FIDIS

Future of Identity in the Information Society

Title:	"D 7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools"
Author:	WP7
Editors:	Mireille Hildebrandt (VUB)
Review:	Claudia Diaz (KUL), Jozef Vyskoc (VaF)
Identifier:	D7_12_v_1.0_final_before_review-ES-26jan
Type:	[Report]
Version:	1.0
Date:	Wednesday, 04 March 2009
Status:	[final version after internal review]
Class:	[Public]
File:	WP7 Deliverable 7.12

Summary

Behavioural Biometric Profiling allows for data controllers to pick up on a variety of behavioural patterns, 'leaked' by citizens in their everyday lives. These patterns can be used to re-recognise a person without having recourse to identification in the sense of a name or address. In an Ambient Intelligent environment such pattern recognition would allow for massive group profiling, inferring a great many profiles that entail knowledge about health risks, earning capacity, life-style preferences, criminal intentions.

This deliverable builds on previous joint research into profiling, detecting the pitfalls of invisible data collection and processing. It elaborates on the concepts of Ambient Law and Transparency Enhancing Tools, investigating to what extent an integrated set of legal transparency rights and technological transparency tools could ensure the right balance between the production of new knowledge generated by BBP and the possibility for citizens to anticipate the application of such knowledge to their person.

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

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	22.04.08	• First draft, scenario I Chapter 2 (Mireille Hildebrandt, VUB)
0.2	29.04.08	• Chapter 1 (Mireille Hildebrandt, VUB)
0.3	08.05.08	• Insertion scenario II Chapter 2 (Emmanuel Benoist, VIP) • Addition to Chapter 1 (Rainer Böhme, Stefan Berthold, Stefanie Pötzsch, TUD) • Addition to Chapter 5 (Rainer Böhme, Stefan Berthold, Stefanie Pötzsch, TUD) • Editorial comments
0.4	09.05.2008	• Chapter 3 (Bart Custers, TILT) • Editorial comments
0.5	26.05.08	• Addition to Chapter 2 (Vasilliki Andronikou, ICCS); • Addition to Chapter 3 (Bart Custers, TILT) • Addition to Chapter 5 (Hans Hedbom, KAU) • Editorial comments
0.6	29.06.08	• Additions to Chapter 1 and 5 (Emmanuel Benoist, VIP and Rainer Böhme, Stefan Berthold, Stefanie Pötzsch, TUD and Mireille Hildebrandt, VUB) • Adjustments of Chapter 2, scenario II (Emmanuel Benoist, VIP) • Insertion Chapter 4 (Els Kindt, KUL-ICRI and Mireille Hildebrandt, VUB) • Editorial Comments
0.7	16.07.08	• Additions, revisions by Bart Custers (TILT)
0.8	10.09.08	• Integration revisions of chapter 4 (Els Kindt, KUL-ICRI) • Preparation of version for Dresden workshop
0.9	02.10.08	• Integration section 5.2.2 (Maren Raguse, ICCP) • Editorial revisions
0.9.1	07.11.08	• Integration of revisions of section 5.1.2 (Hans Hedbom, KAU)
1.0	20.01.09	• Introduction, conclusions, editorial revisions (Mireille Hildebrandt, VUB) • Lay-out and bibliography (Els Soenens, VUB)
1.0	26.01.09	• Integration of comments Hans Hedbom (Mireille Hildebrandt, VUB) • Distributed for internal review
1.0	03.03.09	• Integration of the internal reviewers comments

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:

Chapter	*Contributor(s)*
0	Mireille Hildebrandt (VUB)
1	Mireille Hildebrandt (VUB), Rainer Böhme, Stefan Berthold, Stefanie Pötzsch (TUD), Emmanuel Benoist (VIP) Hans Hedbom (KAU)
2	Mireille Hildebrandt (VUB), Emmanuel Benoist (VIP), Vasilliki Andronikou (ICCS), Bart Custers (TILT)
3	Bart Custers (TILT) Mireille Hildebrandt (VUB)
4	Els Kindt (KUL-ICRI), Mireille Hildebrandt (VUB)
5	Rainer Böhme, Stefan Berthold, Stefanie Pötzsch (TUD), Hans Hedbom (KAU), Maren Raguse (ICPP), Mireille Hildebrandt (VUB)
6	Mireille Hildebrandt (VUB)

Table of Contents

0 Executive Summary 8

1 Introducing BBP and TETs 10
1.1 What is Behavioural Biometric Profiling? 10
1.1.1 Behavioural Biometrics (BBs) 10
1.1.2 Profiling 11
1.2 Requirements for identification or verification 12
1.2.1 Identification and verification 12
1.2.2 Enrolment 12
1.2.3 Requirements 13
1.3 Performance standards 14
1.4 What are Transparency Enhancing Tools? 15
1.4.1 Developing working definitions 15
1.4.2 Economic perspective on TETs 17
1.4.3 The relationship between PETs and TETs 18
1.4.4 From transparency enhancing *technologies* to transparency enhancing *tools* 18
1.5 The relevance of TETs for BBP 19

2 BBP cases & scenarios 21
2.1 The Smart Car (Driver Fatigue Detection) 21
2.1.1 Technical description (reliability) 21
2.1.2 Scenario: Who is driving? 22
2.2 Web Profiling (Key Stroke Behaviour) 23
2.2.1 Technical description (reliability) 24
2.2.2 Scenario: who is typing? 24
2.3 Support for the Elderly (Gait & Emotion detection) 26
2.3.1 Technical description 26
2.3.2 Scenario: "InLiFE" (Independent Life For Everyone) Application 27

3 Vulnerabilities generated by the usage of BBP 31
3.1 Introduction 31
3.2 Selection, unjustified discrimination 33
3.3 Stigmatisation 34
3.4 Confrontation 35
3.5 Limited information supply 35
3.6 De-individualisation 36
3.7 Moral principles 36

4 Vulnerabilities of the present legal framework regarding BBP 38
4.1 Introduction 38
4.2 Respect for private life 38
4.3 Data protection regulation 40
4.3.1 Transparency of BBP systems through information obligations and access rights? 41
4.3.2 Consent 43
4.4 Do the right to privacy and the protection of personal data protect against the disadvantages of group profiling on the basis of BBP? 44

5 The role of TETs in the case of BBP 47
5.1 Technological TETs 47

5.1.1 Technological View on TETs and Differentiation from PETs 47
5.1.2 Examples of existing technological TETs 51
5.1.3 Requirements for technological TETs in the context of BBP 58
5.2 Intermezzo: Privacy Mirrors, or 'playing with the system' *59*
5.3 Legal TETs *62*
5.3.1 Legal view of transparency tools, difference with opacity tools 62
5.3.2 Examples of new transparency tools 63
5.3.3 Recommendations for new legal TETs, with regard to group profiling, personalized profiling and BBP 70

6 Conclusions: Ambient Law, the Legal articulation of transparency rights into the BBP technological infrastructure? 73

7 Bibliography 76

8 Abbreviations 81

0 Executive Summary

Behavioural Biometric Profiling (BBP) is a relatively new type of profiling, based on measurements of bodily behaviours such as key-stroke behaviour, gait and facial expressions. Though we cannot yet assess the extent to which behavioural biometrics profiles (BBPs) are capable of an accurate unique identification of individual citizens, the prototypes seem promising. This calls for further research as to their reliability as well as to the potential drawbacks of their more general usage. One of the concerns here is the violation of privacy that stems from the fact that BBPs do not depend on deliberate input, but rather on data 'leaked' in the course of everyday activities.

Next to BBPs' claimed capacity to uniquely identify a person, BBPs can also be linked to other data, thus constructing a rich profile of a person's habits, life style, consumer preferences, health status, earning capacity, credit worthiness etc. Because BBPs can re-recognize you without having access to personal information like a name and address, the legal status of the ensuing composite personal profiles is unclear. When a BBP is linked to other data it can also be used to construct group profiles, for instance correlating a specific typing rhythm with the onset of Parkinson's disease or correlating certain ways of speaking with the onset of violent behaviour. When these group profiles match with your data, they could 'cause' certain decisions, like the decision to raise the premium for your health insurance or the decision to treat you as a potential suspect of a violent crime.

The general lack of awareness of the profiles that can be generated by means of BBP, creates an urgent need for transparency tools (TETs). These TETs should be capable of providing suitable feed-back about what happens to the data people 'leak', but also about how group profiles that match with their data could impact their choices in life. Technological TETs may either depend on information provided by the data controller or draw on the machine-readable behaviour of your environment. Without the means to test the reliability of the information supplied by a data controller it remains unclear to what extent these types of TETs provide for real transparency. This problem is avoided when using TETs that *counter profile* the environment, allowing a person to anticipate how the environment responds to her behaviour. However, in this case she may not be sure whether the environment provides enough evidence of the consequences of being profiled. In both cases TETs contain a substantial measure of privacy sensitive information, thus creating new vulnerabilities.

After exploring the scope of BBP and TETs, in chapter 1, we present three scenarios – in chapter 2 - to introduce possible implications of wide-spread usage of BBPs in everyday life. The main function of these stories is to sensitize the reader to the promises as well as potential pitfalls of this new technology.

To come to terms with the vulnerabilities exposed in the scenarios, we carefully analyse which types of vulnerabilities are to be expected if BBPs become part of our daily routines. In chapter 3 we explore how BBP can result in unjustified discrimination, stigmatisation, undesirable confrontation with knowledge about e.g. a person's health, limited information supply and de-individualisation. Most of these vulnerabilities are typical for all types of group profiling, but some are especially worrisome because of the lack of awareness that data are leaked and processed and because it is not easy for a person to deliberately change her

biometric behaviour. Resistance against being profiled in a certain way then becomes difficult if not altogether impossible.

The present legal framework is not geared to BBP. In chapter 4 we investigate the right to privacy and data protection legislation as tools for (1) the *protection of* personal data and (2) *against* unwarranted applications of group profiles, in the case of BBP. We conclude that the legal status of BBPs as personal data is unclear, while it seems obvious that this type of profiling will threaten the right to privacy, especially because no deliberate input is required. We discuss the extent to which consent could justify the processing of one's biometric behaviours, especially in the light of the fact that you have little control over the leaking of these data. As to the legal protection against the application of group profiles art. 15 and 12 of the data protection directive D/95/46/EC could be of use, in as far as group profiling enables an environment to make autonomic decisions that seriously influence a person's life. However, because the socio-technical infrastructure to support the exercise of these rights is not in place, these rights play the role of paper dragons rather than that of effective remedies.

In chapter 5 we explore which - existing or still to be developed - technological and legal TETs can provide effective remedies for the *protection of personal data* and *the protection against the application of illegitimate group profiles*. Technological PETs and TETS will be distinguished in terms of the objective they aim to achieve: whereas PETs aim to provide and increase the control over one's personal data, TETs aim to provide feedback. Since it is difficult to hide one's biometric behaviours, TETs are especially important in the case of BBPs. We find that whereas privacy enhancing technologies (PETs) have been developed beyond the stage of prototypes, the design of technological TETs is still in an early stage. On top of that present-day TETs mostly focus on providing access to (the processing of) personal data. Indeed, technological TETs that provide feedback about group profiles inferred from other people's data or from anonymised data have not yet been developed at all. This may be due to the fact that profiling techniques as well as the resulting profiles are economic assets of the companies that have invested in them, and as such protected as trade secrets or by means of intellectual property rights. As to legal TETs, this chapter explores some recently proposed legislation containing new legal TETs that might be of interest for the regulation of BBPs.

Chapter 6 concludes with a summary of how the notion of AmLaw - as developed in previous work of Work Package 7, see e.g., the FIDIS deliverable 7.9. titled 'A Vision on Ambient Law' (Hildebrandt and Koops, 2007) – can be made operational in the field of BBPs. Looking into the range of existing and emerging technological TETs we evaluate the extent to which they could indeed turn paper dragons into effective remedies. The deliverable thus ends with recommendations of a set of technologically embodied legal rights and a reference to the research agenda this calls for.

Note: This section is mandatory for all deliverable and should help to get an overview of the topics covered in the document.

1 Introducing BBP and TETs

In this introductory chapter we will introduce working definitions of Behavioural Biometric Profiling (BBP) and Transparency Enhancing Tools (TETs). We will explain how BBP differs from both physical biometric profiling and from other types of behavioural profiling and describe how BBP is a form of profiling while its results can also be linked with other data to build more extensive profiles. BBP will be introduced as an enabling technology of Ambient Intelligence (AmI), like sensor technologies and RFID, raising issues of reliability and interpretation. We will explain how BBP relates to issues of identity and identification.

After working out a summary working definition of TETs we will describe how they relate to the issues raised by BBP and give some examples of how TETs should provide transparency for citizens who are confronted with the application of BBP.

1.1 What is Behavioural Biometric Profiling?

1.1.1 Behavioural Biometrics (BBs)

In a white paper on keystroke dynamics a behavioural biometric (BB) has been defined as:

> 'a measurable behavior trait that is acquired over time (versus a physiological characteristic or physical trait) that is used to recognize or verify the identity of a person' (Biopassword Inc., 2006:2)

Before further discussing BBPs we will first look into the difference between a behavioural and a physical biometric (PhB). Biometrics derives from the Greek 'bios' and 'metrikos', meaning 'life' and 'measure' (Andronikou et al., 2007:2). Hereunder we will briefly discuss the 'bios'-aspect and the 'metrikos'-aspect of BBs in comparison with PhBs.

1.1.1.1 Bios – the living body

In as far as a BB is used for verification or identification it uses a bodily trait, rather than a piece of knowledge (like a password) or a token (like a smart card) to achieve its purpose. Also, other than e.g. a *transactional behavioural profile*, a BB involves bodily movement instead of a symbolic (inter)action like the buying or selling of goods or services (Backhouse and Canhoto, 2008). BB is to be distinguished from a physical or physiological biometric (PhB), which is also a bodily trait. PhBs, like fingerprints, face recognition, iris or retinal scanning and hand geometry, are relatively stable bodily traits that do not change rapidly in time. The PhB does not measure bodily *actions*, like in the case of BBs, which are by nature more dynamic.[1] For this reason, according to many authors, the difference between behavioural and physical biometrics resides in the dynamic character of the BBs, even though PhBs may show some dynamic in the course of person's life, due to aging or disease. So, while both PhBs and BBs will need regular updating, because both will vary in the course of

[1] The distinction of both types of biometrics is relative. Though behavioural biometrics are inherently dynamic, this does not mean their dynamic patterns are not stable over a period of time. And though behavioural biometrics can be distinguished from physical biometrics they are also conditioned by physical traits.

one's life, PhB consists of the measurement of a trait and BBs consist of the measurement of an action, which has a relatively unique pattern, thus allowing identification and verification of a unique human person. Examples of BBs are keystroke dynamics, speech recognition, signature verification or gait recognition.

One of the pertinent differences between transactional and biometric behaviours is that it is not easy to deliberately change such behaviour. One could call it 'a habit of the body', which is precisely why it qualifies as a 'signature' that has some permanence over time. Speaking of a 'habit of the body' indicates that we are speaking of automated behaviours, that may have been acquired in a learning process but are performed unconsciouslessly. This fact – of the automated, unconscious nature of biometric behaviours – implies that

1 other than in the case of transactional behaviour it is not easy to deliberately change or hide biometric behaviour (it is difficult to imagine legal or technological opacity tools for BBP)

2 for this reason, other than in the case of transactional behaviour, having access to the consequences of one's behaviour does not necessarily help in preventing undesired profiling (transparency tools for BBs allow anticipation of undesired profiling but they don't provide an alternative).

1.1.1.2 Metrikos – measuring of the dynamics

Whereas in the case of PhB the bodily trait that is measured concerns an analysis of a particular part of the body of an individual person, like a fingertip, an iris or the back of a hand, in the case of BB the bodily trait that is measured concerns an analysis of bodily movements or actions. In both cases the measurement is based on a statistical analysis of the pattern that is exemplary for either the physical bodily trait or for the behavioural bodily trait. This statistical analysis is basically a matter of data mining, which allows the visualisation of patterns that are mostly invisible to the naked human eye. This is not to deny that we do not easily identify a person by her gait. In fact we are quite used to profiling people on the basis of behavioural biometrics. The difference is that we have no access to the cognitive process that produces such recognition, while in the case of computer mediated recognition the process is designed by computer scientists and the resulting patterns (profiles, templates) are made explicit. The underlying processes that produce these explicit patterns may however, also in the case of machine-made pattern-recognition, be inaccessible even to those who designed the process (e.g. in the case of neural networks).

1.1.2 Profiling

BBs are templates or profiles, constructed on the basis of a series of measurements of bodily behaviour. These measurements form the data that are 'mined' to detect the pattern that is relatively unique for a particular person. In that sense a BB is the result of profiling.

These BBs can be used as a resource for further profiling, for instance by linking the BBs to web surf behaviour, to the occurrence of a specific disease, to location data, to performance in school, earning capacity etc. In that case the implications are far reaching and difficult to

anticipate, like in many other cases of profiling. As in the case of RFID-systems and sensor technologies BBs are an enabling technology for smart applications and Ambient Intelligence (AmI). The implications concern both privacy issues and social sorting, due to the fact that profiling technologies make visible what is invisible to the human eye (patterns), allowing extensive monitoring or surveillance as well as refined categorisation. In chapter 4 such implications will be further investigated, figuring out in which ways BBs differ from other profiling technologies.

As to BBP we need to remember that BBs are the result of BBP, while they enable further profiling. So, *a BB is a profile as well as a data* that can be used to generate other profiles. Within the framework of work package 7 we are focused on the implications of using BBPs as a source for (group) profiling, meaning that the focus is not on their usage for unique identification. However, to discuss the implications of using BBPs for group profiling we need to assess how they provide tools for unique identification. Therefore, in the next section, we will discuss the requirements for identification and verification on the basis of BBBs, and the performance standards used to calculate their reliability.

1.2 Requirements for identification or verification

1.2.1 Identification and verification

Biometrics in general can be used for identification or verification (Reyman-Greene, 2001:116); (Cattin, 2002:19-20). In the case of identification a biometric is taken from a person which is then matched against a data base of biometric templates, to detect whether the biometric profile of this person matches with one of the biometric profiles in the data base. In the case of verification a biometric profile is taken from a person who claims a specific identity, after which the biometric profile is matched with the profile that is registered as the profile of the claimed identity in order to verify the claim. For identification a data base is needed, while for verification one could carry a smart card with the claimed identity, which can then be verified with the biometric profile taken from the person carrying the card.

1.2.2 Enrolment

In both cases (identification and verification) we first need to establish the identity of the person in terms of the biometric profile in order to register the template against which to match the profile taken from a person who needs identification or verification. This is called enrolment.

Enrolment can be *immediate*, meaning that a person can be enrolled at any point in time within a short period of time, allowing immediate identification and verification. It can also be *gradual*, meaning that a person's biometric trait is measured repeatedly before consolidating it into the template.

Another important characteristic of BBs is that enrolment can be *silent* (Biopassword, 2006:9), meaning that the biometric template is constructed without user notification. This type of enrolment is not always possible, because often people will have to provide deliberate input for enrolment. In the case of genetic biometric profiles they may have to provide blood, in the case of iris scanning they will have to actively participate to allow the registration of

the template.[2] However, in the case of keystroke dynamics or gait analysis this is not necessary. With the use of special software programmes (in the case of keystroke dynamics) or sensor technologies (for gait analysis) a first template can be generated, allowing what has been called re-recognition (Dotzer, 2006), even if the identity of the person is not known in terms of name, address etc.

This type of silent enrolment has advantages as well as disadvantages. The advantage is that the enrolment (as well as verification and identification) is seamless and non-invasive, implying that whoever is to be identified or authorised need not be aware of the processing of her data (Biopassword Inc., 2006:11; Checco, 2003). Access to specific physical or online environments of data can thus be secured without much hassle. On the other hand, the disadvantage is that such invisible enrolment allows invisible monitoring and surveillance, enabling the manipulation of a person who need not even be identified in the traditional sense of the word. We will further discuss this in chapter 4.

1.2.3 Requirements

To be of use as a tool for unique identification and verification a biometric needs to allow unique identification on the basis of characteristics shared by all human persons. Gamboa and Fred (2004) distinguish the following aspects as pertinent for an adequate identifier:

- Universality (of the *types* of characteristics). Universality is a presumption of biometrics, which can however not be taken for granted. It needs testing and qualification in terms of the population within which a specific characteristic is 'universal'.

- Uniqueness (of the *singular mix* of characteristics, allowing individuation). Soft biometrics, like gender or eye colour, allow identification with a category without allowing unique identification. For this reason its usage is restricted to cases in which partial identification is sufficient (thus also allowing a measure of privacy because unique identification is not achieved). One could imagine that certain behavioural biometrics are part of a cultural heritage (e.g. gait), while certain physical biometrics may vary between different populations (genetic profiles). If one does not take this into account one could claim a match, while the relevant characteristic is specific to a group rather than a person, thus enabling a false positive. Again, like in the case of universality, uniqueness is a presumption that cannot be taken for granted and needs testing. In the end, a biometric template is a statistic inference.

- Permanence (invariance over time). As mentioned, with PhBs as well as with BBs this invariance is relative, requiring regular updating. In the case of PhBs this relative invariance concerns a trait, in the case of BBs a dynamic. In fact, while matching BBs, the profiles can be fine-tuned each time the match is made (since matching is always

[2] The distinction has to be relativised. Genetic biometric profiles can be obtained from a hair or blood sample, which could provide occasion for silent enrolment. Generally speaking this will, however, be a more cumbersome process, used in forensic profiling rather than commercial applications.

statistical, never absolute).[3]

- Collectability (the characteristics must be measurable and easy to acquire). BBs will usually require sensor technologies en special software programmes to process the data.

- Performance (accuracy). Below we will discuss the performance standards.

- Circumvention (must not be easy to spoof). Behavioural biometrics may be of interest because the behaviour that is measured is not deliberate or even conscious and may be difficult to imitate or change, especially when one is not aware of being profiled.

- Acceptable for those subject to identification/verification. This concerns both usability and privacy/autonomy issues. In as far as BBP is invisible its usability may be easy while many privacy and autonomy concerns can be raised. We refer to chapter 4.

1.3 Performance standards

Permanence is - of course – relative. There are no absolute matches in the case of behavioural biometrics, only comparative measures.

Performance is measured in:

- FRR (false rejection rate) indicates the percentage of false negatives that is anticipated: those whose identity claim is rejected while they are in fact who they claim to be, or those who cannot be identified while in fact their template is present in the data base.

