implemented by an additional authentication function and functionality for the qualified electronic signature.[105]

The broadened application area of the identity card raises questions about the confidentiality of personal (and biometric) data stored on the MRTD.[106] However, the blueprint of the identity card includes a clear separation between the applications. The biometric data which is stored on the chip will only be available to the passport application, and thus just for the purpose of borderline control. The other applications will have access on the name, address, and validity of the MRTD.[107]

5.3.4 Protocols beyond BAC and EAC

In parallel to their formal analysis of the security protocols of MRTDs, Pasupathinathan et al. propose a replacement for EAC, the On-Line Secure E-Passport Protocol (OSEP).[108] With OSEP, the authors particularly tackle the questions of (a) confidentiality, (b) the freshness and authenticity for messages, and (c) possibly exploding computation complexity induced by certificate verification. In addition, OSEP uses a similar PKI structure as proposed in the ICAO standards. Thus, the authors argue, it would be easy to adopt OSEP into already implemented MRTD infrastructures. Instead of verifying large trust paths in the PKI, however, OSEP uses flat hierarchies in order to avoid DoS attacks. The back side of this protocol is the requirement to be online for authentication. This allows new attacks over limited network resources, but the overall evaluation is positive over currently applied protocols such as EAC.

5.3.5 Conclusion

The German passport remains, due to weak security, a privacy-invasive technology. The lacking security, particularly with respect to confidentiality, leads to the thread of unwittingly giving away personal data about biometric features. Recent works verify in a formal manner that security leaks exist in BAC and even in EAC. Most of these leaks are known since years and have been demonstrated in experiments. The communication protocols, however, only protect the communication between MRTD and reader. It is likely that new weaknesses appear in the data handling implementation of MRTD. Particularly, the implementation of an appropriate source of time is still subject of research. In addition, the current specification of EAC requires the MRTD to write data to persistent internal memory.[109] This and the resource limitation of MRTDs leads to the well-known question, namely how to balance optimized memory management and secure functionality.

In the case of the upcoming German electronic identity card, we observe that additional

[104] Bundesministerium des Inneren 2008; Reisen 2008.
[105] Bender et al. 2008.
[106] Roßnagel et al. 2008.
[107] Kindt & Müller 2007.
[108] Pasupathinathan et al. 2008b.
[109] Pasupathinathan et al. 2008a.

services have been incorporated in order to provide one device for several application areas. This seems to contradict the recommendations of the FIDIS Budapest declaration. However, according to the specification,[110] these new services have no access to the biometrics stored on the MRTD for the passport application and the user interface of the new applications differs in several ways from the passport application. The main difference is probably that the user is required to activate the new functionality with a PIN. Thus, it will be transparent to the user when it is not the passport application she is going to use.

[110] Bundesministerium des Inneren 2008; Reisen 2008.

6 Political decisions

6.1 Biometrics, the New Passport Act and a Dutch Central Database

Since 2006, all Dutch passports are issued as a biometric passport with an RFID chip embedded for storing the face scan. Two finger scans will be added from the end of September 2009 onwards. In addition, an amendment[111] to the Passport Act enables the storage of four finger scans in a central data base, the Municipal Vital Records (*Gemeentelijke Basisadministratie*), on top of two finger scans on the chip in the passport itself. The storage of the biometric fingerprint data on a central database is not a requirement of the EU Directive but a decision that has been specifically left to the member states. The Dutch amendment to its Passport Act goes against the FIDIS D3.14 recommendations on the regulation of central storage of biometric data as well as for transparency of biometric systems.[112] On 20 January 2009, the Dutch Parliament (Second Chamber) passed the amendment with a majority formed by the parties PvdA, VVD, ChristenUnie, SGP, CDA, PVV and the independent MP Verdonk. The Senate Commission for Home Affairs (BZK/AZ) published a report on 24 March 2009,[113] which received a ministerial reply on 28 April 2009.[114] The Senate (First Chamber) then passed the new Passport Act in June 2009. In this Chapter, we will examine the arguments for and against the central storage of biometrics as discussed in the parliamentary debates.

In the debate, several objections were raised by parliamentary representatives against central storage. Relevant arguments were, amongst others, that the new law created the possibility of function creep *re* citizens' biometric data and that the new law would mean a significant departure from the basic principles of Dutch criminal law. The Minister offered several counterarguments that were subsequently accepted by a majority of the house.

Firstly, the Minister pointed out that provision of data for criminal purposes from a central online consultative travel document administration does not differ from the present situation. The provision of data for the same purposes already occurs from the decentralized administrations. The only difference is the possibility to provide fingerprint data, this will now be introduced but is, however subject to strict conditions.

