FIDIS

Future of Identity in the Information Society

Title:	"D7.2: Descriptive analysis and inventory of profiling practices"
Author:	WP7
Editors:	Mireille Hildebrandt (VUB) James Backhouse (LSE)
Reviewers:	Thierry Nabeth (INSEAD) Martin Meints (ICPP)
Identifier:	D 7.2
Type:	[Deliverable]
Version:	1.0
Date:	Wednesday, 29 June 2005
Status:	[Final]
Class:	[Public]
File:	fidis-wp7-del7.2.profiling_practices.doc

Summary

Deliverable 7.2 represents a genuine attempt to crystallise the multi-disciplinary nature of the FIDIS Network of Excellence in a document assessing the many facets of profiling, with contributions coming from across a wide spectrum of disciplines. Profiling is a powerful, critical and worrying technology because it is probably the only way that massive volumes of data about individual and group behaviour can be mined, whether for nefarious or benign purposes. Ever larger volumes of data have been the holy grail of generations of social scientists, medical researchers and technologists, and with profiling alongside new data-gathering technologies such data is available with the means to mine it for all its value. This deliverable examines how different approaches to profiling are taken, reviewing along the way some of the different technology contexts in which it can be used. Though matters of privacy and security loom behind every corner, the main focus of this deliverable is not on such issues. Subsequent deliverables will move into this. Clearly, with its multiple applications in marketing, law enforcement and surveillance, e-medicine and e-health - to name just some, there exist currently many avenues along which profiling might progress, but unless the consumers and citizens of today and tomorrow have more knowledge of the actual workings of this technology, they will not be able to make informed decisions about how to respond when they are increasingly importuned for their personal data in the future. This report hopes to make a useful contribution to the vital task of explaining how profiling may impact the life of citizens and consumers in the coming years.

Copyright Notice:

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	27.01.2005	• Initial release (Mireille Hildebrandt)
0.2	01.02.2005	• Changes in structure and integration comments of Ana Canhoto
0.3	25.02.2005	• Integration comments Martin Meints
0.4	09.03.2005	• Changes in structure and content (especially definitions), following comments during the March workshop
0.5	03.05.2005	• Integration contributions from Ana Canhoto (5.3.1), Martin Meints (5.1.1, 5.2, 5.3.2, Appendix), Simone van der Hof (3.3.2, 4.3, Appendix), Emmanuel Benoist (3.3.1); provisional input added from Thierry Nabeth, Mark Gasson & Emmanuel Benoist, Angelos Yannopoulos, Anton Vedder
0.6	23.05.2005	▪ Integration of contributions from Jean-Paul van Bendegem and Mark Gasson (3.2.2 and 3.2.3 and Appendix), Anton Vedder (3.2.4), Zeno Geradts (5.4 and Appendix), Angelos Yannopoulos and Vasiliki Andronikou (3.3.2 and Appendix), Claudia Diaz (Appendix), and Thierry Nabeth, Albert A. Angehrn and Pradeep Kumar Mittal (3.3.2, 5.5 and Appendix).
0.7	02.06.2005	• Streamlining and editing Mireille Hildebrandt and Els Soenens.
0.8	14.06.2005	• Final edit James Backhouse, Mireille Hildebrandt and Els Soenens.
0.9	28.06.2005	• Integration of the comments of the internal reviewers, Thierry Nabeth and Martin Meints.
1.0	29.06.2005	• Post-edit for delivery (Denis Royer)

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)*
1 Executive Summary	M. Hildebrandt
2Working definitions	M. Hildebrandt, participants workshop March
3 Descriptive analysis	M.Hildebrandt, M. Gasson, A. Canhoto, J.-P. Van Bendegem, A. Vedder, E. Benoist, Th. Nabeth, J. Backhouse, A. Yannopoulos and V. Andronikou.
4 Purposes and effects	M. Hildebrandt, S. van der Hof, A. Canhoto, M. Meints
5 Fields of application	A. Canhoto, M. Meints, Z. Geradts, Th. Nabeth
6 Issues for further clarification	M. Hildebrandt
7. Appendix	A. Z. Geradts B. B. Körffer and M. Meints C. A. Yannopoulos and V. Andronikou D. E. Benoist E. E. Benoist and B.Anrig F. J.-P. Van Bendegem G. Th. Nabeth, A. Angehrn and P. Kumar Mittal. H. C. Diaz
8. Glossary	M. Hildebrandt
9. References	All, compilation by E. Soenens

Table of Contents

1. Executive Summary

Information society – knowledge society
In the eyes of many, one of the most challenging problems of the information society is the fact that we are faced with an expanding mass of information that both increases and changes as we move along. *Selection* of the *relevant* bits of information seems to become more important than the retrieval of all these data: the information is all out there, but what it means and how we should act on it may be one of the big questions of the 21st century. If an information society is a society with an exponential proliferation of data, a knowledge society must be the one that has learned how to cope with this.

Profiles as automated knowledge construction
One of the attempts to deal with the information explosion is the automated construction of 'knowledge' by the data mining of large data bases. With the use of mathematical, or rather statistical techniques, it becomes possible to search massive quantities of data for patterns of correlations that produce a new type of knowledge. This knowledge, consisting of linear or nonlinear correlations between data, is what profiles are all about. Rather than just a collection of unrelated data, a profile is a set of correlated data. Whereas data is information, profiles – when interpreted – are knowledge constructs.

Interdisciplinar perspective of the main text
In this FIDIS deliverable 7.2 researchers from 11 FIDIS partners have put together their expertise and experience in the field of profiling. The aim of this deliverable is first of all to provide a comprehensive descriptive analysis of the process of profiling. It hopes to have created some common ground between the social, technological, mathematical and computer science perspectives that inform the process of profiling. As a consequence, apart from chapter 4, this deliverable does not yet elaborate extensively on issues of privacy, security and equality – even if present around every corner. Also the legal implications of profiling are not dealt with at this point. Deliverable 7.2 studies the techniques, technologies and practices of profiling, including its purposes and effects. It should function as a building block for subsequent deliverables that elaborate the legal aspect and the relationship with Ambient Intelligence (FIDIS deliverable 7.3); the implications for Europe as a constitutional democracy (FIDIS deliverable 7.4) and the relationship between RFID, AmI and profiling technologies (FIDIS deliverable 7.7).