- FAR (false acceptance rate) indicates the percentage of false positives that is anticipated: those whose identity claim is accepted while in fact they are NOT who they claim to be, or those who are identified as a person they are NOT

- EER (equal error rate) or CER (cross-over error rate), defined as the value at which FAR and FRR are equal)

- ROC (receiving operating curve), whereas the graphic of FAR is seen as a function of FRR

There is a trade-off between FRR and FAR: the lower the FRR (the lower the security) the higher the FAR (the higher the usability), while also the higher the FRR (the higher the security) the lower the FAR (the lower the usability). Security is deemed high when unauthorised access is limited, usability is deemed high when people are not too often

[3] Note that two different people could be wrongly identified as the same person, because their data are aggregated as those of one and the same person (e.g. two people using the same keyboard at different times of the day, with their keystroke behaviour interpreted as representing different moods).

mistakenly denied access. Acceptability of a biometric system will depend on its usability as well as its security: people will easily get irritated if they are refused access because the system misidentifies them as unauthorised; this will also be the case when people realise that the system mistakenly provides access to unauthorised persons.

The question of which performance is acceptable will depend on the consequences of a false acceptance or a false rejection: are we speaking of safety issues, of access to social benefits, of immigration, credit card payments, access to health records or other sensitive information. Are the risks involved major or minor; are the opportunities that depend on access major or minor? Is there a smooth procedure for due process or is there no way to contest the systems decision? This point is especially relevant in the case of biometrics because it is not easy – and often not possible – to change one's bodily traits.

Another measure of the performance of biometrics is the percentage of persons that can be enrolled. Its influence is to be seen in the uniqueness of the identification system. If there is only one way to log-in a system and 5% of the users can't log, that is a problem. If 10% of a population can not receive a biometric passport, it is a big problem. Moreover, as seen in the "UKPSBiometrics Enrolment Trial Report",[4] disabled persons may suffer of discrimination (in this UK study, 40% can not be enrolled for iris-scan).

1.4 What are Transparency Enhancing Tools?

1.4.1 Developing working definitions

In *FIDIS deliverable 7.7 RFID, Profiling and AmI* (Hildebrandt and Meints, 2006) TETs have been defined tentatively as:

> Transparency enhancing technologies, which have not been developed yet. Their function is not the history management of the data of a data subject, but the anticipation of profiles that may be applied to this particular subject. This concerns personalised profiles as well as distributive or non-distributive group profiles, possibly constructed out of anonymous data. The point would be to have some idea of the selection mechanisms (application of profiles) that may be applied, allowing a person adequate anticipation. To be able to achieve this the data subject needs access - in addition to his own personal data and a profiling / reporting tool - to additional external data sources, allowing some insight in the activities of the data controller. Based on this additional information the data subject could perform a kind of counter profiling.

In *FIDIS deliverable 7.9 A Vision of Ambient Law* (Hildebrandt and Koops, 2007) TETs have been further examined as an urgent counterpart to PETs and the *integration* has been argued of technological transparency tools with legal transparency enhancing tools. The idea of Ambient Law is that the legal protection against a specific technological infrastructure is *articulated* into the technological architecture: *embodiment* of legal rights in the technologies they aim to protect against. The main thrust of the idea of TETs is that AmI requires data

[4] See at http://dematerialisedid.com/PDFs/UKPSBiometrics_Enrolment_Trial_Report.pdf.

optimisation which may run counter to the idea of data minimisation that inspired PETs. If smart applications depend on as many relevant data as possible (while the relevance cannot be established in advance, especially in the case of unsupervised learning techniques) they will not function in a scenario that is based on hiding one's data. However, to protect oneself against invisible visibility, against surveillance and social sorting, legal tools must be created that provide rights of access to the profiles that can impact one's life and their effectiveness must be ensured by articulating them in the technologies needed to enable such access. While PETs 'think' in terms of the protection of personal data, TETs 'think' in terms of protection against invisible profiles. From the perspective of profiling technologies, the question of whether data is 'personal data' cannot be answered in advance because we never know which data will be correlated with which other data and which knowledge will emerge from processing whichever data. At some point anonymised data may be aggregated in a way that enables identification, turning the anonymised data into personal data. Both the promises and the threats derive from the way data are processed, NOT from the data themselves. We need to think in terms of dynamic, volatile, real time profiles instead of stable personal data.

Building on the idea of TETs, as developed in FIDIS deliverables 7.7 (Hildebrandt and Meints, 2006) and 7.9 (Hildebrandt and Koops, 2007), we will now provisionally define two types of Transparency Enhancing *Tools* with regard to profiling.[5] The difference between both types of TETs is that the first depends on an exchange of information between the data controller and the affected data subject, while the second depends on acquiring machine readable data from a user's environment by the user (via e.g. her personal digital assistant PDA) that could indicate potential consequences of profiling (counter profiling). The definition focuses on tools that provide information about how one is being profiled, meaning that we are concerned with a subset of TETs in the more general sense of transparency tools that provide any other type of information e.g. about what data is collected, how it is stored, sold or used for what purpose (other than profiling). In chapter 5 (section 5.2) we will investigate which types of TETs in this more general sense come close to TETs that focus on clarifying how one is being profiled.

Type A: legal and technological instruments that provide (a right of) access to (or information about) data processing, implying a transfer of knowledge from data controller to data subjects, and/or

Type B: legal and technological instruments that (provide a right to) counter profile the smart environment in order to 'guess' how one's data match relevant group profiles that may affect one's risks and opportunities, implying that the observable and machine readable behaviour of one's environment provides enough information to anticipate the implications of one's behaviour.

In this deliverable the focus will be on the first type of TETs, since the second type has not been developed as yet.[6]

As to the aim of TETs, we recount that while PETs build on data minimisation, TETs build on

[5] About the shift from Transparency Enhancing Technologies to Transparency Enhancing Tools, see section 1.4.4 below.
[6] An initial example of such TETs could be found in Privacy Mirrors (Nguyen and Mynatt, 2002).

minimisation of information or knowledge asymmetry. This means that TETs basically aim to clarify:

- How am I being profiled?
- Which behaviours cause which categorisations?
- Which are the potential consequences?

1.4.2 Economic perspective on TETs

From the perspective of democracy and rule of law, minimising knowledge asymmetries is the main purpose of TETs, with a focus on (group)profiles. One way of analysing the potential of specific TETs in this respect is to take an economic perspective, focusing on a reduction of undesirable externalities through abusive data processing practices.

Externalities, such as information asymmetries, are a well-defined concept in economics (Akerlof, 1970). They refer to the fact that actions of (groups of) individuals may affect uninvolved third parties. Externalities can be either positive or negative, but the negative ones are more problematic from a policy perspective. In the case of privacy protection, negative externalities may arise for the data subject if the data controller shares its personal data with a third party, say the data subject's employer or health insurance company (cf. Jiang et al., 2002). A socially ideal solution would be to avoid externalities directly, but this is not always easy as personal data are information goods, which can be replicated at zero marginal cost and for which hidden action is hard to police. So if externalities cannot be prevented, a second best solution is to let the affected data subject anticipate the expected externalities through transparency. In other words, reducing information asymmetries is a means to lower negative externalities *indirectly*. This can be done through different mechanisms.

Böhme (2008) refers to a credit-scoring scenario to describe mechanisms by which the existence of TETs can influence the stakeholders to more socially desirable outcomes for data handling practices. He argues that transparency limits excessive discrimination on the basis of personal information through three channels:

- First, on an *individual level*, pre-emptive transparency-enhancing technologies assist people in making decisions that do not affect their personal 'score' adversely, i.e. increase the probability of being assigned to a more favourable group profile. This means that data subjects can make informed decisions in anticipation of possible (positive and negative) externalities of future actions of the data controller.
- Second, on a *mechanism level*, scoring procedures (including group profiles) that are not strategy proof, or the effectiveness of which depends on the scoring details to remain obscure, become less useful and would thus be avoided. This limits the discretion of data controllers and third parties to impose externalities to socially justified ones (e.g. credit scoring is not a bad thing per se, if better conditions are passed on to bona fide lenders, but arbitrariness in loan granting may lead to inefficiencies).

- Third, on a *social level*, if public scrutiny reveals that a particular scoring function is arbitrarily discriminating and as such incompatible with the society's values, the risk of public uproar and reputation damage might put social pressure on data controllers not to implement abusive profiling practices in the first place.

Further, Jiang et al. (2002) have identified a *detection function* of transparency tools, which can be broadly subsumed to the social level mechanisms. They argue that abusive data handling practices can be prevented by deterrence: TETs should support mechanisms to detect data abuse, at least with non-zero probability, and a complementary legal framework that ensures that malicious data controllers are held accountable.

1.4.3 The relationship between PETs and TETs

As we have seen in our previous work, e.g., del. 7.9 (Hildebrandt and Koops, 2007), some PETs aim beyond the hiding of one's data (by means of anonymisation or pseudonimity) to enhance transparency of data processing (e.g. history management). This means that some TETs can be seen as a subcategory of PETs. This will be further elaborated in chapter 5, section 5.1.

With respect to profiling, TETs may differ from PETs in as far as they do not just focus on privacy but also on the implications for social sorting and surveillance, their main focus being a reduction of the knowledge asymmetry that is brought about by sophisticated group profiling. As discussed above, one way to achieve a reduction of this asymmetry would be a transfer of knowledge from the better informed party (e.g. data controller) to the less informed party (e.g. data subject), type A TETs. This, however, makes TETs dependent on the honesty of data controllers and indicates that other ways must be found to produce user-controllable transparency. Developing TETs that depend on data from the data controller is technically much more demanding – if not impossible – than developing user-controllable PETs. Also, in this case, the apparent advantage of TETs over PETs comes at the costs of weaker security guarantees. The socially desirable outcomes of these TETs depend on the optimistic assumption that the data controller is honest about the true data processing habits. This requirement is difficult to enforce.[7] So TETs that build on data processing rules provided by the data controller, like PETs, will not provide a panacea that solves all privacy concerns of a modern information society.

This means that next to Type A TETs that should provide a precise correspondence between what the profiler knows and what the profiled knows, we should develop Type B TETs, which do not depend on the trustworthiness of the data controller. The obvious drawback of Type B TETs (counter profiling) seems to be that it will not always be possible to 'read' the environment's responses, for instance because the consequences of leaking one's data today may only become visible many years from now. The long-term storage of data means that profiling can take place at a much later point in time, affecting a person in a totally different context at another point in time. Type B TETs thus seem to provide less accurate data, rather

[7] If verifiability could be imposed on data controller, this could be easier. For instance if they would be required to publish them and their input and output could be verified by testing. See chapters 4 and 5 for legal and technical obstacles for (the effectiveness of) such requirements.

guessing what the environment is up to than having precise knowledge of how one's data match the relevant group profiles. Evidently the time problem will not be solved by Type A TETs either, and will require a long term investment in both types of TETs, experimenting different, complementary and overlapping ways of anticipating how profilers are categorising people.

1.4.4 From transparency enhancing *technologies* to transparency enhancing *tools*

Other than in our previous deliverables 7.7 (Hildebrandt and Meints, 2006) and 7.9 (Hildebrandt and Koops, 2007) TETs are now defined as legal *as well as* technological tools. In chapter 5, section 5.1 technological TETs will be discussed and in chapter 5, section 5.2 legal TETs will be discussed. This is important because we need adequate transparency rights, as instruments of constitutional democracy, as well as the technological infrastructure *to be able to* exercise those rights. The concept of Ambient Law (AmLaw),[8] coined in FIDIS deliverables 7.3 (Schreurs et al., 2005), 7.7 (Hildebrandt and Meints, 2006) and elaborated in 7.9 (Hildebrandt and Koops, 2007), is of prime importance here. It reckons that neither legal rules nor technologies are neutral tools in the hands of the legislator and the administration. Both law and technological infrastructure condition to what extent core tenets of constitutional democracy can be actualised. On top of that, law has been articulated in the technology of the script and may need re-articulation in the emerging digital technologies (Hildebrandt, 2008); (Hildebrandt and Koops, 2007). This means that TETs are not merely a way to implement existing legal rules, but should (1) be developed by the (European) legislator in close cooperation with both lawyers and computer engineers and (2) allow for contestation of their application in a court of law. These two safeguards are the two relevant core tenets of constitutional democracy. This will be further discussed in chapter 5, section 5.3 on Ambient Law.

1.5 The relevance of TETs for BBP

Why should we discuss TETs in the same deliverable as BBPs? BBP can take place by means of silent enrolment – meaning that people may not be aware that their behavioural biometric profile is registered and continuously updated. In the case of keystroke dynamics re-recognition would be enough for profiling machines to link the online behaviour of an individual person, without necessarily establishing name or physical address. Extensive profiles can be built, sold and applied, conveying life styles, intimate habits, spending patterns and personal preferences. Due to the possibility of producing such profiles without notification of the person(s) they concern, people may receive offers for targeted services without a clue of what the offer is based on (Zarsky, 2002-2003). Refined price discrimination will be possible if profiling machine 'know your price' which need not have any proportional relation to the costs of production nor to the 'price of your neighbour' (Odlyzko, 2003). On top of that risk assessments will be enabled if behavioural biometrics – used as a unique

[8] In previous FIDIS WP7 deliverables (e.g., 7.3, 7.7 and 7.9) we used AmL as an abbreviation for Ambient Law. To prevent confusion between AmI and AmL, we have decided to abbreviate Ambient Law to AmLaw.

identifier – allows linking all sorts of data across contexts, without any awareness of the person concerned. This may impact the price of insurance premiums or access to education, employment, health care etc.

BBP will in fact allow seamless, targeted, refined proactive adaptation of your environments – for the better or for the worse. The most important precondition for citizen empowerment in the context of BBP will thus be transparency: 'Am I being profiled? How am I being profiled? Which are the consequences?'

TETs, the interplay of legal and technological transparency tools, will thus be a precondition for empowering citizens to interact with their proactive environment, for instance:

- knowing that your gait allows tracing and tracking across different contexts
- finding out how your gait correlates with a group profile on Parkinson's disease (Cattin, 2002: 104)
- contesting a conviction as a psychopath that was based on a match between your facial expressions and a group profile of a personality disorder.

Some of these applications of BBP may sound rather fantastic. However, this is exactly what transparency tools should allow us to investigate: which inferences are made and applied by means of behavioural biometric profiling technologies that impact a person's choices in life? In chapter 5 the idea of TETs will be further developed.

We need to reiterate the point made in section 1.1.1 as to the fact that transparency about the potential consequences of one's behavioural biometrics does not imply that one can now change or hide one's BBs easily (or even at all). Nevertheless it is pertinent that citizens should have access to the profiles that are inferred from and applied to them. Knowing what commercial, governmental, social welfare or health car organisations know about a person, will at least allow people (1) to better anticipate the behaviour of organisations, (2) to initiate democratic participation to regulate the working of BBP and (3) to contest concrete applications in a court of law.

2 BBP cases & scenarios

After exploring the scope of BBP and TETs, we now present three scenarios to introduce possible implications of wide-spread usage of BBPs in everyday life. The main function of these stories is to make the reader aware of the promises as well as to potential pitfalls of this new technology. Because BBP is an emerging technology, mostly in the stage of prototypes, each scenario is preceded by a brief technical introduction that aims to provide a general idea of the reliability of the technologies involved.

2.1 The Smart Car (Driver Fatigue Detection)

2.1.1 Technical description (reliability)

When speaking of a smart car one usually thinks of ACC (adaptive cruise control) that keeps the speed of the car relatively constant and slows down when another car is too close, ABS (anti block system) that slows the car when is detects a potential slip, ATC (automatic traction control), BAS (brake assist) that detects emergency braking and supplements the force of the brake, ETC (electronic throttle control) that translates movements of the gas-pedal into more or less gas, LKA (lane keeping assistance) that keeps the car within the lines of the road whenever it detects that one is attempting to overtake another car in a dangerous situation.

In this scenario we introduce a BBP, developed by (Shanshan et al., 2007), that is capable of detecting the level of fatigue of drivers by measuring three different biometrics that stand for driver fatigue: pupil shape, eye blinking frequency, and yawning frequency. If the biometric profile were to be reliable in real life situations it could replace existing alcohol-tests by providing accurate information on safe driving, irrespective of whether the risky driving style is caused by alcohol, lack of sleep, medication, grief or whatever else.

The technology is based on vision and uses image recognition to process the three BBPs. Since the impact of the three elements on driver fatigue is different as well as nonlinear, the designers employ a genetic algorithm (GA)-based neural network (NN) system to fuse the three characteristics. A back-propagation learning algorithm is used to weigh values and the genetic algorithm is used to optimize the structure of the neural network. A simulation provided good results, meaning that driver fatigue was reasonably exactly detected.

Evidently the testing of this prototype in a controlled experiment cannot be equated with real life situations. Further testing will be necessary and it is unclear as yet, how reliable these types of BBPs will be in the near future.

In developing a scenario we assume that the technology – at some point in the future – has enough reliability to convince consumers, car manufacturers, insurance companies and/or regulators. The aim of the scenario is to provide a sense of the usability and the utility of the technology, as well as the impact it may have on our lifestyle. The aim is also to demonstrate anticipated threats that need further investigation in the legal and socio-ethical chapters.

2.1.2 Scenario: Who is driving?

A day on the road

John Diamond has a really 'smart' car. Besides its 'cool' colour and smooth way of driving, it has a series of smart applications that should enhance safety and prevent him from getting caught up in a traffic jam. John is very proud of his car. When he gets up in the morning he is already looking forward to getting the car started.

This morning John is planning a trip to his office, which is not that far (about 20 miles). When he gets into the car he takes his breakfast with him, since he was a bit late in getting up. Last night he had a late dinner with friends so he is still a bit tired, but hopefully some coffee and a fresh roll will do the job. When he starts driving he notices that the car has shifted to a slow 'mood', meaning that he needs more effort to push the gas-pedal and is generally discouraged from fast driving. John does not like to be slowed down like this but he accepts this 'mood', knowing that it will lower his insurance premium and reduce risking an accident.

Later the same day John is off to one of his clients. He had a productive meeting with two of his colleagues and he is feeling great. The car seems to guess his mood and does not interfere with his driving-style.

John has lunch with his client, who is Italian and loves a good lunch. They pick a nice Italian restaurant and have three courses, during which they discuss future engagements. To celebrate an agreement that is expected to be very beneficial to both of them they order an excellent Amarone and share it between them. In the old days – before John had his 'smart car', he would not have dared to drive after half a bottle of wine. These days he takes the risk, knowing that the car will determine whether he can still drive safely. The success of this technology has initiated a new articulation of regulatory traffic offences. Whoever has a Driver Fatigue Detector in operation in the car, will not be tested for his alcohol intake, if the car prevents driving beyond a certain level of fatigue. However, after getting into the car John suddenly feels very tired. The combination of last night's pleasures, the heavy lunch and the wine create a sudden lapse in his concentration. Within minutes the car signals that John has transgressed the threshold of fatigue-detection, he is forced to park the car and calls a taxi.

Back in the office John asks his secretary to pick up his car, hoping he will be OK by the end of the day (getting back home by car). His secretary sits down in the car but it does not start. The Driver Fatigue Detection – geared to John's profile – calculates that the secretary is too tired to drive safely. The system does not 'know' that the secretary has a habit of frequent eye blinking that confuses the car and disables starting the car. He has to call a taxi to get back to the office, sending another assistant to drive the car. Luckily this assistant has a more regular profile, so she can easily bring the car to the office. However, she loves speeding and taking risk (especially in her boss' car?), knowing the car has Adaptive Cruise Control, so not much can happen.

In the evening – after a double espresso – John tries the car. However, the car is now used to the sharp driving style of the assistant and figures out that John must be very tired to be so prudent. It refuses to continue and John has to call another taxi.

Another day on the road

The next day John – still irritated with his 'cool' and 'smart' car – takes measures to prevent further obstructions. First, he tries dark sunglasses to befuddle the car. However, the car is no fool and refuses to start. It indicates that John should use the special sunglasses that allow the car to 'see' his eyes. John gets back into the house and returns with special contact lenses that change the colour of his eye, and also transform the shape of his pupil. He bought them on the internet some time ago, both for the fun of it and because they were advertised as breaking the car's fatigue detection system. The car 'buys' his new pupil shape and does not interfere with his driving habits. John feels a bit guilty and drives careful, aware that he is not under surveillance anymore.

This day John has to take a long drive in order to meet a client. He settles himself for a long period of quiet driving, knowing that his Adaptive Cruise Control, Lane-Keeping-Assistant, Automatic Traction Control and Automatic Throttle Control will keep him safe and he forgets that he is wearing lenses that hide his pupils. The fact that all these automatic control systems are in working order means that chances to have an accident are very low, which makes a long drive very boring. The car has a personalised audio system that plays his favourite music and – normally also attunes the choice of music to potential loss of focus. Since the car cannot see the real size of his pupils this does not happen adequately. John gets a bit bored and begins to doze off, while the car plays relaxing music. Upon entering the city of destination John notices that he is late and begins to drive a bit faster. The car thinks he is alert and does nothing to prevent him, since he is within the official speed limit. Suddenly a child runs onto the street from between parked cars. An accident happens causing serious injuries to the child.

The day(s) after

John is devastated. He knows that he might have collided with the child even if he had not been wearing the lenses, but he is also aware that he might have reacted differently and prevented the accident. He is wondering whether he should admit to fraud since he used lenses.

John is convinced that the car's monitoring system will give away his successful attempt to mislead the car. Therefore, he decides to call the police and the insurance company to inform them about his actions. He does not know that the insurance company has already started a procedure to inform him that they will not pay any expenses, since they suspect him of fraud.

John's insurance company is continually processing his driving profile. Data for this is transmitted from the car for charging his premium according to his risk on the road. When John uses high risk roads, in dense areas, where many accidents have happened before, he pays higher premiums. The data processing software has detected sharp differences in John's profile recently. Matching with other profiles in their database has shown that John's assistant (who happens to be one of their clients) and two other, unknown persons have been driving the car. The insurance company has not yet identified one of the unknown drivers as John wearing lenses. However, the car's monitoring system will reveal this later, when these data have been accessed. The police have already required access to the data held by the insurance company, in order to assess potential evidence of a criminal offence.

2.2 Web Profiling (Key Stroke Behaviour)

2.2.1 Technical description (reliability)

Every person has his/her own personal keystroke. Elderly people may type with one finger, whereas secretaries may type hundreds of words per minute. But even among people of the same group, differences are large enough to differentiate individuals.

Typing on the keyboard of a computer generates two types of interactions that IT-people call "events". One is generated when the user presses the key, it is the "Key-Down Event"; the other is generated when the key is released, it is the "Key-Up Event". The computer's operating system reacts to those two types of events.