Secondly, referring to the European Court of Human Rights decision in *S. and Marper* v *UK*,[115] the registration system at issue in that judgment was compared to the travel document administration at issue. They are considered as being different based on the following two reasons. First, other than in the UK case, the central administration cannot be characterized as a criminal tracking register. The fingerprint registration applies to anyone who requests a travel document, and not merely to criminal suspects. Hence, there is no stigmatizing effect. Second, other than in the UK case, concerning the central administration, an assessment has been made between the private and public interest. This assessment led to the conclusion that

[111] EK [Dutch First Chamber] 31 324 (R1844).
[112] See Müller & Kindt 2009.
[113] http://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vi3muuvdnnsz/f=y.pdf.
[114] EK [Dutch First Chamber] 31324, *Memorie van Antwoord*, 28 April 2009.
[115] ECtHR 4 December 2008, *S. and Marper* v *United Kingdom*, Nos 30562/04 and 30566/04.

an accurate and effective travel document administration justifies the registration of fingerprints.[116] Based on these arguments, the Dutch government holds that the *S. and Marper* judgment, has no consequences for the central online consultative travel document administration.

The Dutch government's preference for a central online consultative travel document administration derives from the necessity to make the request and distribution process more reliable.[117] Apart from overriding security objectives (the prevention of identity fraud), the central register also provides a better service to the citizen. The request for a travel document should be made independently from the location where the travel document is requested.

The Minister also specifically mentioned the following arguments in favor of the choice for a central administration for the biometric data.

Firstly, a decentralized process would in any case require central components. This includes a central relegation index (*Centrale verwijsindex*). This index checks any prior requests for travel documents. It has to contain a substantial amount of data, which is also present in the decentralized administrations.

Further, all decentralized administrations have to be equipped with software which verifies whether requests are made based on different identities (*biometric search function*). Every request made has to be sent to every decentralized administration (there are about 15,000 requests per day). Even with a decentralized process, a central specialized research facility is necessary to examine the results of this search.

With a decentralized process, the availability of the administrations is more vulnerable than with a central process. In a decentralized process, about 700 administrations and the central relegation index have to be available, bearing the risk of one administration being offline (holding up the process), and this inevitably costs more time than one central process. Also, every decentralized administration is vulnerable to peak loads. In a central process, this can be arranged more efficiently.

In case of maintenance or adaptations, these would have to be done on 700 administrations simultaneously if these are decentralized.

Lastly, a central process can provide better security. A decentralized process would require a higher level of security than the present level. It does not provide less security risks than a central process, because the integrity of all administrations would be at stake.

Besides the issue of creating a central database for the biometric data, the access of criminal investigation agencies to the data stored in the database was a concern of some members of parliament. Article 4b(4) of the new Passport Act provides that the Public Prosecutor can request access to the data in the central register, under the strict rules applying to access to data in the context of a criminal investigation. The answer of the minister was brief, stating that provision of data for criminal purposes from a central online consultative travel document administration does not differ from the present situation.

This is an interesting statement in view of another ministerial answer about finger scans of

[116] This is thoroughly dealt with in the explanatory memorandum of the Bill.
[117] EK [Dutch First Chamber] 31324, *Memorie van Antwoord*, 28 April 2009.

foreigners (including other EU citizens).[118] In contrast to the finger scans of non-foreign inhabitants of the Netherlands, all foreigner; fingers cans are already stored on the foreigner databank, for the purpose of identification. The finger scans are stored to prevent identity fraud and to make the implementation of the Foreigners Act 2000 run more efficiently.

The finger scans are not stored for law enforcement purposes. Therefore, the Commission Meijers has suggested that after the Huber judgment,[119] the European Court of Justice may find a swipe search of the foreigner bank on the basis of Article 55c Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*)[120] unlawful.[121] In a reply to questions from the Dutch Senate,[122] the Minister of Justice has indicated that he does not think this is the case. He refers to the fact that in the proposal for the amendment to the Passport Act, Article 4a(1) stipulates that a face scan and four finger scans of every Dutch citizen are stored at the moment that she applies for a passport. As a result of Article 4b(4) of that same Passport Act, the Public Prosecutor can request access to these data. According to the Minister, the conditions applying to a Dutch passport holder suspect are similar in law to the situation where the suspect 'is a foreigner in all likelihood' and a search request is made by the prosecutor to have access to data in the foreigner databank.[123] An interesting legal point here is whether the Minister in fact implies that swipe searches can be held in both databases to compare the finger scans of a suspect held against all scans in the data base.