In chapter 2 the concept of profiling is analysed by pointing out important distinctions, of which the difference between group profiling and personalised profiling is the most salient one (others include automated and hand made profiles, profiling of on-line and off-line behaviour, construction and application of profiles). Some working definitions are provided that incorporate these distinctions and point to the difference between a collection of data and a set of *correlated* data that describe a particular data subject (whether a person, a thing or an event). The purpose of profiling practices should be taken into account, as this determines both the adequacy of the construction of profiles and their impact on our world. The purpose of profiling is taken to be an assessment of risks and opportunities of the data subject, enabling private and public service providers to tune their services to the targeted group or person and enabling public authorities to anticipate threats to security, public health or any other relevant public good.

Chapter 3, the central chapter of this report, describes both group profiling and personalised profiling in some detail, to get a good grip on the difference between the two and a clear idea of the techniques involved. For group profiling the process of KDD (knowledge discovery in data bases) is analysed. KDD can be described in 6 steps: (1) collection and recording of data; (2) aggregating or preparing of the data in databases; (3) data mining or running algorithms through the database; (4) interpretation of the emerging patterns; (5) decision taking on the basis of the resulting profiles, and (6) proliferation of these profiles in the relevant social contexts. Special attention is given to data mining techniques, to get some interdisciplinary awareness of the nature of this type of knowledge. At the same time the importance is stressed of practical knowledge during the whole process of profiling: a combination of relevant experience, healthy scepticism and trained intuition is needed to collect the relevant data; to store them in a way that allows retrieval of interesting correlations; to find the algorithms that will locate interesting patterns; to have an adequate understanding of the possible meaning of the emerging patterns and to choose the optimum action based on this knowledge, considering also the wider implications in the real world. Group profiling produces group profiles that can be understood as a kind of prototype or abstract person. A group profile does not represent any particular person, but rather categorises persons as belonging to a certain group of category. Personalised profiling, on the other hand, focuses on the attributes of one individual, identifying and representing her on the basis of biometric features or past behaviour. The section on personalised profiling discusses user modelling in relation to adaptive applications and biometric profiling of individual data subjects. Personalised profiling can identify preferences and risks the profiled person may not be aware of, which gives the data controller an advantage in terms of knowledge over the data subject. One of the conclusions of this chapter is that the type of knowledge produced by profiling technologies is in several ways different from the findings of traditional social science research.

Chapter 4 deals with some of the wider implications of this new type of knowledge. After a brief exploration of the role of profiling in the emergence of data surveillance (dataveillance), the implications of personalised profiling are analysed, after which a more abstract mapping is constructed of the anticipated consequences of profiling. This is done in terms of purposes and effects.

Chapter 5 explores several fields of application, ranging from marketing, employment, financial institutions and e-learning to forensics. The different contributions aim to illustrate the state of the art in different fields, without pretending to provide a complete inventory. The idea is that these examples give the reader a sense of the actual functioning of profiling technologies in different contexts.

Chapter 6 locates issues for further clarification that should be dealt with in subsequent deliverables, such as the commodification of (personal) data and issues of privacy, security, trust, usability and equality.

Multidisciplinary Appendix
The multidisciplinary nature of the FIDIS consortium has as a consequence that the partners do not always speak each others language. The objective of this deliverable has been to focus on an interdisciplinary main text, that creates common ground for all those involved in the project. In the Appendix those involved in the different disciplines had the opportunity to address a more specialist audience, thus also allowing a more profound analysis of central elements of the analysis. This concerns forensic profiling in the field of RFID and biometrics;

legal grounds for customer loyalty programs in Germany; physical and behavioural biometric profiling; profiling of web users; mathematical tools for datamining; the nature and use of algorithms; user modelling in virtual communities and a description of the profiling game, played by PhD-students at the first PhD training event at Riezlern.

2. Working definitions of profiling: some distinctions

(VUB, Mireille Hildebrandt; input all partners via workshop 2-3 March 2005)

2.1 How to identify profiling?

In this paragraph we will construct some working definitions, meant to open a discussion rather than to close one. While trying to identify profiling we soon discovered that the term refers to rather different things that do not necessarily share common characteristics, but are related to each other in important ways. Pertinent examples are: (1) the term is used both for the construction and for the application of profiles; (2) group profiles have very different characteristics and a different impact from personalised profiles. Instead of trying to find indisputable characteristics that all meanings of profiling share, we will introduce a number of distinctions to enable a more refined analysis.

To clarify the use of some other terms, we provide some working definitions of a small set of terms often used it the context of profiling in the glossary, three of which we introduce at this point, to prevent possible confusion:

data subject:	the subject (human or non-human, individual or group) the data refer to
data controller:	the subject (person or organisation) that determines the purposes and means of the processing of data
(end) user:	the profiled data subject using a certain device (web, customer loyalty card) that facilitates the recording of data to be stored and processed for the data controller

It is important to notice that the profiled data subject can be a person, an organisation, a thing or other 'object'. In this deliverable we will focus on the use of profiling technologies to identify and represent the identity of persons and groups.

2.2 Profiling as technique, technology and practice

Profiling can provisionally be described as

- **the process of constructing or applying a profile of an individual or a group.**

This process involves *techniques* (methods) and *technologies* (combination of tangible instruments and techniques; hardware and software).[1] To give an example: identifying someone by means of fingerprints is a technique that requires training. At the same time it is a technology, involving hardware (ink and cards and/or electronic imaging devices). Fingerprinting is a good example because it has been practised for a long time before the computer took over; thereby demonstrating that profiling is not new. Interestingly DNA-profiling has relativised the categorical identification that fingerprint-experts used to claim.

Apart from being a technique and a technology, profiling is also a *practice*: a specific way of doing things, within specific contexts, with specific purposes. It requires a learning process

[1]. Compare Ihde D. 1993, *Philosophy of Technology: an Introduction*. New York: Paragon House, 47.

that integrates explicit with implicit knowledge. This means that profiling is a matter of expertise, of professional training and involves more than the mechanical application of explicit rules and procedures. Tesco's Clubcard director, Tom Mason, is quoted as admitting: 'You have to use intuition and creativity as well as statistical know-how, and you have to hope that you have identified the right things to test'.[2] Special attention must therefore be given to the social context in which these technologies are embedded, as they will influence the performance of profiling technologies.[3]

In chapter 5 examples will be given of applications of profiling practices in the fields of marketing, employment, the financial sector, forensics and e-learning, some of which will be further elaborated in the Appendix.