Basically, keystroke behavioural biometrics measures the time during which the key remains down and the interval between two keys (means the difference between a key-down and the corresponding key-up, or the key-up and the next key-down). The second interval can be negative, since two keys can be pressed successively or simultaneously.

A pattern is computed for each person grouping the usual durations and intervals of his/her keystroke. This pattern is then compared to the actual keystroke of the person the system wants to identify, and if the distance remains above a certain level, the person is identified. Different systems exist based on this principle. Some of them are already products sold on the market; as for instance Biochec[9] or Biopassword Inc..[10] There exists also an open source solution developed at the Bern University of Applied Science.[11] Whereas all the systems are based on the intervals between key ups and key downs, there are major differences between them. Some measure the times for typing the same word or pass phrase; during the learning phase, the user retypes many times (15 for instance) the pass phrase, and the system learns the way the phrase is normally typed. Since the phrase is always the same, regularities can be found even on short sentences: according to their promoters, the Biopassword system has an EER of 3%. Other systems are more open, they work on any type of text. The system lets the user type any text (or any given text) and computes a generic profile. Such a profile contains the habits of the user typing any text, so can be used at any moment (not just for the login); it is also more resistant to attacks, since the data typed can not simply be copied.

The algorithms determining if a user matches its profile are also quite different. Whereas some systems simply use standard distance (Bovet and Liechti, 2007), some use more sophisticated neural networks (Revett et al., 2007), or wavelet technology (Chang, 2006) to recognize users.

2.2.2 Scenario: who is typing?

Following the 2008-2009 scandals involving back-office employees having stolen the passwords of other employees (responsible for a disaster costing at least 10 billion euros),

[9] www.biochec.com
[10] www.biopassword.com
[11] wb.chillzone.ch

John Diamond's employer decided to protect the network resources using biometrics. They have deployed an infrastructure, such that web-mail and shared file servers can only be accessed by people authenticated by their keystroke behaviour. They have deployed such a system on the entire infrastructure of the firm. The CIO was charged to explain the goal of all this to the employees. He therefore organized meetings and discussions in each of the services. During the presentation talk, John realized how unprotected his own systems were without the protection of biometrics. So he decided to protect his personal computer and cellular phone using keystroke recognition.

The presentation has convinced John of the efficiency of the protection offered by keystroke biometrics. He is certain now that his daughter Meg can not use his computer and mess-up his files. He is moreover sure that helpdesk personnel don't have any possibility to access his account.

Two visits that change one's point of view

But last week he received in his office two visits that changed his vision of the system. First his son John Junior started his part time job in the IT department of John's firm. He visited his father in his office and they installed a new add-on for Firefox on his computer. This add-on is a key logger, which measures the keystroke and is able to fake it. Junior explained to John that the key logger could register anybody's keystroke and use the stored data to fake his/her identity when connecting a web site, but John isn't very interested in technology, so he let him do. Unfortunately, the firm's CEO Jake Thomson visited John's office at that moment and wanted to know what John was doing. Unable to answer, John mumbled something. John Junior took the opportunity and in the course of their conversation he suggested that Thomson could use John's PC to consult his (the Thomson’s) web-mail account. Naturally, John had previously turned-on the Firefox key logger.

Once the boss was gone, they discovered the treasure hidden in this machine. Not only had they learnt that the boss's password is the secretary's first name, but the key logger was also able to fake the pace at which it was typed, and so they could access the boss's email.

Since then, John's faith in behavioural biometrics on the web has largely been supplanted by disbelief. It is so easy to spoof that even his teenager-boy could enter his boss's private e-mail account.

Where an accident destroys John's life

As described in the previous scenario, John had decided to wear the special lenses allowing him do drive without being monitored by the driver fatigue detector; and his car crashed. Unfortunately his right arm was broken in the accident and John's right hand cannot be used for the next two months. Once in the hospital he wants to notify his office about his accident and tries to phone his secretary, but he can't. It is impossible for him to dial any number, since his phone reacts as if it were stolen. Since John is not seriously injured, he is authorized to return home soon. He then tries to send an email to his secretary, but can't log onto his computer. He is unable to access the internet. Neither his phone, nor his email works. He decides to wait for his son, since teenagers always know better how to use Hi-Tech devices.

But John Junior doesn't have good news. He didn't use his program for recoding the keystroke behaviour of his father and therefore doesn't have any possibility to access his father's email account. But then he remembers that John's boss Thomson has the right to read any email, so the only possibility remaining is to fake the password of Jake Thomson and to log in the system as super user. John can finally read his emails and decides to answer some of them, without noticing that emails are signed with Jake's address!

The day after

The next morning, when John arrives at work he is invited by Jake to his office. This is the essence of their conversation:

"You used my email account to send emails yesterday. Last week somebody sent pornography using my account. You understand that I know you were the author of both, and therefore I have to dismiss you!"

John has completely lost any faith in biometrics on the web. Moreover, he cannot use his computer until complete recovery.

His boss Jake, however, is very enthusiastic about the keystroke profiling software. After the incident with John, he has informed himself about its features and discovered that the patterns may be used to indicate fraud. It turned out that people who committed fraud in the past had a very typical keystroke profile. This profile was matched with the profiles of the current employees and there were five matches. After confronting them with this information, three of these employees admitted to fraud and were arrested and convicted. This has saved the company hundreds of thousands of Euros. The other two people who matched the profile were registered in the fraud database of the police. They were arrested by the police, but had to be released because there was not sufficient evidence against them. Because of this incident, one of them decided to look for another job. The other was fired by Jake, because he did not trust this employee. Even though hard evidence was lacking, he thought it was better to be safe than sorry. Afterwards, no incidents of fraud have taken place.

2.3 Support for the Elderly (Gait & Emotion detection)

2.3.1 Technical description

Emotion recognition based on facial expressions and voice analysis comprises an extremely challenging research field with interesting business applications. Observations and research support the idea that people are more familiar with classifying facial expressions then with the classification of other means of expression (Boyatzis and Sayaprasad, 1994; Fridlund et al., 1984).

Many theories exist concerning the determination and the definition of emotions. The most recent one is the "basic emotions" theory. According to Ekman's group (Ekman et al., 1987), six archetypal emotions exist: surprise, fear, disgust, anger, happiness, and sadness. This theory is based on the idea that emotions are comprised of qualitatively distinct types of biological states. Facial expressions and speech tone are two major ways for emotions

expression. In this scenario states of e.g. being awake, irritation, anger, sadness, pain, a cheerful mood are detected by means of BBP.

We can compare the performance of existing emotion classification techniques, due to the varying databases used for testing, the use of different validation of the mechanisms with different content and size as well as due to the fact that they explore different basic emotion categories. Typically, emotion classification as well as pattern classification includes three main steps; acquisition, feature extraction and selection and classification (Fasel and Luettin, 2003); (Scherer, 1999). The first one deals with the isolation of the material with biometrical significance. The extraction of features invariant to culture, speaker, language and context comprises a rather difficult task. However, the performance and reliability of an emotion recognition system largely depend on the features selected. When it comes to large scale systems or systems operating in real time commonly a reliability compromise is required so that performance doesn't degrade significantly. In fact, extracting and selecting complex features or a great number of them would increase the accuracy of the results but still performance issues would rise – especially when real-time operation requirements are posed.

Distributed processing of the images or voice signals can help reduce the temporal overhead of the emotion recognition processes. In fact, running the emotion and pattern classification mechanisms on a Grid Infrastructure (Foster, 2002) and thus parallelising the process allows using more complex and yet accurate features for the classification process without posing performance limitations.

2.3.2 Scenario: "InLiFE" (Independent Life For Everyone) Application

Who is Mr. Carlson?

Mr. Carlson is a 75 years old man who suffered from a stroke 2 years ago and now faces mobility problems: he is not impaired but can't move in an agile way either, having less strength in the left part of his body and feeling pain in both his legs. Hence, he is not that willing to be walking around and is also afraid of falling. Moreover, he suffers from a mild diabetes that forces him to be careful with his diet and take some pills twice a day. Due to high blood pressure he has to take another pill once a day as well as an aspirin against blood coagulation.

Although his children offered to host him, Mr. Carlson does not want to move with them as he needs to feel independent and he prefers to stay in his neighbourhood where, whenever possible, he can meet some old friends at the cafe after lunch for a cup of tea. However, as he needs to stay at home most of the time and as he is not agile in manipulating objects, whereas also his vision is not that good anymore, he cannot exercise any hobbies and he feels quite lonely most of the time and often even feels useless and sad. His children worry about him and about the quality of his daily life and they want to know whether he is fine.

A typical morning

Mr Carlson is usually awake since early in the morning as he does not sleep much. However, it is too early for him to get up, so he prefers staying in bed listening to the radio. Sensors on the mattress and the pillow detect Mr Carlson's movements, heart rate and breathing and indicate that *he is awake*. After checking with his profile that it is a usual time for him to wake up (so as to avoid waking him up during the night), the radio is turned on automatically broadcasting his favourite channel. As it is a cold winter morning, the heating of the house is automatically turned on so that the house will be warm when Mr Carlson gets up. Since Mr Carlson seemed *rather irritated* during the past days (his voice as captured by the microphones reveals anger, his movements at bed while he is asleep are sharp) instead of an alarm clock ringing, a soft voice notifies Mr Carlson when it is time to get up. **"InLiFE"** automatically raises the blinds. Mr. Carlson is not that eager to get up but the light is quite annoying and so he decides to get off his bed. As he moves towards the door, he trips over a chair and falls down. The camera at the corner of the room detects the incident and a sweet voice asks him if he is OK and encourages him to slowly stand up again. The camera detects that there is a table next to him and suggests that it could support him to stand up. Mr Carlson tries to stand up and finally he makes it. The time he needed to get back on his feet is recorded. The camera detects no pain on his face and no change in his usual way of walking, but it still asks him some questions to verify that everything is Ok. Thus, it asks Mr Carlson, "Are you OK? If yes, then please raise your hand". Mr Carlson does respond but in the meanwhile Rita - Mr Carlson's daughter - has been notified about the event and rings him to make sure he is OK.

Though he loves his daughter, Mr Carlson is irritated by the fact that she is notified of this incident, which he thinks to be too trivial and harmless for an intrusion of his private life.

Out for a walk

After breakfast Mr Carlson should go for a walk, as his legs require daily exercise. But today Mr Carlson seems *quite sad* and does not seem to be willing to go out. The camera detects he is not going out, because he is sitting in the armchair and it also detects his mood through his facial expressions, his still gaze and the inert way of sitting on the chair. Given that he didn't go out yesterday (due to the rain that day), Mr Carlson is encouraged to go out by a gentle voice through the microphone, whereas some nice outdoor photos are shown on the mirror and nice music from Mr Carlson's youth is played through the speakers, all aiming to cheer up Mr Carlson, hopefully inducing him to go out. Most days it would have worked, but not today, Mr Carlson decides to stay in his chair. The expression on his face is still. The **"InLiFE"** decides some external human interaction is needed so it contacts his daughter, who is currently at work, informing her about the problem. Rita, using her mobile phone with a camera, the output of which is streamed to Mr Carlson's TV, talks with her father for a while and manages to convince him to go out. As he is about to leave the house and given that he normally forgets to dress well, **"InLiFE"** advices him to take his thick coat as it is quite cold today. Mr. Carlson remembers his late wife, who always told him to wear his thick coat on moments like this. He feels depressed because his misses the care of his wife, which does not compare to the 'care' of the adaptive environment that surrounds him.

Back from the walk

Mr Carlson goes out and as soon as he steps in the street he meets an old friend. He talks to him for a while about their youth, after which he feels sad again and irritated, so he heads back home. **"InLiFE"** is tracking him and detects that much less time than usual has passed before he came back, so it concludes that he has not really walked. It detects *sadness and irritation* both on this face and in his walking pattern. He takes out an old photo of his youth, holds it and suddenly he starts crying. **"InLiFE"** thus alerts for a possible case of a depression event. It notifies Rita in order for her to call him and encourage him, but Rita does not respond. Thus, **"InLiFE"** calls Mr Tomson – a close friend of his who lives in the neighbourhood – to check on Mr Carlson, urging him to go by to spend some time with him.

The bell rings but Mr Carlson does not want to open the door because he is day dreaming and wants to be left alone. But as **"InLiFE"** has called Mr Tomson, the door opens automatically and he enters the house. Initially Mr Carlson is irritated and shares only a few words with Mr Tomson. But after a while the conversation takes on and Mr Carlson gets in a much better mood, whistling and smiling. **"InLiFE"** will adapt to the new mood in all the interactions.

Later that morning the cleaning lady arrives, who also prepares his lunch. When Mr Carlson, curious to see if his lunch is ready, goes to the kitchen to check on the oven, he triples over the carpet and falls down. **"InLiFE"** *detects the fall*, but since it is aware that the cleaning lady is in the house, a voice is heard in the room informing her that Mr Carlson *has fallen in his room* so that she can go and help him. It seems that despite the fall he is all right.

After lunch

After lunch Mr Carlson goes to have coffee with his friends, but first he usually watches news on the TV. **"InLiFE"** switches on the TV to the news channel automatically when it detects that Mr Carlson is sitting in his armchair. When he goes back home from the café, he looks for his keys but he realises that he has left them indoors, so Mr Carlson presses the bell and says his name. **"InLiFE"** recognizes the voice and checks the fingerprint via a device embedded in the ring bottom; the door is opened automatically. As he has left his keys at home twice this week, the next time he wants to get out, a message will appear in the door reminding him of the keys.

Heart Problem

Mr Carlson must have dinner early because he has to take his pills, so he approaches the fridge and the screen embedded in it shows the possible menus, depending on the fridge's content, on Mr Carlson's health status during the past days and on his preferences (e.g. he never has the same dinner twice a week). Suddenly, Mr Carlson put his hands on the left part of his chest. The **"InLiFE"** recognizes a gesture that could be revealing a heart problem (e.g., ischemic episode). The microphones capture sounds such as "my heart" with a quiver in his voice, while the cameras capture him slowly sitting down on the chair and having difficulties to breath. After some minutes Mr Carlson is fine. However, **"InLiFE"** informs his doctor about the event, who goes by the house. The house door automatically opens at his arrival and he enters the house to check on Mr Carlson. Mr Carlson seems rather disturbed by

that. Fortunately, Mr Carlson did not have any serious problem and the doctor advices him to rest and eat a light meal and so he does.

The doctor does, however, ask Mr Carlson to make an appointment with the oncologist. The information transmitted by "**InLiFE**" has been automatically analysed and Mr Carlson was "diagnosed" as someone with a 95 % likelihood of having stomach cancer at the moment. This profile had been sent to his doctor and as he has not been examined yet, further testing is required to see whether any treatment is required.

Tears

Later in the afternoon Mr Carlson sits down with a set of letters, written to him by his late wife. He reads them and tears fill his eyes, as he remembers the beauty and love of his wife. He is touched by the beauty of his memories and feels grateful for the life they shared. "**InLiFE**", however, again 'thinks' that he is having a depression, calling his daughter and his friend Mr. Tomson. When they enter the house, Mr Carlson gets very upset with the intrusion of his private sphere, he shouts at his daughter and friend and throws them out of the house. He sits down again and hopes that "**InLiFE**" will not call a psychiatrist to intervene.

Going to sleep

In the evening, Mr Carlson has to take three pills, one for diabetes, one for blood pressure and one for blood coagulation. As the cameras capture Mr Carlson going straight to bed, **"InLiFE"** decides to remind Mr Carlson that he must take his pills by winking a light next to them. After he takes the pills, Mr Carlson likes reading cowboys books while lying in bed. **"InLiFE"** offers a set of western books to be displayed on the wall of his bedroom, and Mr Carlson chooses one of them. The book is displayed in big font due to Mr Carlson's sight problems. **"InLiFE"** detects that he yawns and does not read the lines of the book though he is not sleeping yet and thus induces that he is bored so a message is prompted asking him if he would like to read another book. Mr Carlson chooses to read another book and after a few minutes he falls asleep while he is reading. **"InLiFE"** detects that and stops the book show, switches off the lights and the heating.

3 Vulnerabilities generated by the usage of BBP

3.1 Introduction[12]

BBPs are usually produced and used with particular purposes in mind. The user of these profiles expects certain advantages when these goals are reached. In the examples described in the previous chapter, these characteristics are used for safe driving, for identification of computer users and for independent living. Such applications may be very useful, assuming that the technologies used are sufficiently advanced and not prone to (too many) errors. When smart cars do not allow other drivers, this may be undesirable for the car owner. When keystroke behaviour may easily be logged, it may facilitate identity fraud and may, as such, be an unreliable technology. Independent living may be very desirable for elderly people, but when the technology used has too many false alarms, there is the risk that people may no longer respond in case of a real emergency. However, usually such errors tend to disappear when the technologies are further developed. It is likely that the performance standards mentioned in Section 1.3 (FRR, FAR, EER, ROC) will be increased, although they may never become perfect.

But even when technologies do what they are supposed to do, without too many errors, they may cause some unintended problems.[13] The Internet, for instance, allows large scale exchanges of information, for which purpose it was designed. At the same time, however, some of the information may be harmful, such as information to build nuclear devices, hate speech and child pornography. Sometimes it depends on the perspective whether particular information is harmful. For instance, blasphemy may be considered part of freedom of speech by some, whereas it may be considered as infringing freedom of religion by others. BBPs that predict life expectancies may be nice to know for people who are expected to become very old but may be very confronting for people with limited life expectancies. Information on driving behaviour may be interesting for insurance companies to calculate accident risks, but may be very problematic for people whose insurance is cancelled based on such information. As such, most of the advantages and disadvantages of BBPs are dependent on the context and the perspectives of the persons involved. In this chapter, several ethical aspects of using BBPs will be discussed. Particularly the vulnerabilities that BBPs may create for both individuals and society will be described in more detail. Therefore, in this chapter, a moral point of view is taken, i.e., a willingness to take the vulnerabilities of people into account.[14]

---

[12] See also the analysis of group profiling and its implication presented in FIDIS delivery 7.2 (Hildebrandt and Backhouse, 2005).

[13] For a more detailed discussion, see also (Custers, 2004).

[14] See also (Frankena, 1973: 113), on the moral point of view. According to Frankena, a person is taking a moral point of view if (a) he is making normative judgements about actions, desires, dispositions, intentions, motives, persons, or traits of character; (b) he is willing to universalise his judgements; (c) his reasons for his judgements consist of facts about what the things judged do to the lives of sentient beings in terms of promoting or distributing non-moral good and evil; and (d) when the judgement is about himself or his own actions, his reasons include such facts about what his own actions and dispositions do to the lives of other sentient beings as such, if others are affected.

Although examples from different contexts will be described below, it should be mentioned that the aim of this chapter is not to describe all the different contexts in which BBPs are used and all the players involved in these contexts. Rather, in this chapter, vulnerabilities of those involved will be described from a general perspective. These vulnerabilities, though they may vary in seriousness and urgency, are often similar in different contexts. For instance, when BBPs are used for selection, they may infringe someone's autonomy. This is similar in contexts like medical profiling, direct marketing and criminal investigation and prosecution. To what extent the autonomy of the person involved is infringed may vary, as a patient may be much more vulnerable (because of her disease, her dependency on others and her deep and non-voluntary involvement) than an Internet consumer. Being spammed on the basis of BBPs is a much less serious moral problem (if at all) than being subjected to a particular medical treatment without any consent. This may also depend on the context and the perspective of those involved. For instance, when looking at the cases in the previous chapter, it is likely that Mr. Carlson is willing to exchange some privacy and autonomy to be able to live independently.

Before starting to discuss any of the vulnerabilities that BBPs may cause, it is important to underscore the advantages that BBPs may cause (Custers, 2005). BBPs are created and used for a reason. Smart cars may increase driver safety, key stroke profiles may prevent unauthorized computer access and emotion detection may provide (extended) independent living for elderly people. These examples are on a small, individual scale, but BBPs may also influence society on a larger scale, for instance when it turns out that specific driver fatigue frequencies are an indicator for unemployment or when specific key stroke behaviour relates to a potential terrorist threat. As such, the BBPs may be used by government institutions to decide and act upon, to perform their publicly approved tasks, e.g., addressing these groups with unemployment programs or arresting terrorists. The people working with BBPs do not (usually) mean to do any (intentional) harm. They are simply trying to do what they were asked to do, to do their job properly, such as finding target groups for reemployment programs, singling out terrorists, or assessing the efficacy of new treatments for cancer. It is important to keep those advantages in mind, because otherwise all the vulnerabilities that BBPs may cause, may easily lead to the conclusion that BBPs should be prohibited.[15] Although in some cases this might be true, it seems more reasonable to strike a balance between the advantages and disadvantages of BBPs and then decide what to do. This may often lead to additional measures mitigating any negative effects, while allowing the positive effects of BBPs at the same time. Again, such a balance is dependent on the context and the players involved.[16]

The advantages of BBPs also depend on the context in which they are used. Nevertheless, some advantages may hold for many or most contexts. The main advantages concern *efficacy*, i.e., how much of the goal may be achieved, and *efficiency*, i.e., how easily the goal may be achieved. For instance, key stroke behaviour may be very effective to single out target groups

[15] Controversial profiles often involve sensitive personal data, such as ethnic background, religion, political and sexual preferences and criminal records. Racial profiling, for instance, involves physiological biometrics (see section 1.1), but these may be coupled to BBPs. When it turns out that people of particular ethnic or religious backgrounds are more involved in crime, this may cause discrimination, stigmatization and social polarization.

[16] For an example of a more detailed discussion of the perspectives of the different players involved in a medical context, see (Custers, 2004).

for computer courses. Drivers that are often tired may be a target group for sleep regulating medication that can effectively be addressed. Offering courses or medication to these groups may be efficient, as people who do not fit the profile need not be bothered. When these groups can be addressed at a personal level, for instance, by email or by messages on their on board units, this is much more (cost) efficient than by a campaign or advertisement on national TV.

Data mining and profiling may process huge amounts of data in a short time; data that is often too complex or too much for human beings to process manually. When many examples are present in databases, (human) prejudices as a result of certain expectations may be avoided. As such, BBPs may be used as rules of thumb that are more accurate than intuitive rules of thumb. In this respect, it is important to distinguish BBPs that are personal profiles (describing a single individual) and BBPs that are group profiles (describing a particular group). *Personal profile BBPs* describe, for instance, driver fatigue behaviour of Mrs Walker and key stroke behaviour of Mr. William Jones. *Group profile BBPs* describe driver fatigue behaviour for truck drivers or people in Louisiana and key stroke behaviour for managers, cell phone owners or sexual offenders.