6.2 Analysis and conclusion

In the implementation of European Regulation 2252/2004,[124] which requires biometrics to be included in passports and travel documents, Dutch government has adapted the Passport Act not only to include two fingerprint and one face scan in travel documents, but also to create a central databank for storing these biometric data. In the political decision-making process, various arguments were advanced in favor of central storage, mostly relating to efficiency but also to law and order (anti-terrorism, combating illegal immigration, and crime-fighting). A key feature in this process was the desire to make application for travel documents independent from location, so that citizens can request a passport not only at the municipality where they reside, but also at other places. This convenience-enhancing requirement has implications for many of the arguments for central storage, since checking applications from different locations is much more difficult if the biometric data were stored in a decentralized way. As such, the convenience, service-delivery argument led quite easily to the decision to store the biometric data in a central databank.

---

[118] See Article 1(e) and (m) of the Dutch Foreigners Act.
[119] *Official Journal* C 44 21.2.2009.
[120] This refers to a procedure which allows the state prosecutor access to data held by other authorities under certain circumstances.
[121] Commissie Meijers, Letter about *Wetsvoorstel Identiteitsvaststelling verdachten*, 22 January 2009, http://www.commissie-meijers.nl/assets/commissiemeijers/Commentaren/2009/CM0901%20Brief%20Commissie%20Meijers%20Wetsvoorstel%20Identiteitsvaststelling%20verdachten.pdf.
[122] EK [Dutch First Chamber] 31436, C, 17 March 2009, http://www.dnasporen.nl/docs/wetregelgeving/KST128925.pdf.
[123] *Ibid.*
[124] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *Official Journal* L385, 29/12/2004, p. 1-6.

The fact that central storage also has considerable implications for privacy of citizens, not the least through security risks posed by large-scale central databases, was much less discussed in the political and public debate. Only after the Passport Act had been passed by the First Chamber did some minor discussions take place in the media on the privacy implications of central storage of the fingerprints.

It can only be guessed why exactly the privacy risks of central storage of biometric data in a databank mandated by the government were not a key issue in the political and public debates. Experience of the past decade shows that in the decisions by the Dutch legislator, privacy is often undervalued; arguments of security, but also efficiency and convenience, often prevail in the decision-making process.[125] Warnings by security experts of the risks of large-scale central databases[126] hardly penetrate into parliamentary debates. Even official reports criticizing the usefulness of creating huge national-intelligence databases for data mining purposes[127] are largely unheeded by the administration and parliamentarians.

In summary, the 2009 Dutch choice for a central databank with face and finger scans is supported by a large majority in the Dutch parliament. The possible PET alternative (biometric data on the passport only) has been rejected on efficiency and convenience grounds.

The case of a central databank for travel-document biometric data confirms the trend of undervaluing of privacy in political decisions. In the present political climate that values security and efficiency so much, biometrics are therefore much more likely to be shaped as a privacy-invasive technology than as a privacy-enhancing technology.

[125] See e.g. Vedder et al. 2007.
[126] See e.g. Jacobs 2007.
[127] Adviescommissie Informatiestromen Veiligheid 2007.

7 Conclusion

This deliverable has aimed to build on research in biometrics and PETs, in order to study the precise 'PET content' of biometric applications currently in use or under development. PET in this context refers to a technology that protects personal privacy by minimizing or eliminating the collection and/or handling of identifiable biometric data. PETs can 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. The most far-reaching form of privacy-enhancing biometrics is the system-on-card construction, where biometrics are encapsulated in a personal device and do not leave this device. The second most privacy-enhancing measure is the match-on-card construction, where the data do not leave the card either but where the sensor reading the data is external, and therefore located outside the personal device or card. This means that the user still has to trust that the reader and the system do not store any templates.

However, biometrics can also be created in a more privacy-invasive way. We have used the term 'privacy-invasive technology' PIT for these, referring to a technology that invades personal privacy by maximizing or creating the collection and/or handling of identifiable biometric data. An obvious example would be the storage of information in a manner where medical or racial information can be inferred; storing the raw template is privacy invading. This currently only occurs in basic biometric systems that are generally becoming outdated.[128] Equally intrusive however is the use of individuals' biometric data to link their pseudonymity or identity between different applications, domains, and databases. Unnecessary privacy intrusion occurs when a biometric system is used for identification, where verification would already have met the objectives of the application. Finally, the use of biometrics for surveillance purposes seems inherently privacy invasive, since data subjects have no control, and sometimes also no knowledge, over biometric data being processed.