2.3 Profiles as knowledge construct

When checking a dictionary[4] we find three relevant entries for 'profile': (1) an outline; (2) a set of data; and (3) a concise biographical sketch. In the more specific literature on the type of profiles we are addressing here, we find that a profile is considered to be a *knowledge construct*, representing a subject (a person, a thing, an organisation or whatever). This 'knowledge' consists of *patterns of correlated data* and is often built on data collected over a period of time. When referring to profiles constructed on the basis of profiling technologies we could thus define a profile as 'a set of correlated data that identify and represent a data subject'. When the data subject is a single person we speak of a personalised profile, when the data subject is a group/a category or a cluster we speak of a group profile. This distinction is central to this document, see also par. 2.6.

It should be obvious that a profile is not the same as the thing, group or person that is profiled. Certain salient data enable one to draw a picture, an outline, that represents the 'original', always framed from a certain perspective. This is an important point: even if profiles are inferred in real time (think of AmI) and change continuously, they will always remain a reference to an original that cannot be reduced to its profile.[5] This is not to claim that the 'original' can be defined and compared with its profiles, as this definition will itself – again – be a profile. In the case of human beings the 'original' could be understood as the correlatable human person that forever escapes complete determination.[6] At the same time it should be acknowledged that the profile will often impact the 'original'. Just image that your online behaviour is being profiled for an advertising company that is looking for targets that are inclined to buy the products they advertise. The profile that emerges on the basis of monitoring your web surfing habits could indicate that you like sailing equipment; that you

[2] Humby C. Hunt T., et al. 2003, *Scoring points: how Tesco is winning customer loyalty*. London Kogan Page.
[3] Canhoto A. and Backhouse J., 2004, *'Constructing categories, Constructing signs – analysing differences in Suspicious Transaction Reporting practice'*, Information Integrity Group, London School of Economics, London.
[4] Merriam-Webster's Online Dictionary.
[5] Agre P.E., 2001, "Beyond the Mirror World: Privacy and the Representational Practices of Computing." Pp 29 – 62 in *Technology and Privacy*: *The New Landscape*, edited by Agre P.E. and Rotenberg M. Cambridge, Massachusetts: MIT.
[6] Hildebrandt M., 2005, "Are profiles justiciable?" Paper presented at the *Conference Is knowledge justiciable?* Essen , Germany 21 – 23 March 2005; Hildebrandt, M. (2005), "Privacy and Identity: a reply to Archard's *The value of Privacy"*, in *Privacy and the criminal law*, Antwerp Oxford: Intersentia 2005 (to be published).

like refined expensive food and wine; that you go to bed very late; that you read intellectual newspapers, etc. This data could be correlated with data from other – offline – databases, generating even more specific inferences about your preferences, wishes and desires. Still, this does not mean the profile defines you; rather, it offers an interesting perspective on what motivates you. This knowledge will then be used to customise advertisements, to influence your future buying patterns.[7] In the end it will 'regulate your access to, and participation in, the European Information Society'.[8]

This also means that – in the case of a person - the identity constructed during the process of profiling, must not be confused with the identity that the person being profiled experiences as her *sense of self*. The profile follows the logic of the recordable data, with the constraints inherent in computer technology. This issue, the inherently reductive character of a profile, is important because profiles may impact privacy and identity in the strong sense (concerning our sense of self). Since profiles will often affect our lives (providing or prohibiting access, enabling selection, inclusion and exclusion) it is of utmost importance to clarify in what ways and on what basis they affect our lives, without conflating profile and profiled person.

The issue is also important because in computer science and information theory it is often the case that 'an old-fashioned semantic associated network is taken to be the essential structure of all human knowledge'.[9] Knowledge representation (like an ontology) is often understood as a mirror of reality,[10] disregarding the discursive and/or semiotic nature of both knowledge and our perception of reality.[11] This can give rise to misunderstandings between the different disciplines that constitute the FIDIS consortium, challenging the partners to take the perspective of other disciplines to build more integrated forms of knowledge.

2.4 Automated and hand-made profiles

Within the FIDIS network the main focus will be on automated profiling technologies and practices. The advance of automated profiling is connected with the increase in the size of data sets recorded in databases. Two factors contribute to this increase: the increase in the number of records of data subjects and the increase in the number of fields or attributes describing each data subject.[12] This growth, in turn, has been driven by several factors. The increasing availability of computer systems and software applications, the generalised adoption of Internet and, in certain fields, the compulsory record-keeping mandated by government regulation mean that data is being produced and warehoused at unprecedented

[7] See on price discrimination the Report by Turow, Joseph, Lauren Feldman, and Komberley Meltzer, 2005, *Open to Exploitation. American Shoppers Online and Offline.* Annenberg Public Policy Center of the University of Pennsylvania.

[8] Levi M. and Wall D.S., 2004, "Technologies, Security, and Privacy in the Post – 9/11 European Information Society", in *Journal of Law and Society* 31 (2), 211.

[9] Van Brakel J.,1999, "Telematic Life Forms.", in *Techné: Journal of the Society for Philosop*hy *and Technology* 4 (3), 3.

[10] Agre P.E.,2001.

[11] Canhoto and Backhouse, 2004, 4-5.

[12] Fayyad, Piatetsky-Shapiro et al., 1996, "The KDD process for extracting useful knowledge from volumes of data", in *Communications of the ACM* 39 (11) 27 - 34. Hand, 1998, "Data mining statistics and more?", in *The American Statistician* 52 (2), 112 - 118. Bruha I., 2000, "From machine learning to knowledge discovery: a survey of preprocessing and postprocessing.", in *Intelligent Data Analysis* 4, 363 – 374.

rates. As a result, the typical database has increased between 9 and 9,999 times during the past 5 years, as illustrated in table 1:

Table 1: The typical size of some databases[13]

Types of Databases	1999	2004	Growth in size
Transactional	100 gigabytes	1 terabyte	9 times
Data warehouse	1 terabyte	100 terabytes	99 times
Data mart	20 gigabytes	1 terabyte	49 times
Mobile data	100 megabytes	10 gigabytes	99 times
Pervasive data	100 kilobytes	1 gigabyte	9,999 times

However, as we all know, long before computers made their way into everyday life, criminal investigators composed profiles of their unknown suspects, psychologists compiled profiles of people with similar personality disorders, marketing managers made profiles of different types of potential customers, and recruiting organisations wrote profiles of successful candidates for specific jobs. These profiles were often hand-made, even if based on established techniques and technologies.