BBPs, particularly group profiles, may be a useful method of finding or identifying target groups. In many cases, group profiling may be preferable to individual profiling because it is more cost efficient than considering each individual profile. This *cost efficiency* may concern lower costs in the gathering of information, since less information may be needed for group profiles than for individual profiles. But higher costs may also be expected in the time-consuming task of approaching individuals. While individuals may be approached by letter or by phone, groups may be approached by an advertisement or a news item.

Another advantage of using BBPs for group profiling rather than individual profiling is that group profiles may offer more possibilities for selecting targets. An individual may not appear to be a target on the basis of a personal profile, but may still be one. Group profiles may help in tracking down potential targets in such cases. For instance, a person who never travels may not seem an interesting target to sell a travel guide to. Still, this person may live in a neighbourhood where people travel frequently. She may be interested in travel guides, not to use them during holidays, but to be able to participate in discussions with her neighbours. A group profile for this neighbourhood predicts this individual's potential interest in travel guides, whereas an individual profile may not do so. Such selection may also turn out to be an advantage for the targets themselves (Van Wel, 2001). For instance, members of a high-risk group for stomach cancer, such as Mr Carlson, may be identified earlier and treated, or people not interested in cars will no longer receive direct mail about them. However, as will be discussed below, selection may be unwanted or unjustified, in which case it may be a disadvantage for the target.

BBPs for group profiling may be more useful than no profiling at all. Without any profiling, without any selection, the efficiency or "hit ratio" of advertising is usually poor. For instance, advertising using inadequately defined target groups, like on television, is less efficient than advertising only to interested and potentially interested customers. As another example, research has shown that screening for breast cancer among the whole population would not give very different results from screening women in a particular age group only (Coebergh, 1991: 41-49).

3.2 Selection, unjustified discrimination

One of the most obvious risks of BBPs is that they may be used as selection criteria in a way that is considered unjustified by group members or others. Selection is one of the main applications of profiles. Selection to trace the incidence of diseases and provide earlier and better therapy to patients may be useful. But selection may also be used for more controversial issues. When selection for jobs is performed on the basis of BBPs, this may lead to discrimination.[17] For instance, an employer who is hiring new drivers, may want to know the accident history of any candidate that is applying. When slow key stroke behaviour is an indicator of low productivity, an employer may be interested in this as well, even more when key stroke behaviour appears also to be an indicator for frequently reporting ill. The cases in the previous chapter also contained examples of selection. For instance, profiles were used to indicate John's fraud in his car, the fraud in Jake's company and the probability of Mr. Carlson's having stomach cancer. In some of these cases, the selection may be justified, but in other cases, the selection pointed at the wrong people. For instance, of the five employees that may have been involved in fraud, two may have been innocent. Selection may also take place in purchasing products, acquiring services, applying for loans, applying for benefits, etc.

3.3 Stigmatisation

Some of the group profiles constructed by companies, government, or researchers may become 'public knowledge', which may lead to the stigmatisation of that particular group (Vedder, 2000).[18] For physiological biometrics this is quite obvious, as the example of Islamic terrorism shows: in Islamic terrorism Muslims are more likely to be terrorists than non-Muslims. However, the number of Muslims who are actually terrorists is extremely small. It's is hard to find a terrorist, because there aren't that many in our society. If Al Qaeda has 5000 members, this is still only one in a million worldwide.[19] But even though almost no Muslim is a terrorist, we keep talking about Islamic terrorism. Such stigmatisation may also occur for BBPs, for instance when it becomes known that people with frequent driver fatigue are more likely to attract HIV. This does not mean that Muslims are terrorists or people with frequent driver fatigue have HIV. Still, society may treat them differently when people have such knowledge in their minds, as if they have or might have these characteristics. People often seem to have such a tendency of translating statistics into erroneous conclusions. There are many examples of stigmatisation and these examples are not always limited to the ones usually mentioned in human rights documents, such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, or birth.[20]

---

[17] A case study in the U.S. showed that discrimination as a result of access to genetic information resulted in loss of employment, loss of insurance coverage, or ineligibility for insurance. All cases of discrimination were based on the future potential of disease rather than existing (symptoms of) diseases. See (Geller et al., 1996: 71-88).
[18] See also (Last, 1996).
[19] Example from (Schneier, 2007).
[20] These are the criteria explicitly mentioned in Article 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms, prohibiting discrimination.

In the case described in the previous chapter, one of the employees accused of fraud decided to find another job. Even though there was not sufficient evidence to convict this employee of fraud, his employer retained a lack of trust. When no conviction takes place, this may be because he is guilty but evidence was lacking or because he is innocent. When applying for a new job, the registration in the fraud database of the police may turn out to be something that has to be explained to a new employer.

3.4 Confrontation

When people described in BBPs get to know the contents of the profiles, they may discover information about themselves they did not know before. For instance, when BBPs are used for early diagnosis or the prevention of disease, it is possible that people in risk groups be approached with a warning, such as in the case of Mr. Carlson's stomach cancer. In this way, people are confronted with their health prospects, without having requested to be given such information about themselves. Especially in the case of very negative group profiles, such a confrontation may have a large impact on people's lives. Apparently healthy people may be confronted with the fact that they may only have a limited amount of time left, which may upset their lives and the lives of others. In some cases, people may prefer not to know their prospects while they are healthy. These problems may become even greater when little or no treatment is available.

Confrontation with harmful information, for instance, with a limited life expectancy, may cause so much distress to a data subject that he may have preferred not to have such information. In such cases, a data subject may prefer 'not to know' to awareness.[21] However, there are several practical problems in the use of a right to know. For instance, how can a person decide (in an informed way) not to know, if it is not clear what there is to know?[22] Especially in the case of data mining, the unpredictability of the results of this technology may raise difficulties here.[23] Another problem is that is often necessary to provide particular information that is already available to obtain informed consent. This information may already contain parts of the information that a person may not want to know.

3.5 Limited information supply

Another type of risk of BBPs involves one-sided information supply. This may be caused by *customisation*, through which companies try to approach people (customers) in a manner that corresponds with their personal preferences.[24] According to most companies, good service typically includes giving a great deal of attention to a customer and trying to fulfil his needs and wishes.[25] An example of this is an electronic newspaper. Suppose that an electronic newspaper company discovers, by data mining key stroke behaviour, that a particular group, say students, are significantly more interested in international news than in other news. Customisation may then involve that each time a student logs in, he is provided with more

[21] See also (Chadwick et al., 1997). For a further discussion, see also (Hermeren, 1999).
[22] (Macklin, 1992).
[23] The technologies involved may be explained and some possible outcomes, including its reliability, may be suggested.
[24] See also (Sujdak, 2001).
[25] Note that also governments are currently trying to provide more service to citizens by using personalisation and customisation.

international news, which is considered to be good service. But as a result, the student may be provided with less sports news, economic news, etc. Thus, although customisation may lead to a perceived better service, it may also lead to one-sided (or at least limited) information supply. The well-known Internet bookstore Amazon.com, for instance, already provides users with customised offers based on former purchases they made.[26]

3.6 De-individualisation

Although it may seem that BBPs lead to a more individual approach (e.g., by customisation), the use of group profiles may, in fact, lead to *de-individualisation*. This is a paradox. Group profiles result in a tendency to judge and treat people on the basis of their group characteristics instead of on the basics of their own individual characteristics and merits (Vedder, 1999a). Thus, the use of profiles is likely to lead to a more one-sided treatment of individuals. Besides, individuals may be given an identity that is not of their choosing (Bygrave, 2002). Note that this may also be the case for personal profiles.

Still, the negative effects in the case of group profiles may be larger because of non-distributivity, when the characteristics ascribed to group members may not be valid for them as individuals. *Distributivity* (Vedder, 1999b), i.e., the validity of a group characteristic for each member of the group as an individual, is an important factor in the reliability of the use of group profiles. When more than one group characteristic is considered at the same time, the distinction between distributivity and non-distributivity becomes more complex and the distinction between monothetic and polythetic group profiles may be more useful for determining the reliability of the use of group profiles. When at least one property is uniform among all members of the group, this is referred to as a *monothetic* profile. A group profile is *polythetic* when members of the group share a large proportion of properties but do not necessarily have a property in common.[27]

Where members of a group share a large proportion of properties but do not have one particular property in common, it is possible that no overlap in properties occurs among all group members. For instance, the diagnosis of many diseases is based on a checklist for the presence of particular symptoms. When a patient has, say, four of the eight listed symptoms of a disease, this may be sufficient to diagnose the disease. Another patient, having the other four of the listed symptoms, may also be diagnosed with the disease. Although both patients now have in common that they belong to the group of sufferers of this disease, they do not have one symptom in common. Polythetic profiles may present some additional problems in linking statistical relations with causal relations.[28]

3.7 Moral principles

The disadvantages of BBPs described above provide an overview of the vulnerabilities they may cause, mainly to the data subjects involved. All these disadvantages may be contrary to the needs, interests and preferences that individuals may have. This may conflict with the

[26] On the Internet, besides cookies, even secret programs, called *spyware*, are used to collect data for customisation.
[27] This is what Wittgenstein has called a family resemblance.
[28] Monothetic and polythetic group profiles are often the result of multiple causality.

moral principle of doing good (or doing no harm).[29] It may also conflict with other principles, such as autonomy, privacy and individuality. Autonomy involves that people are respected as individuals with control over their own lives. Typically, the disadvantages of BBPs described above, such as selection and confrontation, limit the possibility of individuals to exercise such control. They are increasingly being judged by others, based on information that is available on them in the BBPs. Therefore, the effects described above may lead to unwanted intrusions and/or perceived loss of autonomy (Ravenschlag, 1990). Similarly, it may lead to a perceived loss of privacy, as people are being assessed on information collected on them they may not be aware of.[30] The same is the case for individuality, which also focuses on the singularity of persons. Individuality suggests that people should be considered to be unique individuals. BBPs, particularly group profiles, may violate this, as people are being considered as part of a group. In some cases, characteristics ascribed to groups may even not be applicable to the group members as individuals. For instance, when 95 % of the readers of Car Magazine are male, this does only hold for unidentified members of this group; an identified reader of Car Magazine is either male or female.

Apart from the perspective of the individuals involved, the disadvantages of BBPs may also conflict with moral principles concerning the relations between groups and society. For instance, BBPs resulting in discrimination or stigmatisation may conflict with the principles of justice and solidarity. For instance, when insurance companies using BBPs identify high risk groups, it may be questioned whether they should be allowed to refuse these groups health insurance. This may have as a result that particular persons will not be insured and are left on their own. The question is whether this is right or wrong. Furthermore, it implies that those in low risk groups no longer show solidarity with those in high risk groups.

[29] See, for instance (Beauchamp and Childress, 2001); (Feinberg, 1984).
[30] See also (Solove, 2004).

4 Vulnerabilities of the present legal framework regarding BBP

4.1 Introduction

The description of BBP and of the BBP cases and scenarios above, as well as the vulnerabilities generated by group profiling, demonstrate that the use of BBP as a new technology may create numerous undesired effects against which individuals and society would like to be protected. Besides considerations from a moral point of view and concerns from an ethical perspective,[31] legal rules should also be reviewed as to whether they offer the possibility to regulate BBP. In this chapter, we will look into specific existing legislation that is relevant for BBP, in particular regarding the fundamental right to respect for private life and data protection regulations. We review if and under which conditions the existing legislation mentioned is able to cope with the challenges of BBP.

4.2 Respect for private life

From the chapters above, it should be clear that BBP involves a new kind of invasion of the private life of an individual. The **"InLIFE"** scenario illustrates best how reliance on new BBP technology, which re-recognizes behavioural acts of an individual based on behavioural profiles and acts upon them (this facial expression or behaviour matches the behaviour of a sick or a depressed person, hence a trusted person shall be called, etc), may intrude private life as the technology may provoke effects which are not intended or desired.

The right to respect for one's private (and family) life is recognized as a fundamental right and is as such laid down in international treaties, such as in Article 8 of the European Convention for the protection of Human Rights and Fundamental Freedoms of 1950 ('ECHR') and in the constitutions of EU member states. The right is also mentioned expressly in the Charter of Fundamental Rights of the European Union of 2007.[32] The question arises under which conditions individuals could claim that the use of BBP by a third person invades their private life as protected by this fundamental human right. We think this question must even be raised for the case that an individual has provided his or her consent.

The right to respect for one's private life is stated in general wordings and in principle offers only protection against interference by the State ('vertical effect'). However, it is more and more accepted that fundamental rights can also be invoked in relations between private entities or persons ('horizontal effect'). Examples of such a 'horizontal relation' could be the relation between an elderly person and the service flat institution where he/she retires or the

[31] The difference between moral and ethical considerations has been made in numerous ways. Here it is meant to refer to morality as the individual, subjective consciousness of right and wrong behaviour, whereas ethical considerations are taken to refer to a more objective or general understanding of right and wrong.

[32] Article 7, Charter of Fundamental Rights of the European Union, *O.J.* C 303/1 of 14 December 2007. The meaning and the scope of this right are the same as those of the corresponding article of the ECHR and the limitations which may legitimately be imposed are the same as those allowed by Article 8 ECHR.

relation employee-truck driver and the employer who installed the Driver Fatigue Detection of the first scenario. Furthermore, case law points to a positive obligation of States to protect private life, for example, by enacting specific legislation for the protection of private life.[33]

Because of the general wording, this fundamental right may at first sight seem to be inadequate for protection against the use of new technologies such as BBP. Article 8 ECHR does not refer to BBP nor does it provide indications as to whether it applies to BBP and, if so, how it should be applied. Fundamental rights, however, do not need to refer to specific technologies in order to be effective with regard to these technologies. The meaning of the fundamental right to privacy is explained in numerous cases before the European Court of Justice, the European Court of Human Rights and national courts and is hereby applied to specific cases involving new technologies. New technologies and the effects that such technologies may have on the private live of individuals are hereby analyzed in the case law. In the United Kingdom, for example, the national courts reviewed in 2004 whether Article 8 ECHR applies to the conservation of DNA and biometric data.[34] The general right to privacy is hence applied to new technologies. The European Court of Human Rights has repeatedly stated that '*increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data'*.[35] BBP is such a new communication technology that requires attention from the perspective of fundamental rights and freedoms. The same Court said that '*the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective'*.[36] We may therefore expect that BBP applications will be reviewed in the (near) future in relation to the fundamental right of respect to privacy, meaning that at some point case law will appear on the issues that BBP raises. To the extent that BBP technology intervenes in the daily lives of individuals, without notice, shaping their behaviour, one could argue that this constitutes a breach of the right to private life. The notion of private life is a broad term, not susceptible to an exhaustive definition, but does extend to aspects relating to personal identity and to a right to personal development, also in interaction with other persons. Because of the vulnerabilities of the usage of BBP as described in chapter above, the application of BBP would constitute in our view a breach of this right.

The disadvantage is that this fundamental right, as it is worded in general terms, does not provide upfront in clear terms under which conditions BBP should be further developed or deployed. To find out how the right to respect for private life affects the design and use of BBP, we will have to analyse and apply criteria which have been developed in earlier case law on this fundamental right. If the outcome thereof is considered too unclear or uncertain,

---

[33] See e.g. the decision of the European Court of Human Rights, Storck v. Germany, 16 September 2005, §101, available at www.echr.coe.int: 'Consequently, the Court has expressly found that (…) Article 8 of the Convention (…) require the State not only to refrain from an active infringement by its representatives of the rights in question, but also to take appropriate steps to provide protection against an interference with those rights either by State agents or by private parties' ; see also: European Court of Human Rights, K.U. v. Finland, 2 December 2008, available at www.echr.coe.int.

[34] See House of Lords, Regina v. Chief Constable of South Yorkshire Police, [2004],1 W.L.R. 2196. For the majority, the retention of DNA to identify a person, even without the possibility of obtaining other information on that person, is in breach of Article 8, sect.1. See also footnote 42.

[35] European Court of Human Rights, decision Von Hannover v. Germany, 24 June 2004, §70, available at www.echr.coe.int.

[36] *Ibid.*, §70 & §71.

specific legislation should determine the criteria for BBP applications. However, as long as such specific legislation for BBP is not in place, the fundamental right to privacy remains valuable, notwithstanding the technology that is behind the behavioural biometric profiling.[37]

The right to respect for private life, as articulated in paragraph 1 of Article 8 of the ECHR, is not absolute and exceptions are possible for specific purposes, as articulated in paragraph 2. These exceptions must be in accordance with the law; they must have an aim that is legitimate and they must be 'necessary in a democratic society'.[38] The use of BBP for public safety, such as its use in soccer stadia[39] or even its use in the Driver Fatigue Detection scenario for the protecting of the rights of others, may at first sight qualify for such an exception. However, in as far as such usage is a violation of one's private life, legislation will be required to authorize the interference and in addition we need to test whether such usage is 'necessary in a democratic society'. According to the European Court's established case law, the notion of 'necessity' implies that the interference (i) corresponds to a pressing social need and (ii) is 'proportionate' to the legitimate aim pursued.[40] National authorities have a margin of appreciation in their judgement of the above criteria. This margin of appreciation, however, will depend on the subject. The margin is for example narrow as regards interferences in the intimate area of an individual's sexual life, but may be wider if it concerns acts of individuals in public spaces.

Various countries have enacted specific legislation which regulates the use of cameras in public places (such as streets) and other places accessible to the public (e.g., shops). Mostly, such legislation does not refer to the use of technologies that automatically recognize people or profile people on the basis of their behaviour. While this legislation may provide a sufficient legal basis for the installation and use of cameras, it may not provide a legal basis for the use of a technology, such as BBP, that interferes in a different way with the private life of individuals.

---

[37] Compare also (Lips et al., 2004: sect. 7.3): 'However crucial technology, thus, is for the emergence and development of online personalisation, we feel that the essence of online personalisation goes beyond the mere deployment of a certain technology or combination of technologies.'.

[38] See Article 8 sect. 2 ECHR, which is worded as follows : '§2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

[39] See for an example, the 'Happy Crowd Concept' for the new soccer stadium of ADO in Den Haag, presented by Koos van Woerden at the midwinter meeting of the 'Werkgemeenschap voor Informatie- en Communicatietechnology' in Eindhoven, 31 January 2008. See also http://www.sas.el.utwente.nl/wic2008mwm/PresentatieVanWoerden.pdf, downloaded on 27th June 2008.

[40] In the case mentioned in footnote 30 above, the House of Lords found that the retention of fingerprints and DNA after acquittal or discontinuation of the prosecution and the law on that aspect was not disproportionate because the fingerprints and DNA samples retained were to be used for the purposes of prevention and detection of crime and the prosecution of offences. So, though they considered the retention a breach of art. 8 sect. 1, they found it to be lawful and within the constraints stipulated by article 8, sect. 2.

4.3 Data protection regulation

BBP may not only involve a new kind of invasion of the private life of an individual but also entail an increased processing of personal information and personal data. As set out above, BBP requires not only an enrolment phase, but also the capturing of new samples of biometric behaviour of individuals and the processing of these data for specific decisions.

In case an individual decides to use and apply BBP for exclusively private or household purposes, and that individual retains full control over the application, the data protection regulation, in particular the Directive 95/46/EC (the 'Directive') will in principle not be applicable to the processing of the biometric and other data.[41]

In all other cases, the Directive will apply if the processing takes places as part of the activities of an establishment of the one responsible for the processing (i.e. the data controller, e.g., the employer, the service flat institution, etc) in the European Union. However, in the fields of national security, public safety and the prosecution of criminal offences, the processing of personal data is not regulated by the Directive.[42]

The data protection regulation aims in principle at ensuring the free flow of personal data, while some principles and obligations apply. Below we will address some issues under the Directive for BBP.

4.3.1 Transparency of BBP systems through information obligations and access rights?

As explained in Chapter 13 of Profiling the European Citizen (Schreurs, et al., 2008), the Directive establishes a set of obligations for data controllers and a set of rights for data subjects.

As to the obligations for the data controller, the Directive requires that personal data are processed 'fairly and lawfully' for 'specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'. (Art. 6.1.a & b). The above means that the personal data must be processed for well defined purposes. One could plead for integration of data minimisation and purpose specification into the data analysis systems as a condition a priori for integrating information.[43] This would be a fine example of Ambient Law (Hildebrandt and Koops, 2007). The Article 29 Data Protection Working Party has stated in the context of improved data analysis, that improved data analysis does not mean unrestricted data matching and navigation among different databases.[44] It also means that the

[41] Article 3, 2 §2 of the Directive 95/46/EC.
[42] See also the discussion relating to the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (the so-called third pillar), in sect. 5.2 of FIDIS deliverable 6.7c edited by (Geradts and Sommers, 2008).
[43] See and compare with the Opinion 1/2007 of the Article 29 Data Protection Working Party on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities (WP 129) of 9 January 2007.
[44] Ibid, p. 6. The Working Party also recalls therein its Opinion 3/99 on Public sector information where it stated in the context of data- and text mining tools that '[t]he computerisation of data and the possibility of carrying out full-text searches creates an unlimited number of ways of querying and sorting information, with Internet

data shall be processed in a *transparent way* in order to be fair. A data subject should not be identified through a BBP system without his knowledge as to when and how his behavioural biometric characteristics are used in the system.
BBP systems, however, are very complex and do not offer much transparency. One could increase transparency by pleading for an extended obligation for the controller requiring that at the time of collection of the behavioural biometric characteristics, the data subject receives comprehensive and more detailed *information* about the BBP system than is presently required. As of now, the Directive imposes a rather general information obligation upon the controllers towards the data subject, and this concerns providing information *before* the start of the processing (Article 10 & Article 11). The data subject shall be informed inter alia about the identity of the controller and the purpose(s) of the processing. Only if data are obtained indirectly, some additional information has to be provided, including about the categories of the data that are processed. This information obligation, however, may not be sufficient for BBP systems. Recital 38 of the Directive clarifies, inter alia, that where 'the processing of data is to be fair,[45] the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection'. So, in the case of BBP, a more extended provision of information in order to increase transparency, would be in line with the Directive.[46] However, a more extended information obligation may not be feasible in an ambient intelligent environment. In that case, the BBP deployment could for example be explained through friendly user interfaces messages or TETS clarifying what is happening with the behavioural biometric data in what form and for what function during the process of the use, and this not only before but also at the start of the processing. Another solution could be to require the active cooperation (and hence the knowledge) of the data subject for BBP processing (e.g., by requesting a secret upon presenting the biometric sample). See chapter 5 below.