Several types of decisions in the development process of biometrics applications influence their becoming PETs or PITs. These decisions are taken in the context of a complex process of balancing the interests of individuals to have control over their personal data and a series of other interests such as economic interests, policy and societal interests, security, but also convenience and efficiency interests. All these interests have a bearing on the use of biometrics and its relationship with data protection.

This report has identified a series of possible criteria that can help to determine whether maximization of privacy has been a major factor in decisions on the design and use of biometric applications. These criteria are: obligatory or voluntary nature of the application, choice of biometric, authentication or verification function, multi-factor system use, personal control, access to biometric data, room for function creep, data quality, and interoperability, linkability and profiling.

With these criteria in mind, a number of case studies have been made of processes of

[128] An exception are forensic DNA databases. Many countries retain body samples, so that they can update or extend the biometric template (the DNA profile) in light of technical or legal developments, for example, comparing databases across countries that use different markers in the profile or to include new markers that can be more easily determined in deteriorated crime-scene material.

decision-making regarding various large-scale as well as small-scale biometrics applications. These case studies concern technical decisions made in biometric pseudonyms and iris recognition, using cryptographic techniques for privacy enhancement; technical and organizational decisions made if a Privacy Impact Assessment is conducted in the development of a biometric application; decisions taken during the test stage of voice-recognition and the German ePass applications; and, finally, political decisions made about central storage of biometrics outside travel documents.

Together, these case studies show a differentiated picture of biometrics as PETs or PITs. On the one hand, new applications are developed and commercialized that are relatively privacy-enhanced, as the case study on biometric pseudonyms and iris recognition shows. On the other hand, the voice-recognition case studies show that, in private-sector situations, costs can become a factor that prevents roll-out of a privacy-friendly biometric system. In the public sector, the two e-passport case studies show that despite the technical possibilities, many biometric applications are turned into PITs. For example, in the case study of the Dutch passport, the storage of biometrics on the passport itself could be argued to be relatively PET, because the passport owner keeps some control over who can read and use the biometric information on the passport. However, the decision to store the biometric information in a centralized database as well turns this application of biometrics definitely into a PIT, as it removes the notion of individual control over the data. The creation of a central database and the access such a database may provide to law enforcement and other government agencies is a principal demarkation point in any decision to use biometrics. The existence of a database provides possibilities for the (current or future) use of biometrics for surveillance purposes, and thus constitutes a major factor in the resulting application turning out a PET or a PIT.

We thus observe that drivers behind PITs are political, often surveillance-related, interests, higher costs associated with privacy-enhanced applications, and perhaps also the commercial potential of information collection in a privacy-invasive application. Although these are major criteria in some contexts, they are by no means decisive reasons in many everyday contexts where biometrics are employed.

One of the questions raised by our research is therefore, why, despite the technical possibilities – such as biometric pseudonyms – so few biometric applications are used as PETs. Technical, organizational, policy, and political decisions turn out to have a major influence on biometrics often becoming PITs. One explanation is that in the information economy as well as in today's socio-political climate, the information-yielding potential of PIT applications seems to offer so many economic or political advantages that privacy arguments and PET alternatives pale in significance. However, another explanation is that there may be a lack of technical knowledge of privacy-preserving technologies at the stage where functional requirements for biometrics applications are specified, resulting in the creation of unnecessarily privacy-invasive biometrics.

The possible gap identified in this report between expectations and assessments based on technical knowledge and between economic and political expectations of and requirements for biometric applications is very relevant for the development of the information society, in which biometrics is playing an increasingly vital role in identity management. It is recommended that further research, encompassing more and different types of case studies, is conducted to refine the tentative finding of the PET/PIT gap between technically-informed and commercial or politically-based decisions.

In the meantime, it seems important that both public and private policy-makers become more acquainted with recent technical advances in the field of privacy-enhanced biometrics. An adequate assessment, such as in a Privacy Impact Assessment, of the long-term effect of the use of biometrics on privacy can only be made when decision-makers have realistic expectations based on solid knowledge of functional performance operations. The privacy implications of the use of biometric technology do not only have to be assessed on their own merits, but also in comparison with alternative identification, authentication, and verification systems, including the current situation.[129]

Also, technical, organizational, and policy decisions should be more integrated. An important notion here is 'value-sensitive design':[130] moral values and legal norms should be incorporated in the design process of new technologies and applications at an early stage, which is a more effective and efficient way of ensuring that the resulting technologies and applications meet the normative societal context in which they are to function.[131] Thus, the development of biometric applications should take place according to the notion of value-sensitive design.