In this deliverable the focus will be on automated profiling technologies, that seem to introduce a new type of knowledge construction. The advance of these computerised profiling technologies does, however, not eliminate the handwork. First, some types of profiling can only be custom-made, since they do not involve masses of quantifiable data. Second, even when profiles are generated automatically, both the algorithms that enable the automation and the evaluation of the results will require professional handiwork.[14]

2.5 Profiling online and offline behaviour

In the field of automatically generated profiles, we must also discriminate between profiling that takes online behaviour as its data-input, and profiling that concerns any type of off-line behaviour (e.g. using RFID-tags) or substance (e.g. using biometrics). The growth of online activities (web surfing, chatting, downloading information, subscribing to email newsletters, buying and selling of goods, booking of hotels, tickets for travel or theatre and other transactions) has increased the volume of data sets in databases, as mentioned in the last paragraph. This concerns information explicitly supplied by web users when applying for access or when concluding transactions on the web, but this is not the only (and probably not the main) source of information. Many data are recovered by tracking online behaviour by means of (third party) cookies that record the online activities of as many web users as possible, legally or illegally - discussed further in par. 3.3.2 and 3. With the advance of RFID technologies the tracking of off line behaviour may experience an upsurge, mirroring the possibilities of online tracking (scanner data, customer loyalty cards, transaction data of credit cards etc.), see e.g. par. 5.1.1. At the same time physical and anatomical biometrics seem to

[13] Source: Hardy Q., 2004, "Data of reckoning", in *Forbes*, 173, 151 – 153.
[14] Canhoto and Backhouse, 2004.

enable profiling the hardware of human beings to a previously undreamt-of extent, discussed in par. 3.3.4 and 5.4.

2.6 Group-profiling and personalised profiling: identification and representation

Profiles can be seen as knowledge constructs that represent and identify a data subject. Identification in this case does not mean that profiles should be reduced to tools of individuation. Other than a simple id-token, like an email-address or an attributed social security number, *group* profiles consist in correlated data that describe a person or group as a certain type of person or group, sharing a certain mix of static and/or dynamic attributes with others and thus belonging to the same group or category, even if not all attributes are shared by all members, see par. 3.2.4. In the case of personalised profiling, building on the processing of biometric or behavioural attributes of one person, a rich, sophisticated representation of a particular person can be constructed.

2.6.1 Group-profiling

When looking at the definitions of identification, compiled during the first phase of FIDIS workpackage 2 (the identity of identity), it seems that these definitions are focused on individualising a person or – in other words – disclosing which set of attributes uniquely characterises a person. Identification thus seems based on the difference between one person and everybody else. Even though group-profiling is an instrument of identification, it adds another meaning. Instead of discriminating a person *from* all other persons, group profiling seems to focus on identifying a person *with* (as part of) *a certain group of persons*. Identification – of a person as belonging to a group - could than be defined as

> *the process of establishing that a subject is an element of a specific set of subjects, by means of the set of correlated attributes that defines the group*

However, this seems to presume that the attributes that constitute the group are *all* shared by *every* member of the group, which is often not the case. As will be described in paragraph 3.2.4, this is only the case when dealing with a distributive profile. This means that the set of attributes that define the group are distributed equally to each member of the group. In most cases we are dealing with non-distributive profiles, which means that the attributes that define the group are not all shared by all members of the group. As should be clear, the application of a non-distributive group profile to a member of the related group can give rise to problems if the non-distributive character of the profile is not taken into consideration.

If we link the idea of a profile, as described in par. 2.3 above, to identification technologies, a working definition of a group profile could be:

- **a group profile is a set of correlated data that identifies a group, and/or when applied identifies a person as a member of a group**

Interestingly this group can be a set of people that consider themselves a group, having some kind of interaction as such, but it might also be that a person is identified as belonging to the

group of blue-eyed people, or the group of people with an increased risk of developing breast cancer. In that case the term 'group' means something entirely different. If we follow Custers on this issue, social science research has traditionally focused on groups that consider themselves a group, while profiling based on data-mining *produces* groups in the other sense. Group profiling in this sense is a form of categorisation and could be said to create a profile of an abstract person that does not necessarily apply to any particular person.

Group profiling will be discussed in par. 3.2.

2.6.2 Personalised profiling

Group profiling must be discriminated from the construction of profiles of a single person, for instance on the basis of sets of transactions or other data relating to one person. Most user modelling and biometric profiling fall into this category. Personalised profiling is highly relevant for the design of Ambient Intelligence (AmI) applications. Personalised and group profiling can easily be combined: (1) the use of personalised profiles can be combined with the use of group profiles if a person is estimated to belong to the relevant group; (2) databases containing personalised profiles can be mined to construct group profiles.

Personalised profiling will be discussed in par. 3.3.

2.7 Construction and application of profiles

Another important distinction that should be made is between the process of constructing a profile, for instance by means of data-mining technologies, and the process of applying a profile: using a profile to identify a person as a specific individual (individuation) and/or as a member of a specific group or category (categorisation). Notwithstanding the importance of this distinction, in practice advanced profiling technologies combine construction and application of profiles: while identifying a data subject these technologies adjust the profile, thus continuously applying and reconstructing profiles – often in real time.

Related distinctions concern bottom-up and top-down searches of databases; and correlating and monitoring of behavioural data. Par. 3.2.3, on data mining, will elaborate this.

2.8 Conclusion: profiling and identification

If we take the working definition of par. 2.6 we can define profiling as:

a. **the process of constructing profiles (correlated data), that identify and represent either a person or a group/category/cluster,**
b. **and/or the application of profiles (correlated data) to identify and represent a person as a specific person or as member of a specific group/category/cluster;**

To understand the meaning of profiling, we should add the purpose of profiling. Rather than at individuation, profiling seems to aim for risk-assessment and/or assessment of

opportunities of data subjects. This, however, cannot be taken for granted. If the interests of data user and data subject differ it may well be that the interests of the data controller, who pays for the whole process, will take precedence. Thus – in the end – what counts are the risks and opportunities for the data users. For this reason the purpose of profiling can best be formulated as:

c. aiming at the assessment of risks and/or opportunities for the data user (inferred from risks and opportunities concerning the data subject).

In par. 4 the purposes will be further elaborated and analysed. First, in par. 3 we will analyse the processes of group and personalised profiling.