As mentioned, in addition to the information obligations for the data controller, the Directive provides a set of rights for the data subject. It requires that a data subject *has access* to the data processed about him and *can rectify, erase or block* the processing of data which are incomplete or inaccurate (Article 12). There should in principle be no additional costs involved for the data subject to exercise its right to rectify, erase or block. The Directive requires in addition to the right of access that data subjects have access to additional information 'without constraint and at reasonable intervals', in particular (i) confirmation as to whether or not data relating to him are being processed, the purpose of the processing, the

---

dissemination increasing the risk of collection for improper purposes. Furthermore, computerisation has made it much easier to combine publicly available data from different sources, so that a profile of the situation or behaviour of individuals can be obtained. In addition, particular attention should be paid to the fact that making personal data available to the public serves to fuel the new techniques of data warehousing and data mining. Using these techniques, data can be collected without any advance specification of the purposes, and it is only at the stage of actual usage that the various purposes are defined. So all of the technological possibilities with regard to data usage need to be considered'.

[45] Note that this recital 38 does not refer to 'personal data', but only to 'data'.

[46] See also the Article 29 Data Protection Working Party, Opinion on More Harmonized Information Provisions, WP 100, 25 November 2005. In this opinion, it is explained that it would be acceptable for the Group that the information is provided in a multi-layered way. About the importance of information and the right of access to group profiles in general, see also (De Hert et al., 2007: 156).

categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, (ii) communication to him in an intelligible form of the data undergoing processing and of any available information as to the source of the data, and (iii) knowledge of the *logic involved* in any automatic processing of data concerning him at least in the case of the automated decisions (Article 12). This last section refers to article 15 of the directive, which states the principle that persons shall not be subject to decisions which produce legal effects or affects persons significantly and which are based *solely* on automated processing of data intended to evaluate certain personal aspects, such as performance at work, creditworthiness, reliability, conduct etc. Note that article 15 does not refer to 'data subjects' but to 'persons', which means that the applicability of article 15 has a wider scope than the application to data subjects only. Exceptions however are possible, such as in the course of entering into or performance of a contract or if authorized by law and sufficient safeguards are provided in that law (Article 15, paragraph 2). The obligation of giving access to additional information and the logic involved, requires, in the case of a BBP system, that if the data subject excerces the right of access, appropriate information about the functioning of the BBP system must be given. This could in our view also include an obligation to give information about the profiles that are developed and applied or re-applied to persons.

This information obligation, however, does not mean that the controller needs to disclose all details of the algoritms or other mechanisms. Recital 41 of the Directive explicitly clarifies that the right to know the logic involved in the automated proecssing of data should not adversely affect trade secrets or intellectual property, e.g. in particular the copyright protection, the software or the database. However, even without disclosing all technical details, we think that the controller should be able to explain how a profile is generated and (re-)applied. The same recital 41 concludes that the aforementioned possible conflict with IP rights does not mean that the data subject shall not receive all information he is entitled to, raising the issue of whether the directive thinks we can 'eat our cake and have it too'. The information about the logic of processing is only to be given when individuals request information. This implies that while such additional information can be obtained, this is only possible *post factum*, once information has been processed. This raises two additional questions: to what extent will the individual be aware that his or her behavioural biometric data (BBD) have been processed and (how) will she have access to group profiles built on behavioural biometric of other people that match her data and may be applied to her?

The present information and access obligations under the Directive require that controllers provide information to the data subjects. The information obligation before the start of the processing, hereby complying with the legal obligations, is rather limited and not sufficient to give transparency in the BBP system. One can add, that an individual may easily tire of being constantly confronted with information about the fact that her BBD are being processed. The access rights of the data subjects complete the information obligation by the controllers, therefore increasing transparency, but only once the processing has started. Furthermore, one can question whether individuals will exercise this right by requesting access to the logic of data processing. In addition, and as we shall see in the next chapter, the information provided by the data controller may be very complex and technical, thus defeating the practical effectiveness of such access rights.

4.3.2 Consent

The data protection regulation attaches very much importance to the concept of consent for the regulation of the processing of personal data. Consent is one of the six legal grounds spelled out in the Directive, on which the processing of personal data can be based, ànd it also qualifies as a basis for the processing of so called 'sensitive data', including data relating to health. Consent, however, is also strictly defined in the Directive. Article 2 defines consent as 'any freely given specific and informed' consent. Article 7 states that data may only be processed if consent is given 'unambiguously' and article 8 states that sensitive data may only be processed with the explicit consent of the data subject. At various occasions, the notion of consent has been further explained by Data Protection Authorities, including the Article 29 Data Protection Working Party. The latter has repeatedly stressed that consent constitutes a positive act, excluding *de facto* any system whereby the data subject would have the right to oppose the processing only after it has taken place.[47] Specific consent must therefore be acquired before the processing takes place. In an ambient environment in which BBP would be used, this requirement poses a specific problem, for example in the case consent would only be asked after behavioural biometric characteristics would have been processed for matching a specific profile or because various controllers would be involved in the ambient environment. One could wonder after all whether consent would in such environment be a sufficient legal basis for the BBP processing because of the proportionality issue.

4.4 Do the right to privacy and the protection of personal data protect against the disadvantages of group profiling on the basis of BBP?

In chapter 3 we have analysed some of the moral implications of group profiling, made possible by BBP. These moral implications concern the autonomy, privacy and individuality of citizens whose data match with BBPs, exposing them to a loss of control over the consequences of their actions (autonomy), a confrontation with potentially disrupting

[47] This is implied in the emphasis on prior consent as the only legitimate ground for processing data for which no other legal ground is available. See for instance Art. 29 WP 37 (Working Document on Privacy on the Internet - An integrated EU Approach to On-line Data Protection- November 2000) and WP 148 (Opinion on data protection issues related to search engines, April 2008).

information about themselves that they were not aware of (privacy) and exposing them to being treated as members of a category instead of respecting their singularity (individuality). Moreover, group profiling on the basis of BBPs enables stigmatisation and discrimination.

The right to a private life, often understood as the right to be left alone, is not only a *moral* right but – as discussed above – an important and fundamental *legal* right that can be invoked in a court of law. It is not clear whether this means that one can invoke the right not to be assessed on the basis of information that one is not aware of. For such informational privacy, one could seek protection in Directive 95/46/EC. As indicated above, article 15 of the data protection directive formulates a right not to be subject to an automated decision that has legal consequence or has serious other consequences for a person. Article 12 of the same directive stipulates a right of access to the logic of processing in the case of such decisions. However, if a decision is made by an insurance agent, a doctor, an employer or whoever else, *based on BBP*, these articles seem not to apply (because the decision is not automated). In the case of smart applications that presume real time automated decision-making, it could be that the usage of such applications or the entry into an AmI environment will be made lawful by means of a requirement to sign for an explicit and unambiguous consent, thus legitimising BBP. As has been discussed in (Hildebrandt and Meints, 2006) and (Hildebrandt and Koops, 2007) the paradigm of a smart proactive infrastructure that thrives on real time profiling seems in contradiction with the paradigm of informational self-determination, especially when understood as data minimisation. Real time profiling in a proactive environment does not 'fit' with being informed at the moment of collection of all the purposes for which the data will be used. One would easily tire of all such information, preferring a once-for-all consent to use and sell data to enable the type of targeted services provided in an AmI environment. As Schwartz (2000) has argued, we are faced with a market failure: the fact that most users are not aware of the consequences of leaking their data, turns the exchange of data and services into a trade-off based on ignorance. It seems that neither the right to a private life, nor the protection of personal data confront the specific problems raised by BBP, in the context of group profiling.

In the context of information technologies, the right to privacy is translated as the right to informational self-determination, relating to the autonomy of a person with regard to her personal data. Does a right to informational self-determination protect against selection (and exclusion) on the basis of BBP? If the user of a smart infrastructure has to sign away her rights in order to enjoy the advantages of AmI, what protection is left? Must we trade our privacy and autonomy against the conveniences of smart cars, BBP identification and healthcare provided in the 'privacy' of the home? These issues relate to the fact that group profiling treats people as members of a group instead of as unique individuals,[48] thus attributing characteristics of an average group member to all group members. The rights to private life and data protection do not protect against applying a group profile constructed out of other peoples' (or anonymised) data to a person whose data match this profile, unless we can prove that the profile does not apply to us (incorrect application) or prove that applying the profile leads to unjustified (unlawful) discrimination (unfair application). The crucial issue

[48] In 'normal' life, this is called stereotyping. Social interaction requires a measure of stereotyping to make sense of the 'other'. As long as people can easily figure out how others stereotype them, they can anticipate such 'profiling' and act on it. The problem with machine profiling such as BBP, is its invisibility. See chapter 2 in (Hildebrandt and Gutwirth, 2008).

is that if one is not aware of the knowledge inferred from one's keystroke behaviour there is no way we can object against it being incorrect or its application being unfair. On top of that, even if the profile is correct and discrimination would be lawful, BBP could affect stigmatisation and social sorting on an unprecedented scale (Gandy 2006; Lyon 2002). This could affect the core tenets of constitutional democracy.

It may be hard to imagine how such negative effects of widespread usage of BBPs could be mitigated or countered, unless we opt for a rejection of BBPs altogether. This would, however, deprive us of the advantages of this new technology, described in chapter 3 and apparent from the scenarios of chapter 2. If we are willing to conditionally accept some of the drawbacks of these technologies, the biggest challenge will be to complement the possibility of silent enrolment and the impossibility to change one's behavioural biometric dynamics 'at will', by providing adequate means to anticipate how one is being profiled. To be effective, such means would have to integrate legal and technological instruments: giving citizens a legal right to reduce knowledge asymmetry that incorporates the technical means to exercise the right. In terms of law and economics, this would be a first step in preventing a market failure regarding the exchange of data. Having a good guess as to how one is being categorised on the basis of one's biometric dynamics, including a first impression of the consequences of such categorisation, will allow citizens to opt out of environments that may lead to unfair discrimination and stigmatisation. However, the need to opt out of environment could disadvantage a person anyway, thus achieving the discrimination and stigmatisation one would want to avoid. This indicates that transparency tools will not solve all the issues raised by BBP. However, transparency tools do seem to be a precondition for any other effective remedy, because as long as civil society is not aware of what happens at the level of group profiling, it cannot even begin to institutionalise the safeguards necessary in a democratic society. For this reason, in the next chapter we will make a first attempt at a systematic approach of legal and technological transparency enhancing tools (TETs)

5 The role of TETs in the case of BBP

5.1 Technological TETs

5.1.1 Technological View on TETs and Differentiation from PETs

5.1.1.1 Structuring TET implementations

TETs, in their function of reducing information asymmetries, can be constructed in several ways. We can distinguish them by the concreteness of feedback a TET offers to its users. In the most abstract case, the feedback is limited to a list of stored, processed, and possibly transmitted types of *attributes*. For example, the user would learn that a particular data controller, possibly distributed over multiple devices in 'intelligent' environments, keeps track of her name, address and birth date. However, more concrete feedback from TETs is conceivable as well. This could include the actual *attribute values* dealt with by the data controller. So effectively, the user has the possibility to ask for (and possibly check and rectify) the actually stored values.

The second dimension to distinguish between different TETs is the feedback's level of detail. In the simplest case, the feedback comprises solely *what* personal data is affected. Conversely, the most comprehensive feedback could potentially include a detailed description of all possible consequences arising from the personal data disclosure. Obviously, this dimension has in fact many shades: for instance, the purpose of data processing or, if data is shared with third parties, their identity (or just type of industry) are somewhere in between the mere facts and the full consequences. Table 1 visualises the proposed classification scheme in a two-by-two matrix indicating example feedback of an imaginary gym that processes its customers' behavioural information. For the assignment of individuals to group profiles based on BBP, especially TETs that inform their users about *facts and consequences* for certain *attributes* or *attribute values* are of interest (bottom row).

Table 1: Proposed classification of TET implementations with examples

	Concreteness of feedback	
Level of detail	Attribute	Attribute value(s)
Facts	*"This gym stores your resting pulse rate together with your customer card ID."*	*"The resting pulse rate of your customer card #2001 is 64 bmp and has been last updated on June 1st, 2008."*
Facts and consequences	*"This gym stores your resting pulse rate together with your customer card ID. All rates are shared with the public health insurance system and you will be assigned to a health risk group. Your insurer may offer you a reduction of social security contributions."*	*"Your resting pulse rate of 64 bmp will be transmitted to health insurance company XYZ on June 21st, 2008. Since you have an exceptionally low rate you belong to the group with lowest health risks and you will receive a deduction of 5% of the annual rate in 2009."*

This classification is also useful to discuss technical consequences of new security and privacy problems that go along with the introduction of TETs of a certain type.

5.1.1.2 Privacy and Security Implications

In particular, the concreteness of feedback determines whether additional access control mechanisms have to be in place to prevent confidentiality breaches within the TET. This is so because attribute values themselves can convey sensitive personal information and thus need to be protected from illegitimate access. This is not always easy. Consider an example, where attribute values of a public surveillance camera should be communicated with a TET. In the worst case, the camera has captured several persons of which the data controller (i.e. camera operator) has not a single identifier. So the data controller has to verify the data subject's claim that it is actually recorded based on a manual evaluation of the recorded material. In addition, if the data subject is requested to provide some kind of identifier to the data controller to support its claim for transparency, new privacy problems arise. This is so because the identifier contains personal information itself and would not have been disclosed to the data controller otherwise.[49] Consequently, TETs communicating attribute values are only reasonable and efficient if the data controller already possess a suitable identifier of the data subject. Transparency on video surveillance is probably limited to "low-tech" TETs such as information signs, which belong to the category attribute/facts in Table 1 (top left cell).

Note that appropriately secure identifiers have to be chosen depending on the sensitivity of the attribute values (e.g. sharing the same resting pulse rate with the data subject is probably a too weak identifier to protect the entire training history stored in the gym's databases).

Another potential privacy threat is linked with the level of detail. Consider TETs that feed back attribute values, and these actual values depend on other people's attributes. For example, if the condition "exceptionally low rate" in the above example (cf. Table 1) is defined as the 5% bottom quantile of the distribution (say, this rule is publicly known), then knowledge of one's own attribute values (i.e., being in the group with the lowest health risks) might allow inference (at least in a statistical sense) on all other members' values. Note that this inference risk is rather dim in most situations, and probably more relevant for TETs that provide a high level of detail in their attribute value feedback (bottom right cell of Table 1).

5.1.1.3 Trusted domains for TETs

Comprehensive TETs (bottom right cell of Table 1) combine data processing rules of the data controller with attribute values of data subjects to inform the data subject about possible consequences of actions.[50] The actual calculation can be done in either the trusted domain of the data subject (e.g. client device) or the trusted domain of the data controller (e.g. server). However, as this kind of TET combines information a) from the data subject (attribute value) and b) the data controller (rules), the reliability of the prediction always depends on the

[49] It is conceivable to work around some of these problems by means of anonymous credentials and other privacy-enhancing technologies.

[50] We must note that to have comprehensive TETs one would need to have similarly precise information from the data controller to whom data and/or profiles are sold or provided. In an AmI environment that depends on cross-contextual linking the complexity and the scope of information required would in fact be unlimited.

trustworthiness of both inputs (and the output, if processing is located in the data controller's trusted domain).

To define the architecture of TETs w.r.t. trusted domains, it is useful to distinguish further between

- *'ex ante TETs'* which enable the anticipation of consequences before data is actually disclosed (e.g. in the form of a certain behaviour),

- and '*ex post TETs'*, which merely inform about consequences if data already has been revealed.

In situations where the data subject is not able to measure the relevant attribute values (e.g. biometrical data) itself, ex ante TETs are not applicable. 1 shows architectural options for both ex ante and ex post TETs w.r.t. the assignment of inputs and processing to trusted domains. In the ex ante case, the processing can either be located in the individual's trusted domain, which implies that actual or pretended attribute values have to be transmitted to the data controller and the resulting output has to be made available to the individual. Analogously, for ex post TETs, similar options exist. However, with the difference that the actual attribute values are already in the possession of the data controller and cannot be replaced easily with invented or pretended values.

Note that this schema depicts the simplest possible case with only one single data controller. Obviously, in practice, the functions of the data controller can be distributed among many parties, thereby forming an 'intelligent environment'. The general architectural considerations w.r.t. trusted domains and including the required trust assumptions apply in both cases.

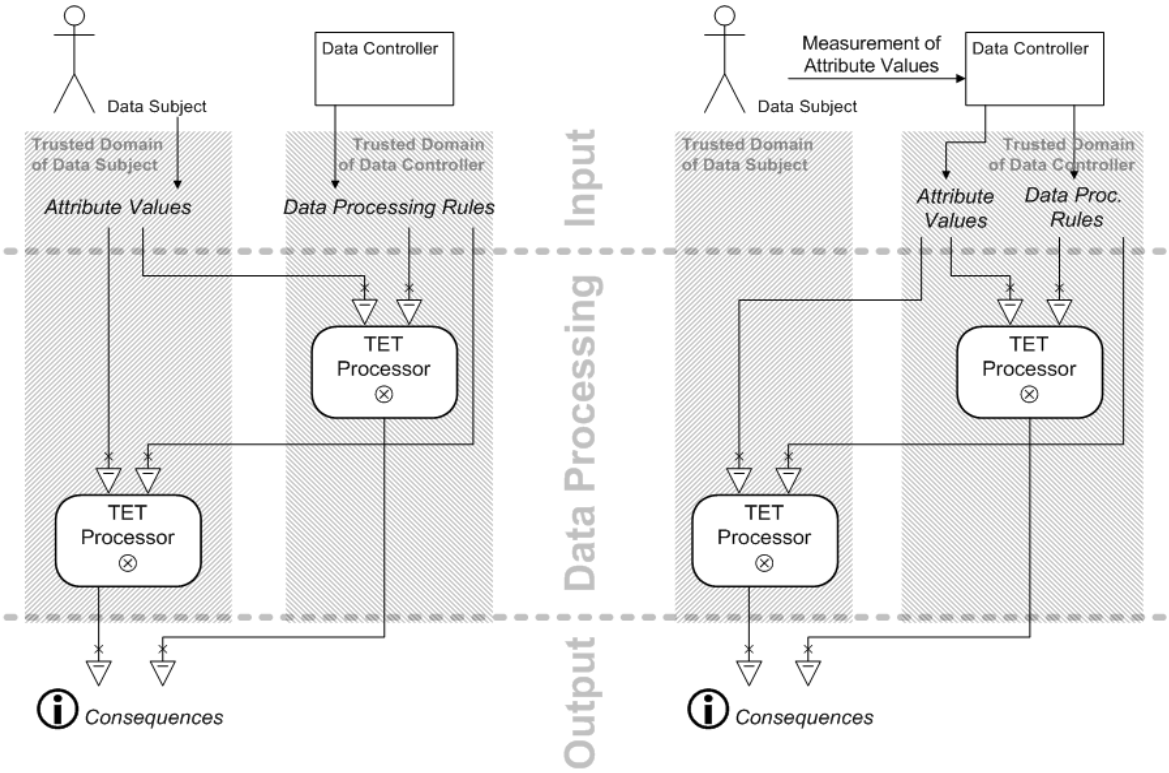


Figure 1: Trusted domains for ex ante TETs (left) and ex post TETs (right)

5.1.1.4 Relation to PETs

TETs and PETs are complementary technologies to reduce information asymmetries between interacting partners. For example, Jiang et al. (2002) name two strategies for realising their "principle of minimum asymmetry" (in an ambient intelligence setup): *Decreasing* the flow of information from data subjects to data controllers and third parties corresponds to our notion of a PET (data minimisation), whereas *increasing* the flow of information from data controllers and third parties back to data subjects corresponds to TETs in our terminology. Since both strategies are so closely connected, they are combined in some practical tools. The close connection between TETs and PETs becomes also evident in Bellotti and Sellen's (1993) framework for privacy protection in AmI environments. We reprint their categories in Table 2, adapted to our terminology.

Table 2: Structured comparison of TETs and PETs

	Type of tool	
Criterion	Feedback about (TET)	Control over (PET)
Capture	When and what information about the data subject gets into the system.	When and when not to give out what information. The data subject can enforce its own preferences for system behaviours with respect to each type of information the data

		subject conveys.[51]
Construction	What happens to information about the data subject once it gets inside the system.	What happens to information about the data subject. The data subject can set automatic default behaviours and permissions.
Accessibility	Which data controllers and third parties have access to information about the data subject and what information they see or use.	Who and what has access to what information about the data subject. The data subject can set automatic default behaviours and permissions
Purposes	What data controllers and third parties want information about the data subject for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for the data subject to have technical control over purposes. With appropriate feedback, however, the data subject can exercise social control to restrict intrusion, unethical, and illegal usage.

Source: Bellotti and Sellen (1993)

The relation between Table 1 and the left column (TETs) of Table 2 is as follows: Category capture broadly corresponds to the lowest level of detail (facts), whereas the other categories of Table 2 gradually increase the level of detail, though they cannot be arranged in an application-independent order: While in some situations, the purpose is more important to assess potential consequences, accessibility may be more telling in others. Table 2 hides the concreteness of feedback dimension (as this is less meaningful for PETs).

5.1.2 Examples of existing technological TETs

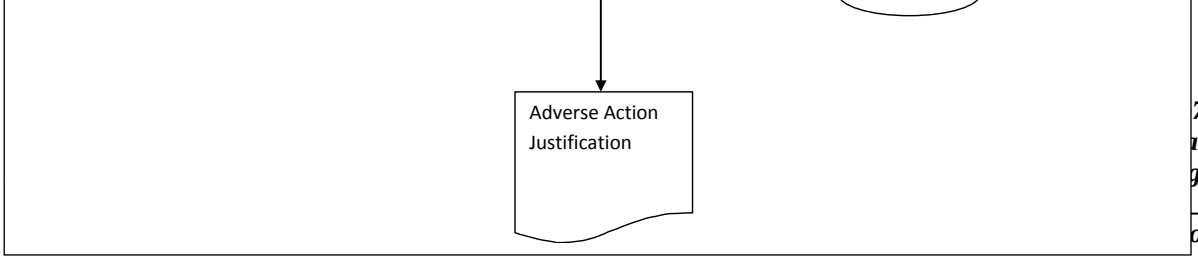
In this section, we present some existing tools that implement TET functionalities. In many cases, the tools also contain features of PETs.