In conclusion, enhancing awareness of the technical possibilities of PETs and applying the notion of value-sensitive design can lead to better informed and more balanced choices in the development of biometric applications. This could reverse the worrying trend that is tentatively found in this report that the various types of decisions lead to biometrics often becoming PITs rather than PETs.

[129] Introna & Nissenbaum 2009, p. 47.
[130] Friedman 1998.
[131] See also Introna & Nissenbaum 2009, who recommend in relation to facial-recognition systems that 'moral and political considerations be seen as on a par with functional performance considerations, influencing the design of technology and installation as well as operational policies throughout the process of development and deployment and not merely tacked on at the end' (p. 47).

Bibliography

Adams, C. (2006), 'A Classification for Privacy Technologies', 35-52.

Adviescommissie Informatiestromen Veiligheid (2007), *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*, April 2007, http://www.nctb.nl/Images/DatavoorDaadkracht_tcm91-131202.pdf?cp=91&cs=25496.

Albrecht, A. (2003), 'BIOVISION: D7.4, Privacy Best Practices in Deployment of Biometric Systems (Final Report).

Andronikou, V., Demetis, D., Varvarigou, Th., 'Biometric Implementations and the Implications for Security and Privacy', 1st in-house *FIDIS Journal Issue*, 1-2007, available at http://journal.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_ Implications _for_Security_and_Privacy.pdf.

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 26 p.

Article 29 Data Protection Working Party, *Opinion on Implementing the Council Regulation (EC) N° 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 30 September 2005, 12 p.

Article 29 Data Protection Working Party, *Working document on biometrics*, 1 August 2003, 11 p.

Ashbourn, J., 'The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies', *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, January 2005.

Backhouse, J., 'Interoperablity of Identity and Identity Management Systems', *Datenschutz und Datensicherheit*, 2006, Vol. 30, No. 9, 568-570.

Bauer, M. & M. Meints (eds.), *D3.1 Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS, 2004, available at http://www.fidis.net/resources/fidis-deliverables/.

BECTA, (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.

Bender, J. D. Kügler, M. Margraf, and I. Naumann, 'Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis', *Datenschutz und Datensicherheit*, Vol. 32, 2008, 173–177.

Bennett, Colin & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, 2006.

Borking, J., *Organizational Motives for Adopting Privacy Enhancing Technologies*, 2008.

Borking, J., *The Business Case for PET and the EuroPrise Seal*, Europrise Deliverable, 2008.

Bos, T., 'Privacy-Enhancing Technologies: Theorie en Praktijk bij de Overheid',*ego,* Vol. 6, No. 2, 2007, 26-28, available at http://www.sbit.nl/ego/bestanden/EKSBIT1.pdf.

Boult, T. E., Scheirer, W. J., Woodworth, R., 'Revocable Fingerprint Biotokens: Accuracy and Security Analysis', *Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference*, 17-22 June 2007.

Bray, E., 'Ethical Aspects of Facial Recognition Systems in Public Places', *Information, Communication and Ethics in Society*, 2004, No. 2, 97-109.

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

2008.

Bundesministerium des Inneren, *Grobkonzept zur Einführung des elektronischen Personalausweises in Deutschland*, Technical Report BMI-IT4-644004/14#5, Referat IT 4 – Biometrie, Pass- und Ausweiswesen, Meldewesen, 2008, available at http://www.bmi.bund.de/cae/servlet/contentblob/122648/publicationFile/15717/Grobkonzept_Personalausweis.pdf.

Burkert, H., 'Privacy Enhancing Technology: Typology, Critique and Vision', in: P. Agre and M.Rotenberg (eds), *Technology and Privacy: The New Landscape*, Cambridge, MIT, 1997, 125-142.

BZK, *2b or not 2b. Evaluatierapport. Biometrieproef. 2b or not 2b*, The Hague: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2005, available at http://www.minbzk.nl/onderwerpen/persoonsgegevens_ en/reisdocumenten/publicaties?ActItmIdt=54771.

Cavoukian, A., *Privacy and Biometrics*, Information and Privacy Commissioner, Ontario, September 1999, available at http://www.pco.org.hk/english/infocentre/files/cakoukian-paper.doc.

Cavoukian, A. & A. Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, Information and Privacy Commissioner, Ontario, March 2007, 48 p., available at http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf.

Cheung K.H., Ad. Wai-Kin Kong, D. Zhang, M. Kamel, Jane You, Ho-Wang Lam, 'An Analysis on Accuracy of Cancelable Biometrics Based on BioHashing', *Lecture Notes in Computer Science*, Springer, 2005, 1168-1172.