3. Descriptive analysis of profiling

3.1. Introduction

Automated profiling (whether group or personalised) takes place in the process of:

- recording data (taking note of them in a computable manner)
- storing data (in a way that makes them accessible, aggregated in a certain way)
- tracking data (recording and storing over a period of time, linking data to the same data subject)
- identifying patterns and trends in the data (by running algorithms through the data base) and
- monitoring data (checking whether new data fit the pattern or produce outliers).

Only facts that are recorded as data 'count' as such. This means that even before the process of profiling starts, a translation takes place, converting events, situations and actions into what some like to call 'raw data'. Precisely because these 'raw data' are not the facts (events, situations or actions) they represent, real life can cause serious problems if the translation into computable data is or becomes inadequate - originally adequate input can prove to be inadequate due to changes in the facts they relate. This problem cannot be solved by building up databases in terms of a consistent knowledge representation (ontology). Consistent databases avoid the problem of subsequent translation between different knowledge representation systems that hold the same type of facts, but in different formats. However, although such a course of action can make data and databases more interoperable, they do not guarantee the actual adequacy of the translation. This problem can only be solved when data are not conflated with the facts they represent, since only then room is created to redefine the facts and/or recognise that the facts do not (anymore, or yet) fit the framework of computable data.

In par. 3.2 we will discuss the construction of group profiles, in par. 3.3 we will discuss the construction of personalised profiles.

3.2 Group profiling

3.2.1 Introduction

In this paragraph we will analyse the construction of group-profiles. As discussed above a group profile is a set of correlated data that identify and represent a group/category/cluster. To understand in what ways the information society has changed the construction of profiles, as compared with traditional social science research, we shall explore the way profiling based on data-mining works. First we will introduce the evolving de facto industry standard CRISP-DM, which will be compared to the semiotic analysis of knowledge discovery in databases (KDD) by Canhoto and Backhouse.[15] In par. 3.2.3 the process of data mining, that is central for group profiling, will be explored in more detail; in par. 3.2.4 the difference between distributive and non-distributive profiles will be described and in par. 3.2.5 some differences

[15] *'Constructing categories, Construing signs – analysing differences in Suspicious Transaction Reporting practice'*, Information Systems Integrity Group, LSE.

will be discussed between profiles as knowledge constructs and the knowledge produced by means of traditional social science research.

3.2.2 KDD (Knowledge Discovery in Databases)

3.2.2.1. Introduction

Generally speaking, the construction of group-profiles in the developing information society is based on computerised searches in large databases, containing massive amounts of (often personal) data. This 'knowledge discovery in databases' (KDD) can be described as 'the nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data',[16] and can incorporate a powerful tool known as 'data mining'. While the term data mining originates from the database research community, the term KDD comes from artificial intelligence and machine learning community.[17] However, the two terminologies are often used synonymously. In that case, the term 'data mining' is used in a broad sense to refer to the overall process of analysing data to discover previously unsuspected relationships that provide to the database owners interesting or valuable information.[18] More correctly, the term KDD is used to refer to this overall process, including the interpretation of the emerging results, while the term 'data mining' is used to refer specifically to the step of discovering the patterns and trends in the data.[19] [20] Notably, since this restricted definition of data mining focuses on the manipulation of the data by the computer it is sometimes called machine centred.[21]

3.2.2.2 Modelling the profiling process – towards a de facto standard

Although several models have been proposed, the Cross-Industry Standard Process for Data Mining (CRISP-DM) is a non-proprietary and freely available set of guidelines and a methodology developed to help guide the overall process.[22] Partly funded by the European Commission,[23] the methodology was created in conjunction with practitioners and vendors to supply checklists, guidelines, tasks, and objectives for every stage of the process.

The CRISP-DM model focuses on six key phases of the overall process, shown in Figure 1. The order of the phases is not strict, in the sense that the results of one phase may show that more effort is required in a previous phase; however, the general links between each phase are shown. The surrounding circle shows that the process itself is in fact a continuous process.

---

[16] Custers 2004, p. 17, referring to U.M. Fayyad, G. Piatetsky-Shapiro and P. Smyth, "From Data Mining to Knowledge Discovery: An Overview". In: idem and U.M. Fayyad et al., *Advances in knowledge discovery and data mining*, Menlo Park, California: AAAIPress/ The MIT Press, p. 6.
[17] Fayyad, Piatetsky-Shapiro et al. 1996; Piatetsky-Shapiro 2000, "Knowledge discovery in databases: 10 years after.", in *SIGKDD Explorations* 1 (2), 59 – 61.
[18] Hand 1998. Hand, Manila et al., 2001, *Principles of data mining*. Cambridge, MA, MIT Press.
[19] Fayyad, Piatetsky-Shapiro et al. 1996; Piatetsky-Shapiro 2000.
[20] Jackson J., 2002, "Data mining: a conceptual overview.", in *Communications of the Association for Information Systems* 8, 267 – 296.
[21] Peacock P.R., 1998, "Data mining in marketing: part 1.", in *Marketing Management* 6 (4), 8- 18.
[22] An electronic copy of the CRISP-DM Version 1.0 Process Guide and User Manual is available free of charge at: http://www.crisp-dm.org/
[23] Project number 24.959.