5.1.2.1 The TAMI project

TAMI is a project at MIT/CSAIL laboratory aimed at creating a Transparent Accountable Data Mining (TAMI) system. The idea is to use technology present in (or developed in connection) with the Semantic WEB efforts. In connection with this it is part of a bigger project aimed towards making the WEB policy aware. The current description of TAMI is highly geared towards law enforcement agencies and other governmental agencies using data mining to find evidence or other information about persons.

Weitzner et al. (2006) identify three distinct classes of rule violations that could occur in connection with data mining.

[51] This is especially problematic in the case of BBPs as they build on data one leaks. A person does not really have control over her facial expressions.



1. Adverse actions premised on factual incorrect antecedents.
2. Impermissible sharing of data beyond the collecting organisation.
3. Adverse actions premised on interference from data where the data, while factually correct and properly in the possession of the user, is used for an impermissible purpose

The TAMI system is designed to detect these types of violations and consists of a set of general-purpose interference components (see Fig. 2):

1. The Inference Engine: Used to analyse available data and to asses compliance with relevant rules.
2. The Truth Maintenance System: A persistent store fed by 1 and used to assess the reliability of inferred results and to record justifications and proof antecedents.
3. Proof Generator: Used to construct proofs that adverse actions and critical transactions are justified by facts and permissible under applicable rules.

Using these components it is possible to construct an audit trail that can be used to trace the sources of a decision and also see if the data have been used and handled in a correct manner.

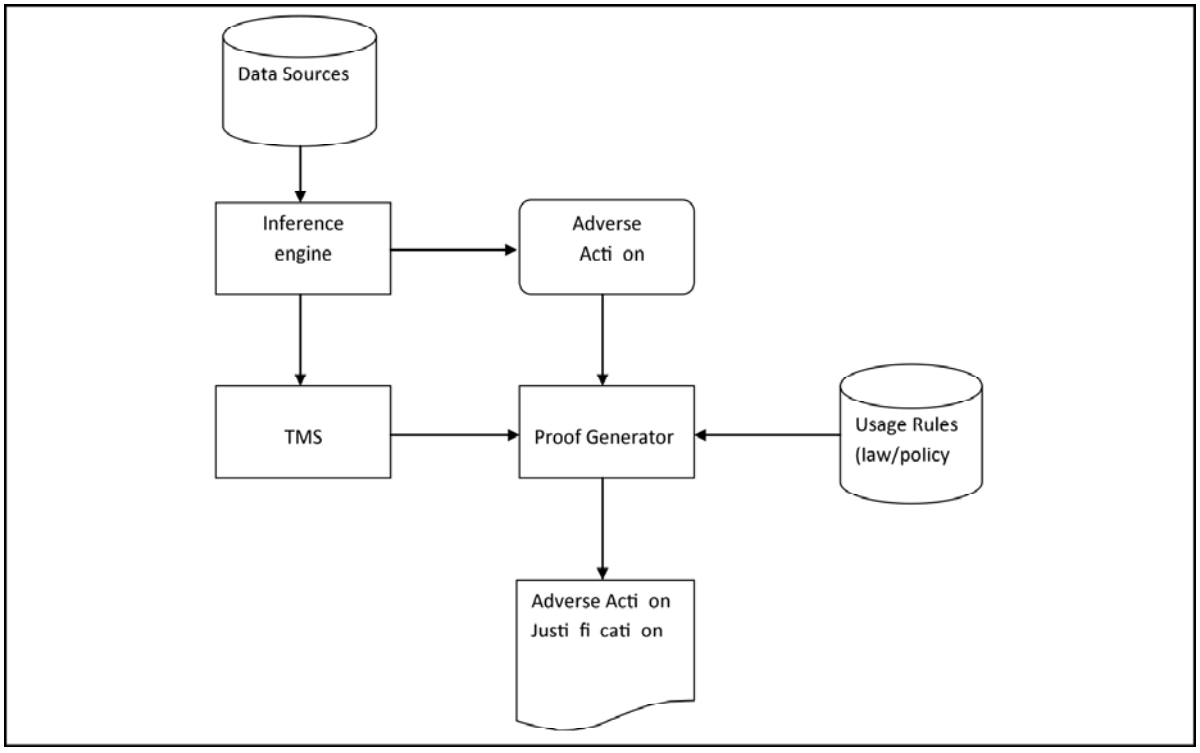


Figure 2: TAMI functional architecture

The TAMI system is still under development and does in the state described by (Weitzner, 2006) use XML and RDF in N3 format for data sources and transaction logs and N3 logic to express rules and policies. As far as we know there is no practical implementation of the

TAMI system. The system, as depictured in Fig. 2, constitutes in our view a system fulfilling the first bullet of the definition of TETs in sect. 1.4 (how am I being profiled) but could probably with alterations and with the right policy and configuration files fulfil the second requirements as well (which behaviours cause which categorisations). Currently TAMI is used to construct after the fact proof of correct handling of data, but by setting up the inference engine to accept arbitrary data sources and for arbitrary inference rules and using it in a predictive manner by feeding in different values and examining the results and the generated proof it could probably be used to give indications on how a given profile will influence the actions taken and the lawfulness of this action.

Set up properly TAMI would thus end up in the lower right quadrant of the classification in Table 1, fulfilling the third bullet in section 1.4 (providing potential consequences of particular attribute values).

As this TAMI system stands today, it constitutes a Type A TET (as described in section 1.4).

5.1.2.2 Privacy Evidence

In a couple of articles (e.g., (Sackman, 2006)), Sackmann et al. discuss an approach based on what they call privacy evidence. The key component in this system is a secure logging facility and an automated privacy audit component to give the user information on how well a system fulfils the promised (or user provided) privacy policy. The general workflow of the system is the following:

1. The data provider delivers his/her privacy policy to the system.
2. The data provider interacts with the system in some way and every action of the system is logged to a secure log file.
3. The data provider can inspect the logs with a specific low view tool that will provide the record that belongs to the respective provider.
4. The log view created by the tool can be sent to an automatic audit facility that compares the log view with the provided privacy policy and construct privacy evidence. These give the user an indication of whether there has been any violation against the policy.

Central to this setup are, besides the policy language, three components: the secure log, the log view and the automated audit facility. The secure log used is a file of encrypted log entries where hash chains are used to make sure that the logs integrity is not tampered with and for key generation to insure forward security. Further some user identification information is used to create the keys for the encrypted entries so that only entries related to a specific data provider are readable by that provider (further details are given in (Sackman, 2006)). The log view is constructed by traversing this file entry by entry and it constructs the view based on the identifier of the data provider. Finally, the automated audit is performed by constructing a violation set (i.e. the set of rules describing violations of the rules described in the policy). This violation set is then compared with the log view and any match in this comparison process constitutes a violation of a policy rule.

As a TET this system fulfils the first bullet of the definition of TETs in sect. 1.4 (how am I being profiled). However, without a data mining component it is hard to see how it could be used to try different policies and to warn users on consequences of policy application. This

system will end up in the right half of the classification table and depending on how the policy is described and the details and type of logging used it will end up either at the bottom or the top half. Most likely, for a typical setting, in the top half.

Since Privacy Evidence tries to infer knowledge about the reliability of the (privacy policy) information provided by the data controller it comes close to a Type B TET, as it performs a kind of counterprofiling. However, as its function is limited to checking the veridity of the privacy policy, it does not qualify as a real Type B TET. If a data mining component were added, counterprofiling on the basis of the audit trails and machine readable responses of the environment this instrument could qualify as a Type B TET.

.

5.1.2.3 P3P

The devices discussed in the next sections (Privacy Bird and to a certain extent also the prototype developed by the PRIME project) elaborate on P3P, which was already discussed in FIDIS deliverables 7.7 (Hildebrandt and Meints, 2006) and 7.9 (Hildebrandt and Koops 2007). The obvious problem of P3P is that one is never sure whether the service provider is actually complying with the privacy policy it declares to be following.

It should be obvious that P3P is a Type A TET, in as far as it provides information about whether data are used for profiling.

5.1.2.4 Privacy Bird

Privacy Bird[52] is a browser plug-in that helps people decide whether the web pages they enter have a privacy policy that is compliant with their own privacy preferences. At the heart of the plug-in is a P3P interpreter and tools for constructing P3P privacy preferences in a user friendly fashion. When installed it will manifest itself as a bird icon in the browser that has different colours depending on how well the web servers P3P policy compares to the users P3P policy. If the policies agree the bird will be green, if they disagree it will be red and if the web server does not have a policy it will be yellow. Different sounds are associated with the different states of the bird and can be used to further enhance the awareness of the user. It is also possible to get more information on the policy of the web server by using menus that turn up when the bird is clicked. This is information on what in the server policy that did not match the user policy, a summary of the server policy in human readable form, contact information to the web page owner and links to the full privacy policy of the web server.

As with many policy tools the question on whether it is a TET or not is highly dependent on the actual policy being described. Privacy Bird will not give you access to data processing or profiles being used. However, if the policy describes the processes and the profiles and gives possible consequences the user could get an idea of what might happen. In our proposed classification Privacy Bird will end up in the Attribute half of the table. The actual quadrant it

[52] Privacy Bird: *http:// www.privacybird.org.*

will end up in is dependent on the information available in the policy currently being evaluated.

As Privacy Bird entirely depends on data provided by the data controller it inclines to a Type A TET, in as far as the policy describes the processes and the profiles and gives possible consequences.

5.1.2.5 The PRIME project

PRIME is a European project that aims at developing tools and concepts for privacy enhanced identity management systems (Fischer-Huebner and Hedbom, 2008). Within the project a proof of concept prototype is developed. This PRIME prototype consists of a PRIME-enabled server side that communicates with the PRIME enabled user side components. For PRIME-enabled web applications, a plug-in has been developed that will give access to the different tools developed by PRIME. Among those tools, three are interesting from a TET perspective: the "Send Personal Data?" Dialog, the concept of PrifPrefs and the DataTrack. Below we will discuss each of these tools. Since the tools are currently prototype tools and still under development we will describe their intended functionality and not the functionality actually implemented at this point.

PrifPrefs

PrifPrefs are privacy preferences stored at the user side describing basically what data or types of data the user is willing to communicate and for what purpose those data may be collected and used. Those privacy preferences can be constructed and customized "on the fly" using the "Send Personal Data?" Dialog (see below) or through an editor and can be tied to a web service (recipient), a pseudonym or a combination of these or they could be generally applicable based on a desired level of privacy. A set of PriPrefs has been predefined which should represent the users' privacy interests and therefore also includes the most privacy-friendly options for acting anonymously or for releasing as little information as needed for a certain service.

The "Send Personal Data?" Dialog

The "Send Personal Data?" Dialog is in essence a policy aware automatic form filler that is issued to obtain informed consent from the user for the disclosure of his/her personal data to a services side. The "Send Personal Data?" Dialog follows the approach of multi-layered privacy notices as suggested by the Art.29 Working Party[53]. When data needs to be sent to the server it will pop up and present the privacy policy of the web server and also help the user decide what privacy implications the data will have. The policy is presented to the user on a purpose by purpose manner acting as an interactive form filler wizard. It will start by asking the user which PrifPref she/he wants to use in this specific case. Based on the PrifPref it will

[53] Article 29 Data Protection Working Party, Opinion on More Harmonised Information Provisions, 11987/04/EN WP 100, November 25 2004, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

then present the information the server wants purpose by purpose indicating if the data asked for and the purpose specified conforms to the stated PrifPref. The user can get more information on why and how the data asked for violates the PrifPref and on possible consequences if the user decides to send the data anyway. The user can also get information on the privacy policy of the server side in a multi-layered style conformant to the Art29 approach. If the actual data to use is stored in the PrifPref it is automatically filled in the form otherwise the user is asked to provide the information. If new information or new purposes are added to the selected PrifPref in this process the user can save this as a new PriPref for later use.

The Data Track

The Data Track is a view handler towards this data base. The purpose of the tool is to let the user keep track of what data he/she has been giving out and to whom. The data is basically presented in two different ways. One view is a table with the different receivers of the data, how many times data has been sent out to this receiver and the dates of the different receiver sessions. By double clicking on a row in the table the receiver can get a more detailed view on exactly what data was sent during this session and the privacy policy that was agreed on when the transfer was performed. The other view is based on a card metaphor where the data are presented as a deck of cards that can be browsed through. The cards basically contain the same information as a table row with the addition of three buttons. These buttons are used for communication with the web server that the cards relate to and they are used to either interactively (if the server has the ability) or in an offline manner request: the deletion of data, correction of data or access to the data that the server currently has stored about the user. The idea here is to make it easy for the user to exercise his/her legal rights towards the data controller. When double clicked, the card view will display the same detailed information as mentioned for the table view above. The Data Track also includes search functionality so the user can find answers more easily to questions such as in what sessions certain information was given or what information a specific receiver has on the user.

5.1.2.6 Summary comment on PRIME tools

The PrifPrefs by themselves are just a tool for constructing privacy preferences and cannot be seen as a transparency tool. However, in connection with the “Send Personal Data?” Dialog and the local Data Track database it could be used to inform the user about what the collected data is used for and whether the services side really requests only the minimal amount of data from the user for the purposes of a requested service. In our categorisation this combination would end up in the lower left quadrant. However, as with all the policy tools, they provide only information on what the data controller promises to do or might do in the case of warnings. However, they do not provide information about what actually happens with the data, i.e. they will thus not give a real insight into the process or the profiles used. Again, this is a Type A TET, in as far as the policy provides information about profiling.

The Data Track helps the user keep track on what data were provided to whom and for what purposes and allows them to access (or request to access) data stored on the server side and compare them with the data stored in their local “Data Track” data base, so that the user can

find out if the server has more or different information than the information that the user has provided to him. It also allows the user to check if the information is correct and to request that the data controller deletes or corrects data that is considered inappropriate or wrong. As of now there is no implemented functionality for checking that the data controller does not cheat here. However, the PRIME architecture discusses solutions containing secure logging, obligation management and different types of encrypted storage solutions in order to minimize the possibility of malicious behaviour. In our categorisation the data track would most likely end up in the upper right quadrant of the classification, since it will tell the user what data actually is stored.

5.1.2.7 The Amazon Book Recommendation Service

Zwick et al. (2004) discuss the Amazon book suggestion service as an example of a service where the customers can directly influence their user profile. As an Amazon customer it is possible to subscribe to a book recommendation service. This service will recommend different books to you based on your previous purchase. By clicking a link in the recommendation the window in figure 3 will appear. This window tells you which previous purchases were used to generate the recommendation. The user can then choose whether he/she wants to remove any of the "input" purchases from his/her profile so that it is not used as a base for recommendations any more.

As a TET this would end up in the lower right quadrant since it indeed gives you information on what particular data caused this consequence. However it will not give any insight into the processes or the profiles used. We believe that the user has very limited capabilities as a customer to influence the result. She/he only know that a specific input generated a specific result not why and how or even how the different input parameters relates to each other when multiple purchases are used to generate a result. Nevertheless it is a good start since it makes part of the profile visible to the user.

Again, this TET depends entirely on information provided by the data controller, thus constituting a Type A TET.

Figure 3: The Amazon Book Recommendation Service

5.1.2.8 Assurance or Trust evaluation tools

As was mentioned in sect. 5.1.1.3 trust plays an important role as long as the user does not have full control over or insight into the data controller's environment or an assurance that the data controller cannot cheat. This state of affairs is quite hard to achieve as long as the data controller have full control and access to all components in his/her system. One way to deter system owners from cheating and to build up or strengthen the trust among the users is to use different types of audits, seals and reputation mechanisms. The role of the Assurance evaluation tool is to harvest the information found about the data controller in lists and other sources generated by the mechanisms mentioned above and present a comprehensive view on the state of the data controller to the user. Based on this the user can then make an informed judgment on whether he/she should trust the data controller or not. Though the information about the data controller is restricted to its general reliability, not disclosing how it may interact with a particular user, these tools seems to come close to a Type B TET, basing itself on a kind of 'counterprofiling. For this reason they might play an important part in judging the accuracy and trustworthiness in the information produced by other TETs. An example of these types of tools are the Assurance Control Function in PRIME that will give the user information on the presences of the data controller in blacklists or disclosure lists and indicate if the controller has been certified by privacy seals of different kinds. Another example is the Web Of Trust[54] (WOT) Firefox plug-in that will warn for sites that are privacy unfriendly based on user judgment.

[54] http://www.mywot.com

5.1.2.9 Other solutions

Of course there exist other transparency solutions than the ones described in the example. However, due to space limitations in this section we have chosen to just briefly mention some of them in this section. On its website the Norwegian government gives its citizens the ability to see what data connected governmental offices have about them through the "minside" web portal[55] and similar portals are under development in more countries within the EU. Regarding keeping track of transactions (i.e. similar responsibilities as part of the PRIME data track) "iJournal" (Brûckner, 2005), a part of Mozilla Privacy Enhancement Technologies (MozPETs) and "iManager" (Jendricke, 2000) for use with PDAs and mobiles should be mentioned. Microsoft CardSpace (Chapell, 2006) also has some transaction tracking capabilities. In as far as they build on machine readable data not provided by the data controller they come close to Type B TETs.

5.1.3 Requirements for technological TETs in the context of BBP

This section lists requirements for the construction of Type A TETs in BBP scenarios. As to Type B TETs further research is necessarily as they build on a very different logic.[56] We started our analysis with the general requirements as proposed by Bellotti and Sellen (1993) for the concrete case of their RAVE system, which includes both aspects of feedback (TET) and control (PET). Our presentation is already adapted to the specific case of TETs for BBP.

- **Trustworthiness**: TETs should be technically stable and reliable to appear trustworthy to the data subject. This means that there are no hidden channels and the TET itself should not expose its users to new privacy risks. In addition, appropriate access control mechanisms have to be in place to ensure the security of personal data.
- **Minimal intrusiveness:** Feedback from TETs should convey a minimal amount of side-information about other subject's personal data. This also includes the absence of possibilities for statistical inference on another person's individual level. In brief, this means the feedback should not create additional privacy problems.
- **Perceptibility:** The presence of TETs should be noticeable by data subjects. Otherwise they may prove to be as useless as typical well-hidden and incomprehensible privacy policies on many contemporary websites. In particular, "low-tech" TETs, such as signs that merely signal the fact that a user's behaviour is monitored, should not be overlooked.
- **Meaningfulness:** TETs should communicate the amount and type of processed personal information to the data subject in a suitable (and possibly configurable) aggregation. This ensures that no relevant information is hidden while avoiding an information overload that exceeds the subject's cognitive capabilities. Too complex (or detailed) information may cease to be helpful for making informed decisions.

[55] http://www.minside.no

[56] Evidently, trustworthiness, minimal intrusiveness, perceptibility, meaningfulness, timing, low effort, standardised interfaces, flexibility and low cost all qualify as requirements for Type B TETs, However, as these types of TETs are hardly discussed in the present report we may expect that the priorities differ and that other requirements need to be included.

- **Appropriate Timing:** TETs should inform the data subjects timely and ideally in advance of a decision on a potential data transmission.
- **Low effort:** TETs should grant access to direct feedback as conveniently and – at the same time – as securely as possible for the data subject. A lack of usability could results in low acceptance and thus impedes the social objectives of TETs.
- **Standardised interfaces:** Access to TETs should be standardised and all TETs should provide for machine-readable interfaces. This allows data subjects to let their own trusted devices manage the communication with TETs. This way, TETs seamlessly interact with user-controlled PETs and therefore complement the framework to reduce information asymmetries.
- **Flexibility:** The definition of personal data may vary depending on the situation. This means that TETs should be flexible enough to be adaptable to changing requirements in a specific environment.
- **Low cost:** Obviously, the cost of installation and maintenance of TETs should be as low as possible to foster acceptance and widespread usage. The distribution of costs between data controllers and data users is another issue to be dealt with separately. This may involve careful regulation, analogously to policy options to support PET adoption (Böhme and Koble, 2007).

5.2 Intermezzo: Privacy Mirrors, or 'playing with the system'

On the cusp of technological and legal transparency tools, it makes sense to discuss the example of Privacy Mirrors (Nguyen and Mynatt, 2002), a framework for designing socio-technical ubiquitous computing systems that should allow users to understand and shape it to fit their privacy needs. As they write 'Privacy Mirrors will allow users to "play" with the system – enacting change and seeing the feedback reflected back to them' (Nguyen and Mynatt, 2002: sect.4.6).

Nguyen and Mynatt build on Bellotti and Sellen (1993) and their notion of feedback and control (see above), on Tom Erickson and Wendy Kellogg's work (2000) on social translucent systems and on Stephen Kaplan and Rachel Kaplan's work (1982) in environmental psychology.

Their objective is to serve the user in understanding and shaping three types of environments: the social, the technical and the physical. This places their framework at the nexus of technical and legal interests, providing a perspective that is broader than a mere technological one while also informing the legal point of view with an insight in the underlying social mechanisms.

The framework they propose incorporates 5 characteristics that should enhance a user's ability to co-create a space of privacy while interacting with and within the environment: history, feedback, awareness, accountability and change. Below we will briefly explain what this means:

History (knowledge of) is the clue to any form of control over future events. Providing information about how the system works and how others interact with the system is preconditional for awareness, accountability and the ability to change. The authors sum up the

type of questions that are relevant in this context, taking into account that to understand information it has to be accessible and not provide for new overloads (turning data into noise instead of information).

> However, because the information resides in a social system as well as a technical system, we want users to understand not only technical state changes but also how people interact with that information (i.e. access and usage, who was involved, where it took place, when it took place, and so on). Much like a hiking trail, social systems do not form instantly, they take weeks, months, sometimes years to gather collective acceptance of rules and norms. Having history information will give people greater insights into the social systems in which they are a part.

Questions for designers raised by the need to record and present history are:

> How to summarize the past so people can more accurately and more easily understand it? What do people want to know? What trends and patterns are people interested in? What specific questions do people want answers to? What needs to be recorded? What doesn't need to be recorded (what needs to be left out)? What is socially unacceptable to record? How does context get recorded alongside the data? Should data deteriorate over time? What needs to be forgotten? Should history be exact, especially when its recall is not framed in the same context? (Nguyen and Mynatt, 2002: sect. 4.1)

Feedback is essential but to prevent overload or the opposite the authors incorporate 3 levels of feedback: a glance, a look interface and an interactive interface.

> Glancing at a Privacy Mirror will give a small amount of information, much in the same sense as when a person walks by an actual mirror and notices in the reflection that something is stuck on his shirt. An example of a glance interface is an ambient display, designed to give information without requiring extra attention or effort from its audience. Stopping and looking at a Privacy Mirror will give more information, because more time is spent scrutinizing the reflection. An example of a look interface is an informational display, designed simply to give information to its audience. Flight arrival and departure screens at airports are typical look interfaces. And interacting with a Privacy Mirror will give the user the most amount of information. The user can ask the system to provide more information, to give greater detail, or to narrow or widen the scope of inspection. An example of an interactive interface is any of the interactive programs that are normally seen on desktop computers.