Clarke, R., *Biometrics' Inadequacies and Threats, and the Need for Regulation*, Computers, Freedom & Privacy 2002, available at http://www.anu.edu.au/people/ Roger.Clarke/DV/BiomThreats.html.

Clarke, R., *Privacy Impact Assessment Guidelines,* Chapman, Australia 1998, available at http://www.xamax.com.au/DV/PIA.html.

Commission of the European Communities, *Communication on the Evaluation of EU Policies on Freedom, Security and Justice*, COM(2006) 332final, 28 June 2006.

Commission of the European Communities, *Communication on improved effectiveness, enhanced operability and synergies among European Databases in the area of Justice and Home Affairs*, COM (2005)597 final, Brussels, 25 November 2005.

Commission of the European Communities, *Communication on Interoperability for Pan-European e-Government Services*, COM (2006) 45, 13 February 2006.

Committee of experts on data protection (CJ-PD), *The introduction and use of personal identification numbers: the data protection issues*, Strasbourg 1991, Chapter II, available at http://www.coe.int/.

Council Of Europe, *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Strasbourg, February 2005, 26 p.

Curtis, K., *The Biometrics Institute Privacy Code*, Canberra, Australia, 2006, available at http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8.

Daugman, J., 'How Iris Recognition Works', *IEEE Transactions on Circuits and Systems for Video Technology*, 2004, Vol. 14, No. 1.

De Hert, P. & A. Sprokkereef, *An Assessment of the Proposed Uniform Format for Residence Permits: Use of Biometrics*, CEPS Briefing Note for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, IP/C/LIBE/FWC/2005-xx, available from www.ceps.be.

De Hert, P., W Schreurs & E. Brouwer, 'Machine-readable identity documents with biometric data in the EU: Overview of the legal framework*', Keesing Journal of Documents and Identity,* Issue 21, 2006, 3-10.

De Leeuw, E., 'Biometrie en nationaal identiteitsmanagement', *Privacy en Informatie*, 2007, No. 2, 50-56.

Dessimoz, D. and Richiardi, J., *Multimodal Biometrics for Identity Documents*, Research Report PFS

341-08.05 v1.0 (September 2005), available at http://www.biometricscatalog.org/documents/ MBioIDStateOfTheArt_v1.0-8.pdf

Dodis, Yevgeniy, Leonid Reyzin & Adam Smith, 'Fuzzy extractors: How to generate string keys from biometrics and other noisy data', *Proceedings of the International Conference on Advances in Cryptology* (EUROCRYPT '04), Lecture Notes in Computer Science, Springer Verlag, 2004.

European Biometrics Forum, *Security & Privacy in large Scale Biometric Systems*, A report commissioned by JRC/ITPS, 2008.

European Commission, Joint Research Centre (DG JRC), Institute for Prospective Technological Studies (IPTS)*, Biometrics at the Frontiers: Assessing the Impact on Society*, Brussels 2005, available at http://www.biteproject.org/ documents/EU_ Biometrics _at_the_Frontiers.pdf.

Friedman, B. (ed.), *Human Values and the Design of Computer Technology*, University of Chicago Press, 1998.

Frost & Sullivan, *Leading European Financial Institution Implements Voice Verification Biometrics to Enrich Customer Experience*, July 2006.

Gasson, M., M. Meints & K. Warwick (eds.), *D3.2 A Study on PKI and Biometrics,* FIDIS, 2005, available at http://www.fidis.net/resources/fidis-deliverables/.

Geradts, Z. & P. Sommer (eds.), *D6.1: Forensic Implications of Identity Management Systems*, FIDIS, 2005, available at http://www.fidis.net/resources/fidis-deliverables/.

Grijpink, J.H.A.M., 'Een beoordelingsmodel voor de inzet van biometrie', *Privacy & Informatie* 2006, No. 1, 14-17.

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

Hes, R., T. F. M. Hooghiemstra & J.J. Borking, *At Face Value, On Biometrical Identification and Privacy*, Registratiekamer Achtergrond Studies en Verkenningen 15, The Hague, September 1999.

Hildebrandt, M. & J. Backhouse (eds.), *D7.2: Descriptive analysis and inventory of profiling practices*, FIDIS**,** 2005, available at http://www.fidis.net/resources/fidis-deliverables/.

Hildebrandt, M. (ed.), *D7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools*, FIDIS, March 2009, available at http://www.fidis.net/resources/fidis-deliverables/.