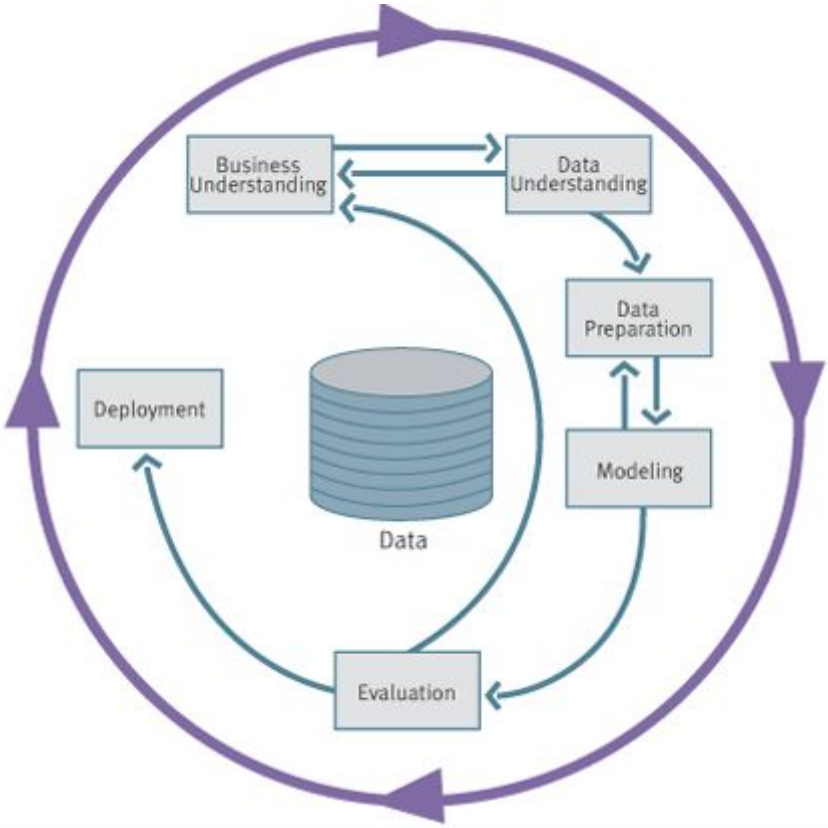


Figure 1: The phases of the CRISP-DM process model (from the CRISP-DM Process Guide and User Manual)

Each of the phases can be described as follows (adapted from the CRISP-DM Process Guide and User Manual):

Business understanding
This initial phase focuses on understanding the project objectives and requirements from a business perspective, then converting this knowledge into a problem definition and a preliminary plan designed to achieve the objectives.

Data understanding
The data understanding phase starts with an initial data collection and proceeds with activities in order to become familiar with the data, to identify data quality problems, to discover first insights into the data or to detect interesting subsets to form hypotheses for hidden information.

Data preparation
The data preparation phase covers all activities for constructing the final dataset (data that will be fed into the modelling tool(s)) from the initial raw data. Data preparation tasks are likely to be performed many times and not in any prescribed order. Tasks include table, record and attribute selection as well as transformation and cleaning of data for modelling tools.

Modelling (Data mining)
In this phase, various modelling techniques are selected and applied and their parameters are calibrated to optimal values. Typically, there are several techniques for the same problem type. Some techniques have specific requirements for the form of data. Therefore, stepping back to the data preparation phase is often necessary.

Evaluation
Before proceeding to final deployment of the model, it is important thoroughly to evaluate the model and review the steps executed to construct the model in order to be certain it properly achieves the objectives. A key objective is to determine if there is some important issue that has not been sufficiently considered. At the end of this phase, a decision on the use of the results should be reached.

Deployment
Creation of the model is generally not the end of the project. Even if the purpose of the model is simply to increase knowledge of the data, the knowledge gained will need to be organised and presented in a way that can be utilised.

Notably, each of these phases has a hierarchical structure, incorporating four further layers of abstraction; see **Figure 2**, which expands the simple model into a full guide for implementing a given application. However, a detailed analysis of these steps is beyond the scope of this document.

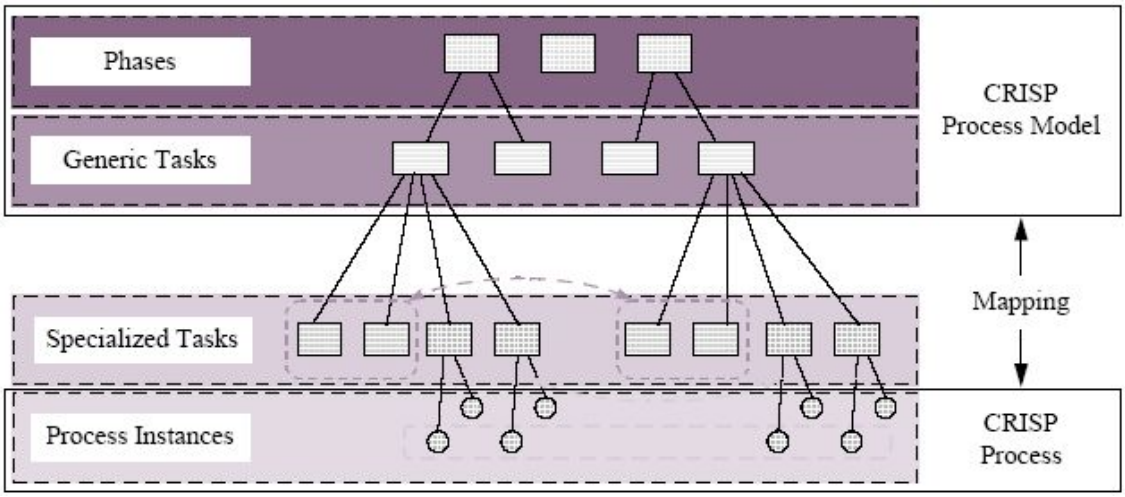


Figure 2: Hierarchical structure of the CRISP-DM methodology

3.2.2.3 Semiotic model of KDD

Canhoto and Backhouse have developed a model, based on semiotics and cognitive psychology. They apply this model to profiling within financial institutions that are obligated by law to report transactions that are suspected to involve money laundering. The profiling they investigate thus produces profiles that may lead to suspicious transactions reports (STR). An elaboration of this case study can be found in par. 5.3.1 below. Their model distinguishes 6 levels to analyse the process of KDD:

- Step 1: data collection; first level: physical
- Step 2: data preparation; second level: empirical
- Step 3: data mining; third level: syntactical
- Step 4: interpretation; fourth level: semantics
- Step 5: Determine actions; fifth level: pragmatics
- Step 6: The application context; sixth level: social situatedness

Step 1: data collection; first level: physical
The first level is the physical. In the case of STR's this refers to the collection of data that will serve as input for the data mining process that should produce profiles of STR's.

Collection of data can take place in a deliberate way, by asking people for information, or in less explicit – even illegal – ways. While off-line shopping with cash requires no identification or exchange of personal data, online purchases usually demand some input of personal data that in most cases will be stored and often sold as part of a database. Also, surfing behaviour can be observed and stored by (il)legal spyware that is located invisibly on websites or local computers without explicit or implicit consent. For example, as one visits certain websites, 'cookies' are placed on one's computer to allow monitoring of movement around that specific site in order to improve the user experience. In more nefarious applications, data on all of your on-line behaviour can be remotely stored, processed and used at a later moment. Notably, these cookies or other software are not necessarily related to the website you visited,[24] see also section 3.3.2.