Questions for designers raised by the need to provide feedback are:

> How to address the senses effectively for feedback? How to provide different levels of information? Where to provide feedback? How to provide feedback to groups as well as individuals? What feedback is important to people? (Nguyen and Mynatt, 2002: sect. 4.2).

Awareness is preconditional for users to understand how their behaviour feeds back into the social and technical environment. With awareness the authors refer to:

> 1. How users participate in the socio-technical system
>
> 2. How others participate with respect to them and their information

3. How everyone can and cannot participate (features and constraints) in the socio-technical system

An example of their framework is a Groupware Calender System (GCS). They illustrate the awareness generated by the application of their framework to the GCS, by highlighting how the framework facilitates social, technical and physical awareness with the users:

> *Social* – They may find out that their calendar information is not used or seen by their supervisors, but rather that their calendar information is more likely used by their subordinates. They may be able to better understand and predict their colleagues' needs because they are more aware of their colleagues' action with respect to them.
>
> *Technical* – They may be able to understand that any new calendar information will not be shared with others until they synchronize their Palm devices.
>
> *Physical* – With awareness, they may realize that opening their window blinds allows in sunlight that overexposes their cameras, affording them a little privacy by controlling how much video information leaves their space.

Questions raised for designers by the are:

> How to convey cognitive models of larger socio-technical systems? What are different awareness needs? Do users want affirmation that someone is looking? Do users want to see social dynamics of particular users? Do users want to see social dynamics of a workgroup? (Nguyen and Mynatt, 2002: sect. 4.3)

Accountability presumes that users know the consequences of their interactions with the environments. Referring to Erickson and Kellog (2000), they advocate the concept of the social translucence of socio-technical systems:

> Accountability provides the "I know that you know," to socially govern people's actions. This information "provides a basis for inferences, planning, and coordination".
>
> When someone accesses a piece of private information, the owner of that information should be able to determine who accessed that information. At the same time, when someone accesses a piece of private information, the person doing the accessing should also know that his actions have been processed in some way. The feedback to both parties creates a you-know-that-I-know-that-you-know condition that, as we have just said, brings already well-defined social and cultural practices into the situation.
>
> As an additional benefit, accountability also plays a role when a vague or not well-formed privacy space is approached. Knowing that you-know-that-I-know-that you-know gives a concrete subject and shared understanding for people to communicate and form social norms for that space. It is also interesting to note that the owner of the information is not necessarily responsible for the usage of that information. Sometimes the responsibility can be delegated to the recipient. For example, people have their parents' phone numbers. However, it is not up to the parents to set when their children can and cannot call. The caller shares some responsibility for that before each call.

Some questions for designers, raised by the need for accountability are:

> How to provide accountability while maintaining social lubricants such as plausible deniability? What kinds of interfaces will hold people more accountable than others, especially in the disembodied digital world? (Ngyen and Myatt, 2002: sect. 4.3)

Change is made possible by providing using with different levels of awareness of what is going on, providing the feedback that is preconditional for control. The framework of Privacy Mirrors aims to show people how others see them, allowing them to (re)construct their identity, which is fundamentally a relational construct and to shape their socio-technical environment. The authors use the example of the GCS to illustrate how their framework should operate:

> For example, if a user knows how his calendar information is being accessed, he can affect the flow of that information by changing the permissions of those accessing the calendar information. Affecting a change through this type of technical means may be an engineering challenge. As another option, the user can elect to produce change through more social means. The user might want to change his coding scheme, such that while the descriptions are still available, they only make sense to him. For example simply "Morgan."

Questions for designers that are raised by the need to facilitate change are:

> How to present the language of change to people? What is the language of technical change? Is it direct manipulation of the feedback provided by the system? Could it be setting privacy preferences by example and letting the system work out the rules of information flow? (Nguyen and Myatt, 2002: sect. 4.4)

In terms of the typology of TETs, provided in section 1.4, the framework of Privacy Mirrors can be seen as an attempt to provide an integration of Type A and B transparency tools. Since the 'mirrors' are integrated into the socio-technical infrastructure the information they provide in a way depend on the data controllers (Type A). However, to the extent that this framework allows users to counter profile the system, by using the system, it seems to incline towards an independent means to predict the outcome of their behaviours in terms of the systems response, as well as the responses of other users (Type B). It seems obvious that the framework faces immensely complex design questions, and we are not aware of any attempt to actually build a prototype that incorporates the history, feedback, awareness, accountability and change with regard to BBPs. Nevertheless, by integrating the social perspective, the framework provides for the beginnings of a socio-technical infrastructure that allows for the technological embodiment of legal protection against invisible visibility (Hildebrandt, 2009).

5.3 Legal TETs

5.3.1 Legal view of transparency tools, difference with opacity tools

The protection of private life seems to be a typical opacity tool (chapter 14 in Hildebrandt and Gutwirth, 2008). It is important to realise that the protection of privacy is especially important in public spaces (Nissembaum, 2004), because CCTV and other monitoring technologies transform the anonymity formerly associated with public spaces into an increased

identifiability. BBP could provide a substantial contribution to this identifiability, especially since BBPs allow re-recognition without actually identifying you in terms of your name or address. On top of that this re-recognition can occur without your awareness (silent enrolment). In order to protect your private life, you must be aware of potential violations. If privacy implies opacity it is important to become aware of the invisible visibility made possible by BBP (Hildebrandt, 2009). To exercise your right to privacy you need legal tools to uncover the extent to which you are being made transparent by profiling technologies. This means that transparency tools are a precondition to exercise the right of privacy: *to know which behaviour you want to hide you need to know how profiling technologies interpret your behaviour and which consequences are attached to these interpretations.*

Data protection legislation provides for a set of transparency tools that are relevant in this context: art. 10 and 11 provide for an obligation for the data controller to supply information to the data subject whose data he is collecting, art. 11 provides for a right for data subjects to obtain information from a data controller. Referring to chapter 4 of this deliverable and the legal analyses made in earlier work of Work Package 7 of (E.g., FIDIS deliverables 7.3 (Schreurs et al., 2005), 7.5 (Hildebrandt and Gutwirth, 2005), 7.7 (Hildebrandt and Meints, 2006) and 7.9 (Hildebrandt and Koops, 2007)), we conclude that the present generation of legal transparency tools affords insufficient protection against the application of group profiles. Below we shall analyse the potential of two new legal transparency tools, both concerning draft legislation of Germany.

5.3.2 Examples of new transparency tools

5.3.2.1 Transparency of the logic behind credit scoring

This section gives an overview of legal provisions passed in Germany in response to the lack of transparency in a commonly used form of profiling: credit scoring. Credit scoring does not utilize behavioural biometric profiling. The characteristics taken into account can be categorized as follows:

Table 3: Categories of characteristics used in credit scoring programmes

Socio-Demographic data	**Information on general financial condition**	**Contract Data**
Address	Assets	Number of transactions
Duration of tenancy	Banking security / real estate	Volume of transactions
Number of relocations	Ownership of residential apartment	Account balance / overdraft
Social background	Household invoice	Number of bank accounts
Sex	Amount of liabilities	Number and amount of credits
Marital status	Monthly income	Number of credit cards
Age	Monthly expenses	Banking security

Number of children	Obligation to pay alimony, car expenses, regularly expenses	Duration of contractual relations
Type of household	Ability to pay rates	Willingness of customer to provide information
Educational background	Types of credits	Reliability of information provided by customer
Educational qualification	Number of credits	
Profession	Number of credit inquiries	
Type of employment	Insolvency	
Duration of employment	Number of inquiries by credit-scoring agencies	
Employer	Number of Access right requests	
Imprisonment and end of imprisonment	General financial knowledge	
Nationality		
Car ownership		
Health status		
Religion		

However, due to the fact that credit scoring is very common and has been practiced for many years we can see a first generation of legal transparency enhancing tools being discussed and passed which regulate this kind of profiling. Type A TETs with regard to credit scoring is impaired by two aspects. Some credit-scoring agencies take the willingness of the customer to provide information into account when calculating the credit score. Refraining from providing requested information may thus result in negative consequences. Furthermore, the knowledge asymmetry between data controller and data subject regarding the fact which characteristics are used for the profiling, which weighting is applied and which potential consequences exist is similar to the knowledge asymmetry regarding behavioural biometric profiling. As explained in sect. 1.1.1.1 above, it is not easy to change our biometric behaviour, just like socio-demographic characteristics like age, sex, educational and social background are impossible or difficult to change.

One widely applied business case of profiling practices is credit scoring. In an attempt to assess the creditworthiness of potential business partners and customers, companies seek for statistically supported means to calculate a "credit score" indicating the probability with which a contractual party will comply with her contractual obligations. In the case of the deliverance of services or the selling of goods the main contractual duty of the other party is in-time and full payment. If goods or services on the one side and payment on the other side

are exchanged simultaneously, the seller does not face the risk of payment failure because he simply can refrain from handing over the good or service if he realizes the contracting party will not facilitate payment at that moment. If the service or good is provided prior to the payment, the seller faces the above described risk of payment failure. In this case of subsequent deliverance of service and payment the entity offering the good or service very often faces a problem hampering the risk assessment: the customer is often not personally known to the company running a shop or a business. Without any personal relation existing prior to closing a contract the company cannot conduct a personalised assessment of the potential customer's creditworthiness based on individual characteristics. To fill this gap an economic sector is aiming at meeting companies' demands and mitigating credit risks that potentially occur when closing contracts with unknown parties. Credit-scoring agencies offer their service to parties engaging in business transactions to rate customers by means of a credit score.

This credit score aims to map the probability of duly payment by the customer and is calculated based on a number of values and socio-demographic information. The algorithms behind this calculation are treated as business secrets and currently any attempt to obtain information on how exactly the score is calculated (which kind of information is taken into account and which weighting is applied) is turned down by credit-scoring agencies. However, the credit score can have an enormous impact for the customer because companies are likely to refrain from engaging in business relationships with a badly rated individual.

The Independent Centre for Privacy Protection Schleswig-Holstein carried out a study commissioned by the German Federal Ministry of Food, Agriculture and Consumer Protection in 2005 (Kamp and Weichert, 2005). The study titled "Scoring systems for an assessment of creditworthiness – chances and risks for consumer" extensively analysed the credit scoring services currently existing in Germany, the applicable legal requirements, compliance of existing services with these requirements and derived from this analysis an overview of existing gaps in legislation. The authors concluded that credit scoring currently lacks sufficient transparency for consumers. Some of the characteristics taken into account for calculating the credit score are highly questionable with regards to their relevance for assessing the payback probability. Individual deviations from group profiles are not sufficiently factored in. This refers to the implications of non-distributive group profiling, described in sect. 3.6 above.[57] In this respect (Kamp and Weichert, 2005) emphasise: "Certain factors especially demographic characteristics have a questionable relevance for estimating the consumers´ reliance. Even though these factors may imply a certain statistical significance, individual discrepancies and the danger of discrimination have to be considered, too. Secondly the use of scoring systems entails a lack of transparency for the consumer. Information about credit-scoring is seldom made an integral part of the credit agreement. Public information about credit-scoring is rarely presented by the companies and certain reluctance is noticeable, when the consumers request information on the stored data." Furthermore, (Kamp and Weichert, 2005) conclude that currently existing transparency regulations provided by the German Data Protection Act are not fully complied with by the credit institutions and the credit-scoring agencies. The consumers have the right to be

[57] Cf. (Hildebrandt and Gutwirth, 2008: sect. 2.3.2).

informed about their calculated scores, the used information and the rating of the information in the process of the credit scoring already under existing German law.

The German government passed a draft amendment law to the Federal Data Protection Act on 30. July 2008.[58] The law still has to be passed by the German parliament and may prior to that be subject to changes. The draft amendment law currently would add a new section to the Federal Data Protection Act. In this newly elaborated provision Article 28b regulates the requirements for credit-scoring. The draft law furthermore amends the already existing provision Article 34 Federal Data Protection Act on notification of the data subject. The new section of Article 34 reads:

In the case of a credit-scoring calculation the data controller shall notify the data subject upon request as to

- all probability scores collected or saved for the first time within a six month period prior to receipt of the notification request,
- the types of data used to calculate the probability score,
- the constitution of the probability score in the specific case in an easy and generally intelligible form.

The scope of the new notification obligation has been very controversial throughout the public discussion regarding the planned regulation of credit scoring. When Kamp and Weichtert carried out their study in 2005 they contacted 500 credit institutions in order to find out about how they calculate the credit score and which characteristics are taken into account. Only 29 responded to the questionnaire. The vast majority of companies was reluctant to reveal more information regarding the exact procedure applied for credit scoring. This reluctance is still common practice towards data subjects referring to their rights granted under Article 34 of the Federal Data Protection Act, "Provision of information to the data subject". Also supervisory authorities seeking to obtain more detailed information regarding the scoring procedure were turned down based on the argument that scoring procedures are trade secrets of the credit-scoring agencies. Protecting this trade secret, so the argument went, constitutes an "overriding legitimate interest" of the data controller that exempts him from the obligation to provide information under the currently effective[59] Article 34. The wording of the current provision is: "[…] If the personal data are stored in the course of business for the purpose of transfer, the data subject may request information on their origin and recipient only if there is no overriding interest in protecting trade secrets. […]"

---

[58] Entwurf eines Gesetzes zur Änderung des Datenschutzgesetzes. Available in German at http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2008/Einzelseiten/Infrormationen__Aenderung__BDSG.html.

[59] An English-German translation of the Federal Data Protection Act is provided by the Federal Data Protection Commissioner at: http://www.bfdi.bund.de/cln_007/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf.

The parliamentary readings have led to first changes in the draft law, cutting down on transparency initially foreseen for the data subject. The scope of the notification obligation regarding the types of data items used has been restricted in comparison to the initial draft. The original draft included an obligation to notify as to "the types of data used to calculate the probability score *listed in descending order mapping the importance for calculating the score in the specific case*." The current draft does not include an explicit obligation to indicate the importance and weighting given to specific characteristics.

However, the reasoning of the draft law given by the government in August 2008[60] further elaborates on the scope of the notification obligation and explicitly refers to the argument of trade or business secrets as an overriding legitimate interest which is voiced by data controllers who seek to avoid having to reveal the exact process of credit scoring. The reasoning first addresses the government's intention for introducing regulation on credit scoring and especially information obligations regarding the types of data used for calculating the credit score: "Due to lacking disclosure of what types of data are used for scoring procedures, data subjects currently can not or can hardly track how his or her specific score value is calculated and how decisions based on this score value are made. In order to enable the data subject to correct incorrect data and to disprove the calculated probability score in his or her specific case, the types of data used shall be revealed to him or her."

This reasoning indicates that the German government's intention was indeed matching the definition of a legal transparency enhancing tool as described in this report (sect. 1.4.1). The intention is to enable data subjects to understand and challenge being assigned to a group profile.

Regarding the legitimate interest to protect trade secrets the reasoning further states: "In addition, obligation 3 constitutes the duty to explain the constitution of the probability score in the specific case in an easy and generally intelligible form. This ensures that on one hand companies don't need to reveal the underlying score algorithm as they have an overriding legitimate interest regarding it's protection, and that on the other hand the facts and circumstances on which the probability calculation is based must be revealed to the data subject upon request in a way lay people can understand. Thus, no complex mathematic formulae need to be revealed, especially as they are not generally understandable. Rather must the data subject be put in a position to understand the underlying facts and circumstances. The result must always be insofar comprehensible to the data subject that he or she can properly exercise his or her rights, reveal possible mistakes in the basis of calculation and explain deviations from the automatically gained typical rating of the underlying facts. The data subject shall be enabled to argue his position with the data controller and in this way achieve an appropriate review of the decision. […]"

The German legislator clearly identifies the colliding interests and seeks to regulate a compromise in the sense of a legal TET. A limit regarding trade secrets as overriding legitimate interests is drawn on code basis, meaning the credit-scoring agency does not have to reveal the exact computational algorithms. But because the computation result and the associated application of group profiles has such an enormous impact on the data subject's

[60] Available at: http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2008/0501-600/548-08,templateId=raw,property=publicationFile.pdf/548-08.pdf.

life, companies processing personal data to calculate a credit score must reveal enough information about their business model to not hamper the data subject in exercising his rights.

When applying the aforementioned legal transparency requirements to behavioural biometric profiling some shortcomings become apparent:

As behavioural biometric profiling can be conducted remotely without the data subject's knowledge and consent (silent enrolment, see sect. 1.2.2), any notification right which is to be carried out only "on request" of the data subject and ex post to the profiling does not help to provide ex ante transparency. If the data subject is to be put in a position of "knowledge symmetry" in order to allow for a deliberate change in behaviour aiming at avoiding certain profiling results, notification of the fact that behavioural biometric profiling is carried out at all and based on which characteristics and weighting must be offered prior to the profiling process.

5.3.2.2 Transparency in the new German draft law regulating requirements for genetic analysis and the use of genetic data

In Germany a discussion has taken place for several years about the issue of genetic analysis and the threat a use of genetic data poses for individuals regarding their right to informational self determination as well as potential discrimination. The advancements in genetic research and the availability of commercial genome analysis initially provided by foreign companies such as deCODE, Complete Genomics and 23andMe pushed the public discussion.

Genetic data is not behavioural biometric data. The processing of genetic data does however raise similar questions with regard to the sensitivity of the data, suitability for (hidden) profiling and discrimination. Just like behavioural biometric data genetic data cannot be altered or controlled.

The German government was called upon to propose legislation regulating requirements for a collection of genetic data as well as the further use of and access to such data by the data subject as well as third parties. While the German Code of Criminal Procedure contains provisions regarding an analysis of genetic (DNA) data by criminal investigative authorities, no such sector specific regulations have existed regarding the relations between citizens and those between citizens and private entities like insurance companies or employers.

German insurance companies joined a self-commitment to refrain from requesting a genetic analysis of potential customers before closing insurance contracts concerning for example health insurance, occupational invalidity or life insurance until 2011.[61] This self-commitment is applicable to contracts concerning an insurance sum of less than 250.000 Euros.

[61] See interview at: http://www.gdv.de/Publikationen/Periodika/Zeitschrift_Positionen/Ausgabe_Nr._38_Oktober_2004/inhaltsseite13253.html.

For all of these types of insurances sickness/illness caused by certain genetic dispositions may lead to the event covered by insurance. Insurance companies announced they respect the insurance holder's right to "not know" of any genetic disposition (in German: *Recht auf Nichtwissen*).[62] However, in order to "preserve the information balance" insurance companies want to treat knowledge about a medical disposition resulting from a (voluntary) genetic test like any other information the insurance holder is obliged to give on risk affecting conditions.[63]

In November 2006 the Draft Law on Genetic Examination of Humans was drafted.[64] The health committee of the German parliament held a public consultation regarding the draft law in November 2007.[65] The German government passed the draft law on 27 August 2008.[66] The law needs to be passed by the German parliament and is likely to be amended by the parliament during the parliamentary readings.

Even though the law will not create a general right to track how genetic data will be used the legislator clearly aimed at regulating the areas (currently seen by the legislator) where a discriminating use of genetic data may be encountered and where plans of using such data have either been announced or are already being carried out (medical examination, insurance companies for risk assessment, work life, paternity tests).

In its current state, the draft law regulates requirements for:

- genetic analysis for medical purposes including requirements for:
  - consent
  - information obligations for the examining doctor
  - notification of data subject with regard to examination results
  - storage and destruction of genetic material and results
  - genetic analysis of individuals who are incapable to consent (e.g. impaired or under aged individuals)
- genetic analysis to examine paternity
- genetic analysis in the area of insurance business
- genetic analysis in the area of work life (prior and after establishing a contract)
- current state of the art concerning scientific and technical requirements for such an analysis. This includes creation of a "commission for predictive genetic diagnostics" which will be affiliated to the Robert-Koch-Institute. This commission with 17 experts from the fields of medicine, biology, ethics, law, patient and consumer representatives will elaborate guidelines on the current state of the art for predictive genetic diagnostics.

An overview on specific provisions is given below:

---

[62] Die Welt, Gendiagnostik – Verlangen Versicherungen bald einen Gentest?, 16.4.2008. Available at: http://www.welt.de/politik/article1908974/Verlangen_Versicherungen_bald_einen_Gentest.html.
[63] Frankfurter Allgemeine Zeitung, Versicherungen wollen keinen Gentest verlangen. 17.4.2008. Available at: http://www.faz.net/s/Rub0E9EEF84AC1E4A389A8DC6C23161FE44/Doc~E9EF071ECBCC24F5AB45F004BBD42168B~ATpl~Ecommon~Scontent.html.
[64] Entwurf eines Gesetzes über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz – GenDG). Available in German at: http://dip21.bundestag.de/dip21/btd/16/032/1603233.pdf.
[65] See http://www.bundestag.de/aktuell/archiv/2007/gendiagnostik_kw45/index.html.
[66] See http://www.bundesregierung.de/nn_1524/Content/DE/Artikel/2008/04/2008-04-16-gendiagnostik.html.

Article 4 regulates a "prohibition of discrimination". The provision reads: “No one shall be discriminated against based upon his or her genetic properties nor based upon the genetic properties of a related person. No one shall be discriminated against based upon his or her decision (or the decision of a person related to him or her) to take or not take a genetic analysis or because of the results of such an analysis."

Article 9 regulates an obligation to consult a medical doctor: “A diagnostic genetic examination may only be conducted by medical doctors. A predictive genetic examination may only be conducted by a medical specialist for human genetics.”

Article 10 regulates the requirements for a valid consent: “A genetic examination for medical purposes may only be conducted and a sample necessary for this examination may only be taken if the concerned person has

- decided whether and in what scope a genetic examination for medical purposes shall be conducted, whether and how the results of this examination should be brought to the concerned person’s knowledge or should be destroyed, whether an unexpected result of the examination should be brought to the concerned person’s knowledge or should be destroyed
- given his or her consent to the examination and the necessary sampling in writing.[…]

Consent can be withdrawn at any time with future effect.”

Article 11 “Information obligation”: “Prior to giving consent the responsible medical person must inform the concerned person of the nature, consequences and scope of the genetic examination. The concerned person must be given an adequate period of time for reflection until the examination.