ICAO-NTWG, *Electronic-manchine readable travel documents & passengerfacilitation*, ICAO Guidlines, April 2008, http://www2.icao.int/en/MRTD/Downloads/Guidance%20Material/ Machine%20Readable%20Travel%20Documents%20-%20Passenger%20Facilitation.pdf .

Introna, L. & H. Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, New York Centre for the Study of Technology and Organization, 2009.

Jacobs, B., 'Select before you Collect', *Ars Aequi*, Vol. 54, 2005, 1006-1009.

Jacobs, B., *De menselijke maat in ICT*, 2007, available at http://www.cs.ru.nl/B.Jacobs/MM/.

Jaquet-Chiffelle, D.-O. et al. (eds), *D2.6: Identity in a Networked World – Use Cases and Scenarios*, FIDIS, 2006, available at http://www.fidis.net/resources/fidis-deliverables/.

Jay, R. and Hamilton, A., *Data Protection. Law and Practice*, London: Sweet & Maxwell, 2003

Juels, A., D. Molnar & D. Wagner, 'Security and Privacy Issues in E-Passports', *Proc. 1st Intl. Conf. on Security and Privacy for Emerging Areas in Communications Networks, IEEE Computer Society*, Los Alamitos, CA, 2005, 74-85.

Kindt E. & L. Müller (eds) (2007), *D3.10: Biometrics in identity management*, FIDIS, December 2007, available at http://www.fidis.net/resources/fidis-deliverables/

Kindt, E., 'Biometric applications and the data protection legislation,' *Datenschutz und Datensicherheit*, Vol. 31, No. 3, 166-170, 2007, available at http://www.fidis.net/fileadmin/fidis/publications/2007/DuD3_2007_166.pdf.

Koc-Menard, S., 'Trends in terrorist detection systems', *Journal of Homeland Security and Emergency*

Management, Vol. 6, No. 1, 2009.
Koops, Bert-Jaap, 'Technology and the Crime Society: Rethinking Legal Protection', *Law, Innovation & Technology*, Vol. 1, No. 1, 2009.
Koorn, R. et al., *Privacy Enhancing Technologies. Witboek Voor Beslissers*, The Hague: Ministerie van Binnenlandse Zaken, 2004.
Linnartz, J.P. & P. Tuyls, *New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates*, AVBPA 2003, LNCS.
Lips, A.M.B., J.A. Taylor & J. Organ, 'Identity Management as Public Innovation: Looking Beyond ID Cards and Authentication systems', in: V.J.J.M. Bekkers et al. (eds.), *ICT and Public Innovation*, 2006, Amsterdam: IOS Press, 204-216.
Meints, M. & M. Hansen (eds), *D3.6: Study on ID Documents*. FIDIS, December 2006, available at http://www.fidis.net/resources/fidis-deliverables/.
Meints, M., 'Implementierung großer biometrischer Systeme: Kriterien und deren Anwendung am Beispiel des ePasses', *Datenschutz und Datensicherheit*, Vol. 3, No. 31, 2007, 189-193, available at http://www.fidis.net/fileadmin/fidis/publications/2007/DuD3_2007_189.pdf.
Mitchison, N., M. Wilikens, L. Breitenbach, R. Urry & S. Portesi (2004), *Identity Theft: A Discussion Paper*, EUR 21098 EN European Communities, 2004, available at https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.
Müller, G. & K. Rannenberg, *Multilateral Security in Communications*, Vol. 3 Technology, Infrastructure, Economy, München: Addison Wesley, 1999.
Müller, L. & E. Kindt, *D3.14: Model implementation for a user controlled biometric authentication*, FIDIS, August 2009, available at http://www.fidis.net/resources/fidis-deliverables/.
OECD (Organization for Economic Cooperation and Development), *Biometric-Based Technologies*, April 2006.
Oliver, G.M., *Study of the use of biometrics as it relates to personal privacy concerns*, 1999, available at http://faculty.ed.umuc.edu/~meinkej/inss690/oliver/Oliver-690.htm.
Pasupathinathan, V., J. Pieprzyk & H. Wang, 'An on-line secure e-passport protocol', in: L. Chen, Y. Mu & W. Susilo (eds), *Proceedings of the 4th International Conference on Information Security Practice and Experience (ISPEC)*, LNCS, Berlin Heidelberg: Springer, 2008b, 14-28.
Pasupathinathan, V., J. Pieprzyk & H. Wang, 'Security analysis of Australian and E.U. e-passport implementation', *Journal of Research and Practice in Information Technology*, Vol. 40, No. 3, 2008a, 187–205.
Pfitzmann, A. & M. Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v.0.30*, 26 November 2007, available at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.
Ploeg, I. Van der, 'The Illegal Body: 'Eurodac' and the Politics of Biometric Identification', *Ethics and Information Technology,* 1999, No. 1, 295-302.
Prabhakar, S., S. Pankanti & A.K. Jain, 'Biometric recognition: security and privacy concerns,' *Security & Privacy Magazine*, IEEE , Vol.1, No. 2, 2003, 33-42.
Prins, C., 'Making Our Bodies Work for Us: Legal implications of Biometric Technologies', *Computer Law & Security Report*, Vol. 14, No. 3, 1998, 159-165.
Ratha N.K., J.H. Connell & R.M. Bolle, 'Enhancing security and privacy in biometrics-based authentication systems', *IBM Systems Journal*, Vol. 40, No. 3, 2001.
Reisen, A., 'Digitale Identitäten im Scheckkartenformat', *Datenschutz und Datensicherheit*, Vol. 32, 2008, 164–167.
Rejman-Greene, M. (Ed.), *Roadmap for Biometrics in Europe to 2010*, BioVision, 15 October 2003.
Ribbers, P., *Privacy Risks, Benefits and Costs,* Deliverable F3 of WP0301 PRIME Consortium, 15