So, whilst off-line transactions or other behaviour are often observed without leaving much of a trace, on-line transactions or surfing-habits often produce traces in the form of sets of data that are stored and processed and may be retrieved for entirely different purposes (even if this is illegal). The use of CCTV, embedded sensors, RFID-technologies and the emergence of Ambient Intelligence (AmI) could ultimately make off-line behaviour recordable and traceable in similar fashion.

What is important at this point is that however massive the amount of data in a database, incorrect and/or incomplete data may impact the construction of profiles by producing false negatives and false positives. This indicates the importance of the first two phases, described in the CRISP-DM model: business understanding and data understanding.

[24] For further details, see: http://www.cdt.org/testimony/ftc/991130mulligan.shtml; http://www.epic.org/privacy/profiling/; http://www.rfits.dk/English.3349.0.html

Step 2: data preparation; second level: empirical
The second level is the empiric. This refers to the processing of the collected data such that aggregated data are available at client level. Collecting and organising data in a consistent and useful way is commonly called warehousing.[25] In the case of anti-money laundering profiling technologies, the purpose is to identify suspicious transactions and, to do this, different transactions have to be linked to the same client, which will enable the identification of certain patterns of behaviour that give rise to suspicion of money laundering.

As data are collected they may not be of any use until aggregated. To increase the linkability personal data may be aggregated on the basis of residence, income, life-style or employment, medical history etc. The preliminary step in this process is the linking of personal data to each other as referring to the same person (even if the identity of this person is not known). In the case of anonymity this will not be possible, and in the case of pseudonymity this will be possible only for data linked to the same pseudonyms. This means that attempts to develop identity management devices that enable users to remain anonymous or to use pseudonyms, will affect the possibilities to construct profiles.

The empirical level of data preparation concerns the phase of data preparation in the CRISP-DM model. At the same time it presumes an effective business and data understanding, which means that the professionals working with the model may often revert back to these phases, to enhance the quality of data preparation.

Step 3: data mining; third level: syntactical
The third level is syntactic. An analyst will go through the data to find useful patterns (profiles), or to check if an existing profile fits with the aggregated data. This is the phase of modelling or data mining in the CRISP-DM model. Data mining is focused on the *automated* discovery of patterns in data or sets of data. The simplest pattern to be found is a linear correlation, for example:

A occurs in 93% of the cases that *B* occurs.

In data mining communities the term correlation is used only to refer to linear correlations. In many cases non linear or curvilinear correlations will emerge during the data mining process, made visible in graphs, that show non linear patterns (curves) that can be translated into non linear functions between the relevant variables. It should be remembered that a correlation does not imply a causal relation. In some cases the relationship itself may be meaningless because the causal relation is dependent on one or more other factors. Given these spurious correlations, misinterpretation is not uncommon.[26] Data mining techniques will be extensively dealt with in par. 3.2.3, as it is the core of the profiling process.

After patterns of correlated data have been discovered, the adequacy of the profile has to be tested by checking whether it indeed detects transactions that raise suspicion of money laundering. This concerns the phase of evaluation in the CRISP-DM model. The problem of automated anti-money laundering profiling technologies is that usually they over-report, necessitating human resources alongside the automated profile - checking its results by hand.

[25] Berry and Linoff, 1997, *Data mining.techniques: for marketing, sales and customer support*. New York.
[26] For some examples of spurious correlations see: http://www.burns.com/wcbspurcorl.htm

Changing the profile however may result in too many false negatives, which increases the risk to financial institutions of being fined for not detecting suspicious transactions.

Step 4: interpretation; fourth level: semantics
The fourth level concerns semantics, which means putting the patterns that are identified as an indication of suspicious transaction into context. This can, for instance, be the legal context that determines which transactions are to be reported (in fact it is the case that thresholds are specified above which transactions have to be reported). Failing to disclose suspicions is an imprisonable offence in the UK since 2002, so the legislation offers an incentive to over-report for fear of being sanctioned.

Although it is possible to discover patterns and trends between data, the question is what they signify. It is possible to construct profiles, based on correlations, without having any interest in what caused or motivated the correlation. Or, while being interested, still acting on the profiles without having a clue as to reasons or causes. This is typical for marketing research since the 1970s. Regression analysis is a good example: people are for instance categorised as potential customers or credit risks on the basis of correlations found in large databases with personal data on life-style, income, employment, etc. The marketing specialist is not interested in finding out what motivates or causes the correlation; only in whether it works.[27] Even genetic profiles (linking specific genes to specific diseases for instance) are often based on correlations without any insight in the causal chains that could be involved. In contrast, data mining is able to uncover patterns and trends and also reveal the causal relationship behind them. This makes it a powerful tool, perhaps with more potential than the on-line analytical processing (OLAP) approach, discussed in par. 3.2.3.1.

Custers claims that 'when a pattern in data is interesting and certain enough for a user, according to the user's criteria, this is called *knowledge*'.[28] He defines patterns as 'interesting when they are novel (which depends on the user's knowledge), useful (which depends on the user's goal), and nontrivial to compute (which depends on the user's means of discovering patterns, such as the available data and the available people and/or technology to process the data)'. The pattern's certainty, according to Custers, depends on the integrity of the data and the size of the sample. To decide on the interest and certainty of the correlated data (the profile), the data user will have to evaluate or interpret the profile; this again refers to the evaluative phase of the CRISP-DM model.

Step 5: Determine actions; fifth level: pragmatics
The fifth level concerns pragmatics. At his point they integrate the theory of cognitive prototyping, that claims that experience leads to the construction of categories that function as a kind of prototype. The importance of such prototypes regarding a client's profile and anti-money laundering cannot be underestimated. On the one hand, if the prototype is adequate, it will facilitate identification for STRs, on the other hand, if it is too static or ill-suited, it will hamper identification (producing false positives and false negatives). Canhoto and Backhouse stress the role of professional experience both for the construction of algorithms at the syntactic level and for the interpretation of the profiles that are produced, that may call for

[27] Early criticism on such research Armstrong J.S., 1970, "How to Avoid Exploratory Research", in *Journal of Advertising Research*, 4, p. 27-30.
[28] Custers, Bart, 2004, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology.* Nijmegen: Wolf Legal Publishers, p. 19.

further action (reporting a transaction as STR or not). In terms of the CRISP-DM model we again find ourselves in the evaluation phase, that may demand looping back to earlier phases, as discussed while explaining the model.