The information to be given comprises in particular:

1. purpose, kind, scope and significance of the genetic examination including the results possible to gain with the equipment to be used for the genetic examination […],

2. possible health related risks associated with the genetic examination and the necessary sampling,

3. a reference that test results may give knowledge about relatives and an indication of possible physical and psychological stress caused by the examination results,

4. the planned use of a genetic sample and the examination results,

5. the right to withdraw at any time the consent given,

6. the right of the concerned person not to know including the right not to take notice of examination results or of part of the examination results, but to have them destroyed.”

Article 22 concerns use of genetic examinations by insurance companies: “The assurer must neither ask the insurance holder prior or after closing the insurance contract to conduct a genetic examination or analysis nor to request the revealing of results of prior predictive genetic examinations or analyses nor may the assurer receive or use such results.”

The draft law has been criticized because it currently fails to regulate the use of genetic data for research purposes. The Federal Privacy Commissioner stated that he will suggest an

amendment of the draft law with regard to such provisions.[67]

In the context of TETs this regulation can serve as an example of a first attempt to directly address information asymmetries resulting from an intransparent processing of sensitive data.

Not only does the law lay down specific requirements for who may generate this data (only medical doctors). It does also lay down requirements for an informed consent that exceed the requirements for an informed consent as elaborated in Working Paper 114 by the Article 29 Working Party.[68] For specific business sectors and models of risk assessment based on genetic data the law even regulates a general prohibition of the use of this kind of sensitive data for profiling.

5.3.3 Recommendations for new legal TETs, with regard to group profiling, personalized profiling and BBP

The proposed German legislation regarding the usage of human genetics initiates some specific rights that seem highly relevant in the context of BBPs. Since this legislation concerns the genetic diagnostics of a particular person, they regard personalized profiling (the application of group profiles to a particular person, specifying health risks runs by this particular person, based on epidemiological medical research).

Firstly, a general prohibition of discrimination on the basis of genetic diagnostics is introduced. In the case of BBP we suggest extending this prohibition to the usage of BBPs that generate sensitive *knowledge* about a person such as about her mental and physical health, ethnicity, personal character and other types of knowledge that allow for unjustified discrimination.

Interestingly, in the case of the proposed German legislation, this prohibition is coupled with a right to request the destruction of such knowledge and with a strict prohibition of insurance companies to demand, access or use any such knowledge. Again, we suggest to extend the right to request destruction of sensitive knowledge to the knowledge produced by BBPs, and similarly to extend the prohibition for insurance companies to sensitive knowledge generated by BBPs.

To turn these rights and obligations into effective remedies they need to be complemented with transparency rights, which provide individual citizens with the means to require destruction of specific knowledge with regard to their personalized BBP and with the means to contest decisions taken on the basis of sensitive knowledge derived from BBPs.

---

[67] See press release on 28/08/2008: Schaar begrüßt Kabinettsbeschluss zum Gendiagnostikgesetz. Available at: http://www.bfdi.bund.de/cln_027/nn_531002/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM-25-08-SchaarBegruesstKabinettbeschlussGendiagnostikgesetz.html.

[68] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 25.11.2005. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

In section 5.2.1 we concluded that the present generation of data protection rights provides insufficient legal TETs with regard to group profiling. This insufficiency is triggered by (1) the absence of a clear and unambiguous right of access to group profiles that may be applied to you and (2) the absence of the technological infrastructure to exercise such a right. In section 5.3 we will return to the second point, in this section we will elaborate on the first point.

Art. 12 of Directive 95/46/EC states that a data subject has a right to obtain from the controller: knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in art. 15 (1).

Art. 15 of the same Directive states that every person has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Recital 42 of the Preamble of the same Directive states that whereas every data subject must have the right to know the logic involved in the automatic processing of data concerning him (…), whereas this right must not adversely affect trade secrets or intellectual property and in particular the copy right protecting the software, whereas these considerations must not, however, result in the data subject being refused all information.

Obviously the rights and obligations described in these articles and recital do not provide for an unambiguous right of access to group profiles that match one's data. Firstly, the right is given to a data subject and it is unclear whether a person whose data match with a group profile that was constructed out of other people's data has a right of access to the profile. Second, the right is restricted to a situation in which automated decisions are taken, ruling out all situations in which routine human intervention is at stake. Third, the rights of the data controllers or those who developed the relevant software seem to trump a data subject's rights of access.

A more straightforward right of access to group profiles that match with your data should build on the articulation in the proposed German legislation regarding credit scoring:

In the case of a BBP that concerns a particular individual, based on behavioural biometric group profiling, a data controller should provide that person with access to:

1. the types of data used to construct the group profile, and their relative impact on the constitution of the profile;
2. the constitution of the group profile in the specific case in an easy and generally intelligible form.

The advantage of requiring this type of information from a data controller is that – at least on paper – a person can demand to be informed about which of her behaviours generate what types of sensitive knowledge.

6 Conclusions: Ambient Law, the Legal articulation of transparency rights into the BBP technological infrastructure?

AmLaw tries to cope with the fact that written legal rules may no longer constitute an effective remedy in the case of autonomic computing or AmI, due to the fact that the complexity of the technical infrastructure is hidden and inaccessible for ordinary citizens.

Combining the results of sect. 5.1, 5.2, 5.3 and 5.4 the following recommendations can be made in terms of Ambient Law. We reiterate that,

in order:

- to prevent unwarranted invasion of our privacy in the form of the disclosure of highly sensitive knowledge about our health status, ethnicity, personal character etc.;
- to prevent unbridled discrimination on the basis of such sensitive knowledge;
- to allow for the contestation of decisions taken on the basis of BBP (due process),

we must develop:

- new legal transparency tools
- that need to be articulated in the BBO technological infrastructure.

Inspired by the German proposal for the regulation of credit scoring, we suggest the following legal TETs:

In the case of a BBP that concerns a particular individual, based on behavioural biometric group profiling, a data controller should provide that person with access to:

1. the types of data used to construct the group profile, and their relative impact on the constitution of the group profile;
2. the constitution of the group profile in the specific case in an easy and generally intelligible form.

Obviously, these constitute Type A legal TETs, as the technological infrastructure to exercise these rights depends on cooperation by the data controller, or on taking a case to court and entering the long process of enforcing compliance via a legal procedure. Next to this type of transparency right, therefore, Type B legal TETs must be developed, for instance ensuring:

3. a fundamental right to counter profile one's environment by collecting, aggregating and analysing machine readable data that allow one to guess the response of one's environment to one's biometric behaviours.

Based on the present state of the art regarding technological TETs, we suggest investing in the following research:

With regard to Type A TETs, technologies need to be further developed that allow for:

1. detection of the violation of rules with regard to collection, accuracy, sharing or usage of data (like in the case of TAMI), especially by further developing the inference machine to work with arbitrary data that allow a person to 'play around' and test which biometric behaviour results in what type of responses (this inclines towards Type B TETs)
2. creation of automated audit facilities based on logging of meta data (like in the case of Privacy Evidence), especially by further developing a data mining component that allows to try out different privacy policies, providing potential consequences (which inclines towards Type B TETs)
3. creation of data tracks that allow a user to view what data she leaked when and to whom, for which purpose, allowing a user to request access to the data in order to require correction or destruction (like in the case of the PRIME prototype), enhanced by e.g. developing a data mining component that can simulate the inference of profiles of the data, based on access to data bases containing anonymised behavioural biometric data from other users (this again inclines towards Type B TETs)
4. creation of a 'playground for users' in which they can see which of their data matched with what type of group profiles, allowing them to change the input to discover how this changes the applicable profiles (like in the case of Amazon.com), finally allowing them to erase their own behavioural biometric data or to even prevent the collection thereof (though this 'playground' still depends on the data controller, it follows the logic of Type B TETs)

With regard to Type B TETs, the following types of technologies need to be developed:

1. personal digital assistants (PDAs) that observe, record, aggregate and mine machine-readable data leaked by the environment, as well as those leaked by the owner of the PDA, in order to infer how the environment responds to a person's biometric behaviours (counter profiling)
2. human machine interfaces (HMIs) that provide easily accessible information about the actual and inferred future behaviours of one's environment, correlated with one's own biometric behaviours; this information should not necessarily consist of text or graphs but should rather 'speak' to one's behaviours in a more immediate manner

As to counter profiling, we insist that this will provide a much needed perspective that is independent from those provided the relevant data controllers. If the right type of HMIs can be developed, this should provide us with intuitive guidance *for* or 'gut feeling' (Gigerenzer, 2007) *about* our interactions with and within autonomic environments. In fact, Gigerenzer claims that the beauty of our autonomic brain processes lies in the fact that these processes do not consist of the calculation and computation all possible data but instead depend on a learning process about which are the simplest rules to be followed to achieve our goals. The example of a socio-technical 'mirror', developed by Nguyen and Myatt (2002), as discussed above, demonstrates how such a framework could allow a user to 'play around' with her socio-technical environment, based on different levels of information provision. At the same

time, we should not entirely depend on such intuitive counter profiling. We also need to create effective – technologically embodied - rights to open the black box that resides with the data controller in order to refine our intuitions or to contest the application of a profile. Only an effective mix of Type A and B TETs will do the job of giving us an idea about the consequences of our actions, which is a precondition for the protection of our privacy and many other private and public interests that may be fragile in AmI environments.

The recommendations imply a research agenda, in order to further operationalise the technologically embodied rights that have been proposed. If we want to provide the European citizen with a socio-technical environment that allows her to play with the system in order to find out how her behaviour is interpreted, we urgently need to invest in collaboration between social scientists, computer scientists and legal scholars with regard to these new legal-technical tools. The amount of questions raised by these proposals on all 3 accounts (social, technical and legal) are numerous if not indefinite and we shall have to work on them while building the AmI environments that utilize BBPs. Recalling Neurath's reference to the need to repair a ship on the open sea, this should not be a problem but an urgent and rewarding challenge.[69]

[69] 'There is no way of taking conclusively established pure protocol sentences as the starting point of the sciences. No tabula rasa exists. We are like sailors who must rebuild their ship on the open sea, never able to dismantle it in dry-dock and to reconstruct it there out of the best materials. Only the metaphysical elements can be allowed to vanish without trace.' (Neurath, 1959: 201).

7 Bibliography

1. Akerlof GA (1970) The market for 'lemons': Quality, uncertainty and the market mechanism. Quarterly Journal of Economics 84: 488–500

2. Andronikou V et al. (2007) Biometric Implementations and the Implications for Privacy and Security. FIDIS Journal 1. Available at: http://www.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf

3. Article 29 Data Protection Working Party (2004) Opinion on More Harmonised Information Provisions. WP 100 Version of 25 November 2004. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

4. Article 29 Data Protection Working Party (2007) Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities. WP 129 of 9 January 2007. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp129_en.pdf

5. Art. 29 Data Protection Working Party (2000) Working Document on Privacy on the Internet - An integrated EU Approach to On-line Data Protection. WP 37 of 21 November 2000. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

6. Art 29 Data Protection Working Party (2008) Opinion 1/2008 on data protection issues related to search engines. WP 148 of 4 April 2008. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf

7. Article 29 Working Party (1995) Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 25.11.2005.

8. Article 29 Working Party (1999) Opinion 3/99 on Public sector information. WP 20 of 3 May 1999. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp20en.pdf

9. Backhouse J, Hildebrandt M (2005) Descriptive analysis and inventory of profiling practices. FIDIS Del D7.2. Available at: http://www.fidis.net/resources/deliverables/profiling/#c1764

10. Beauchamp TL, Childress JF (2001) Principles of biomedical ethics. Oxford: Oxford University Press

11. Bellotti V, Sellen A (1993) Design for Privacy in Ubiquitous Computing Environments. In: Proc. of The Third European Conference on Computer Supported Cooperative Work (ECSCW'93). Milan, Italy: Kluwer Academic Publishers, pp. 77–92

12. BioPassword Inc. (2006) Authentication Solutions Through Keystroke Dynamics. BioPassword White Paper. Available at: http://www.infosecurityproductsguide.com/technology/BioPassword.html

13. Böhme R (2008) Conformity or Diversity: Social Implications of Transparency in Personal Data Processing. In: Proc. of Workshop on the Economics of Information Security (WEIS), Tuck School of Business, Dartmouth College, Hanover, NH, June 2008. To appear.

14. Böhme R, Koble S (2007) Pricing Strategies in Electronic Marketplaces with Privacy-enhancing Technologies. Wirtschaftsinformatik 49: 16–25

15. Boyatzis CJ, Satyaprasad C (1994) Children's facial and gestural decoding and encoding - relations between skills and with popularity. Journal of Nonverbal Behavior 18: 37-55

16. Bovet P, Liechti O (2007) Webbiometrics. Diploma thesis University of Applied Sciences Bern. Available at: https://staff.ti.bfh.ch/fileadmin/home/bie1/diplomarbeit/webbiometrix-2007-2008/Endbericht_WebBiometrix.pdf

17. Brand JD et al. (2001) Visual Speech: A physiological or behavioural biometric?. Lecture Notes In Computer Science 2091: 157-168

18. Brûckner L, Voss M (2005) MozPETs – a Privacy Enhanced Web Browser. In: Proc. of the Third Annual Conference on Privacy and Trust (PST05) Canada

19. Bygrave LA (2002) Data protection law; approaching its rationale, logic and limits. Information law series 10. The Hague, London, New York: Kluwer Law International

20. Cattin PhC (2002) Biometric Authentication System Using Human Gait. PhD Thesis Diss. ETH No. 14603. Zürich. Available at: http://e-collection.ethbib.ethz.ch/eth/redirect/matching.php?type=diss&nr=14603&part=fulltext

21. Chadwick R et al. (1997) The right to know and the right not to know. Aldershot, U.K.: Avebury Ashgate Publishing Ltd.

22. Chappell D (2006) Introducing Windows CardSpace .Windows Vista Technical Articles

23. Chang W(2005) Keystroke Biometric System Using Wavelets. Lecture Notes in Computer Science 3832: 647-653

24. Checco J (2003) Keystroke Dynamics & Corporate Security. WSTA Ticker Magazine

25. Coebergh JWW (1991) Preventie van sterfte aan borstkanker door vroege opsporing. Ethiek en recht in de gezondheidszorg 20: 41-49

26. Custers BHM (2005) The Risks of Epidemiological Data Mining. In: Tavani H (ed.) Ethics, Computing and Genomics: Moral Controversies in Computational Genomics. Boston: Jones and Bartlett Publishers, Inc

27. Custers BHM (2004) The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Tilburg: Wolf Legal Publishers

28. De Hert P et al. (2007) De WBP na de Dexiauitspraken. Privacy en Informatie 4:147-157

29. Dötzer F (2006) Privacy Issues in Vehicular Ad Hoc Networks. Lecture Notes on Computer Science 3856: 197-206

30. Ekman P et al. (1987) Universals and cultural differences in the judgments of facial expressions of emotion. Journal of Personality and Social Psychology 4: 712–717

31. Erickson T, Kellogg W (2000) Social Translucence: An Approach to Designing Systems that Support Social Processes. ACM Transactions on Computer-Human Interaction 7, 1: 59-83

32. Fasel B, Luettin J (2003) Automatic facial expression analysis: A survey. Pattern Recognition 36: 259-275

33. Feinberg J (1984) Harm to others. Oxford: Oxford University Press

34. Fischer-Huebner S, Hedbom H (eds.) (2008) Deliverable D14.1.c Framework V3, March 2008. PRIME Project

35. Frankena WK (1973) Ethics. Englewood Cliffs, New Jersey: Prentice Hall

36. Fridlund AJ, et al. (1984) Facial expressions of emotion. In: Siegman AW, Feldstein S (eds.) Nonverbal behavior and communication (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

37. Foster I (2002) What is the Grid? A Three Point Checklist. GRID Today, July 20th, 2002

38. Gamboa H, Fred A (2004) A behavioral biometric system based on human-computer interaction. In: Jain AK, Ratha NK (eds.) Biometric Technology for Human Identification. Proceedings of the SPIE 5404: 381-392

39. Gandy O (2006) Data Mining, Surveillance and Discrimination in the Post-9/11 Environment. In: Haggerty KD and Ericson RV The New Politics of Surveillance and Visibility. University of Toronto Press

40. Geller LN, Alper JS, Billings, PR, Barash, CI, Beckwith J, Natowicz M (1996) Individual, family, and societal dimensions of genetic discrimination: a case study analysis. Science and Engineering Ethics 2, 1: 71-88

41. Geradts Z, Sommers P (2008) Forensic Profiling. FIDIS deliverable 6.7c. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.7c.Forensic_Profiling.pdf

42. Gigerenzer G (2007) Gut Feelings. The Intelligence of the Unconscious, Penguin

43. Hermeren G (1999) The right to know and not to know. In: Who owns our genes; proceedings of an international conference. Tallinn, Estonia: Nordic Committee on Bioethics & Nord Biotechnology

44. Hildebrandt M (2009) Who is Profiling Who? Invisible Visibility. In: Gutwirth S et al. (eds.) Reinventing Data Protection?. Dordrecht: Springer

45. Hildebrandt M, Gutwirth S (eds.) (2008) Profiling the European Citizen. Cross-Disciplinary Perspectives. Springer: Dordrecht

46. Hildebrandt M, Koops BJ (2007) A Vision of Ambient Law. FIDIS Deliverable 7.9. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf

47. Hildebrandt M, Meints M (2006) RFID, Profiling and AmI. FIDIS Deliverable 7.7. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf

48. Hildebrandt M and Gutwirth S (2007) Profiling the European Citizen. Cross-disciplinary perspectives. FIDIS Deliverable 7.5

49. Jendricke U et al. (2000) Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet. In: Proc. of the 16th Annual Computer Security Application Conference.

50. Jiang X et al. (2002) Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing. In: Borriello G, and Holmquist LE. Proc. of Ubicomp 2002: 176-193. New York, NY: Springer

51. Jin S et al. (2007) Driver fatigue detection using a genetic algorithm. Artif Life Robotics 11: 87–90

52. Kamp M, Weichert T (2005) Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken der Verbraucher. Kiel. Available at: http://www.bmelv.de/cln_045/nn_749972/SharedDocs/downloads/02-Verbraucherschutz/Markt/scoring.html__nnn=true

53. Kaplan S, Kaplan R (1982) Cognition and Environment: Functioning in an Uncertain World. Praeger Publishers

54. Kettebekov S (2004) Exploiting prosodic structuring of coverbal gesticulation. In: International Conference on Multimodal Interface: 105-112

55. Last J (1996) Professional Standards of Conduct for Epidemiologists. In: Coughlin SS, Beauchamp TL (eds.) Ethics and epidemiology. New York/Oxford: Oxford University Press

56. Lips A et al. (2004) Issues of online personalization in commercial and public service delivery. Tilburg

57. Lyon D (2002) Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination. New York, Routledge

58. Macklin R (1992) Privacy and control of genetic information, In: Annas GJ, Elias S (eds.) Gene Mapping. Oxford: Oxford University Press.

59. Neurath O (1959) Protocol sentences. In: Ayer AJ (ed.) Logical Positivism. Free Press, Glencoe, IL

60. Nguyen DH, Mynatt ED (2002) Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems. Georgia Institute of Technology. Atlanta. Available at: http://smartech.gatech.edu/handle/1853/3268

61. Odlyzko A (2003) Privacy, Economics and Price Discrimination on the Internet. In: ACM International Conference Proc. Series 50. Proc. of the 5th international conference on Electronic commerce: 355-366

62. Padmanabhan B (2007) Clickprints on the Web: Are there signatures in Web browsing data?. Available at http://knowledge.wharton.upenn.edu/papers/1323.pdf

63. Ravenschlag I (1990) Een moreel recht om niet te weten. In: Ravenschlag I et al. (eds.) Aids; Instellingen, individu, samenleving. Baarn: Uitgeverij Ambo BV

64. Rejman-Greene M (2001) Biometrics - Real Identities for a Virtual World. BT Technol J 9, 3: 115-121

65. Revett K et al. (2007) A machine learning approach to keystroke dynamics based user authentication. Int. Journal of Electronic Security and Digital Forensic. Interscience Publishers

66. Sackmann S, Strüker J, Accorsi R (2006) Personalization in Privacy-aware Highly Dynamic Systems. Communications of the ACM 49, 9: 32-38

67. Scherer KR (1999) Vocal effect expression: A review and a model for future research. Psychol. Bull.:143–165

68. Schneier (2007) Beyond Fear. New York: Springer

69. Schreurs et al. (2008) *Cogitas ergo Sum*. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In Hildebrandt M and Gutwirth S (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives. Springer: Dordrecht

70. Schreurs et al. (eds.) (2005) Report on actual and possible profiling techniques in the field of Ambient Intelligence. FIDIS Deliberable 7.3. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.3.ami_profiling.pdf

71. Schwartz PM (2000) Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control and Fair Information Practices. Wisconsin Law Review: 743-788

72. Solove D (2004) The Digital Person; Technology and Privacy in the Information Age. New York: New York University Press

73. Sujdak EJ (2001) Ethical issues with target marketing on the Internet. Paper presented at the International Symposium on Technology and Society (ISTAS 01), July 6-7, 2001, Stanford, Connecticut

74. Van Wel L (2001) Web mining in a business context: An ethical perspective. Master's thesis. Eindhoven: Eindhoven University of Technology

75. Vedder AH (2000) Discriminatiegronden in het Informatietijdperk. In: Holtmaat R (ed.) De toekomst van gelijkheid; de juridische en maatschappelijke inbedding van de gelijkebehandelingsnorm. Deventer: Kluwer.

76. Vedder AH (1996b) Privacy en woorden die tekort schieten. In: Nouwt S, Voermans W (eds.) Privacy in het informatietijdperk. Den Haag: SDU Uitgevers

77. Vedder AH (1999a) KDD: The challenge to individualism. Ethics and Information Technology 1: 275-281

78. Weitzner J et al. (2006) Transparent Acountable Data Mining: New Strategies for Privacy Protection. Computer Science and Artificial Intelligence Laboratory Technical Report: MIT-CSAIL-TR-2006-007. Massachusetts Institute of Technology, Cambridge, Ma, USA

79. Zarsky TZ (2002-3) Mine Your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion. Yale Journal of Law and Technology 5: 1-56

80. Zwick D, Dholakia N (2004) Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. Journal of Macromarketing 24, 1:31-43

8 Abbreviations

AmI - ambient intelligence
AmLaw ambient law
BB - behavioural biometirc
BBP - behavioural biometric profile
CER - cross-over error rate
EET -
EER - equal error rate
FAR - false acceptance rate
FRR - false rejection rate
GA - genetic algorithm
PhB - physical or physiological biometric
NN - neural network
PET - privacy enhancing tool
TET - transparency enhancing tool (legal or technological, or both)
WOT - web of trust