February 2008.
Rodotà, S., *Working document on biometrics*, IPA Herfstdagen on Security, 1 August 2003, available at http://www.win.tue.nl/ipa/archive/falldays2005/Paper_1_ Leenes.pdf.
Roßnagel, A., G. Hornung & Ch. Schnabel, 'Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht', *Datenschutz und Datensicherheit*, 2008, Vol. 32, 168-172.
Soutar, C., D. Roberge, A. Stoianov, R. Gilroy & B.V.K.V. Kumar, 'Biometric Encryption', in: Randall K. Nichols (ed.), *ICSA Guide to Cryptography*, McGraw-Hill, 1999, Ch. 22.
Sprokkereef, A., 'Data Protection and the Use of Biometric Data in the EU', in: Simone Fischer Huebner, Penny Duquenoy, Albin Zuccato & Leonardo Martucci (eds), *The Future of Identity in the Information Society*, *IFIP International Federation for Information Processing*, Vol. 262, Boston: Springer, 2008, 277-284.
Tavani, H & J. Moor, 'Privacy Protection, Control of information, and Privacy-Enhancing Technologies', *Computers and Society*, March 2001, 6-11.
Toh, K.-A., Ch. Lee, J.-Y. Choi & J. Kim, 'Performance based revocable biometrics', *2nd IEEE Conference on Industrial Electronics and Applications,* 23-25 May 2007.
Turle, M., 'Freedom of Information and Data Protection Law: a Conflict or a Reconciliation?', *Computer Law and Security Report*, Vol. 23, 2007, 514-522.
Tuyls, P, B. Skoric & T. Keevenaar (eds), *On Private Biometrics, Secure Key Storage and Anti-Counterfeiting,* Springer, 2007.
Van Blarkom, G.W., J.J. Borking & J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents*, The Hague: CBP, 2003.
Van Kralingen, R., C. Prins & J. Grijpink, *Het lichaam als sleutel*, ITeR series Vol. 8, Alphen aan den Rijn/Diegem, Samsom BedrijfsInformatie, 1997, 2-66.
Vedder, A.H., L. van der Wees, B.J. Koops & P. de Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Rathenau Instituut, Studie 49, February 2007.
Von Graevenitz, G., *Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren*, Berlin: LIT Verlag, 2006.
Wallwork, A. & J. Baptista, 'Understanding Operability', in J. Backhouse (ed.), *D4.1: Structured Accounts of Approaches on Interoperability*, FIDIS, 2005, 19-24, available at http://www.fidis.net/resources/fidis-deliverables/.
Weichert, T., 'Staatliche Identifizierung durch Biometrie', *Datenschutz Nachrichten*, 2004, No. 2, 9-19.
Wright, T., 'Promoting Data Protection by Privacy Enhancing Technologies', *Computer Telecommunications Law Review*, 2007, 6.
Yanikoglu B. & A. Kholmatov, 'Combining Multiple Biometrics to Protect Privacy', *Proceedings of ICPR-BCTP Workshop*, Cambridge, England, 2004.
Yun, Yau Wei & L. Chen Tai Pang, *An introduction to biometric match-on-card*, 2005, available at http://www.itsc.org.sg/synthesis /2005/3_BiometricMOC.pdf.