After the results of the operations have been scrutinised, the resulting profiles will form the basis for certain actions. Often profiles will be used for selection/access purposes: determining for instance employment opportunities, health risks, insurance risks, targeted advertising, categorisation as potential terrorist or criminal. In terms of the CRISP-DM model we are now in the deployment phase.

Step 6: The application context; sixth level: social situatedness
The social level concerns the expectations or social norms that influence and determine the actions of the data-controller, e.g. what are the implications of different cultural settings within the EU for the way data-mining and profiling is practised? Canhoto and Backhouse discuss varying perceptions of corruption in different EU member states, related to different ideas about what is considered legitimate and they refer to different attitudes to banking secrecy. All these informal social norms influence the extent to which certain transactions are interpreted as suspicious. This social level is of real importance, because it puts profiling technologies in context. For FIDIS it is vital to take a broader view on profiling than just the perspective of technology, as this says little of the actual state of the art in the European Information Society.

3.2.3 Data mining

In this section the key step in KDD of data mining will be further explored. The exploration of the techniques involved that we propose to undertake in this section, can be demanding for readers that have not been initiated into computer science. However, since it is a crucial element of the process of profiling we will attempt some initial clarifications of the techiques involved (further elaboration will take place in the Appendix). As these techniques determine the outcome of the process of profile construction, we advocate some interdisciplinary understanding as a precondition to evaluate the implications of the application of profiles.

Data mining can be defined as data processing, using sophisticated data search capabilities and statistical algorithms to discover patterns and correlations in large pre-existing databases; a way to discover new meaning in data.[29] Data mining is a multidisciplinary field with strong quantitative roots. Its techniques have been developed mostly by the artificial intelligence community (e.g., machine learning and pattern recognition) and the mathematical community (e.g., statistics and uncertainty processing).[30] In general, there are two approaches to this data mining phase. top-down and bottom-up analysis.

3.2.3.1 Top-down analysis

Data mining techniques may proceed from a deductive process that looks for confirmation, or indeed departures, from accepted patterns or models of behaviour. In this sense, data mining

[29] See http://www.elook.org/dictionary/correlation.html.
[30] Bruha I., 2000.

is done in order to test hypotheses;[31] to fit models to a dataset;[32] or to identify behaviours that depart from the norm.[33] Hence, the goal is to *monitor* behaviour. This type of data mining comes close to traditional research in the social sciences, because it starts with a hypothesis that is then tested. This approach can be defined as On-Line Analytical Processing (OLAP), a particular decision support tool, since the database is essentially used simply to test the accuracy of a number of hypothetical patterns and relationships (usually manually generated). The approach becomes ineffective when the number of variables in the data is too large, and therefore too difficult or time-consuming to find a good hypothesis, let alone be sure that a better explanation does not exist.

3.2.3.2 Bottom-up analysis: directed and undirected

This approach differs from OLAP because, rather than verify hypothetical patterns, it uses manipulation of the data itself to uncover automatically such patterns. Data mining in this form is essentially an inductive process. Bottom-up analysis aims to generate hypotheses that can *explain* behaviour observed or predict future behaviour. As mentioned before, one of the interesting characteristics of profiling is the fact that the data user is not really interested in explaining behaviour in terms of causes or reasons, but only in the predictive significance of correlations. In general terms, bottom-up analysis can be performed with the support of a domain expert who will suggest which fields / attributes / features are the most informative – this is referred to as *directed bottom up approach.*[34] Such an approach by its very nature adds bias to the mining process. Equally, the assessment may utilise all available data[35] – this is referred to as *undirected bottom up approach*. It should be clear that *directed* bottom up analysis indicates some intuitive or reasoned hypothesis as to possible correlations. In practice, to a degree most data mining proceeds as directed bottom up analysis (to prevent the proliferation of spurious correlations).

In any automated KDD process, the basic tool used in data mining is either an algorithm or a heuristic.

3.2.3.3 Algorithms and Heuristics

It *seems* easy enough to define what an algorithm is. Given an initial state (a set of data, a description, a physical system, …), an algorithm is a procedure to transform the initial state into a desired end-state with certainty (or, if not, at least as close as possible to certainty). Usually the procedure has to be communicable or implementable and therefore an additional element of the definition is that an algorithm is *finitely expressible* (although consulting an oracle, say Delphi, if absolutely reliable, should be considered an algorithm, even when the oracle is not capable of explaining its powers).

The most important properties of algorithms relevant to a discussion about data mining and related topics are to the philosopher-mathematician's mind the following:

- The **choice of language** wherein to express the procedure can have a tremendous effect on the "success" of the algorithm (as is well known in computer science, hence the immense

[31] Berry and Linoff 1997; Chung and Grey, 1999, "Special edition: Data mining.", in *Journal of Management Information Systems* 16 (1) 11 – 16.
[32] Fayyad, Piatetsky-Shapiro et al. 1996.
[33] Jackson J., 2002.
[34] Berry and Linoff 1997.
[35] Nash K., 2001, "Casinos hit jackpot with customer data", on *CNN.com*.

variety of computer languages) because it influences strongly, among other things, the complexity of the algorithm,

- The **choice of support** or carrier for the algorithm. We tend to focus on computer programs as typical instantiations of algorithms, but if one agrees that kitchen recipes also count as algorithms, matters become more complex, for, in a kitchen setting, causality relations do play a part. A computer is, in that sense, a rather atypical object for its causality structure is deemed non-existent.
- All too often ignored is the problem of how one can know that the algorithm does what it is designed to do, i.e., **program verification**. Usually one runs into problems because the verification is much more complex than the program itself. A glance at the *Journal for Automated Reasoning* will reveal the scale of such problems. Hence the term "desired" in the definition of algorithm is highly problematic: do we have any guarantee that we will recognise the end-state as the "desired" state?
- Likewise, although the situation is improving, not enough attention is given to the problem of **inconsistency**: what to do if the algorithm is internally inconsistent, where the algorithm contains contradictory instructions: "if A is the case, do B", together with "if A is the case, do not-B" (this, of course, being the bottom case, easy to identify). Additional algorithms are needed to repair algorithms. Standard procedure is often to introduce *preferences*, but then the question is what the preferences are based on. If, e.g., an *Amazon* client changes his taste, should the program continue to suggest items according to the client's old taste or not?
- Perhaps less well-known are the intrinsic limitations to finding patterns. Any algorithm, if finitely expressible, will have limits to the complexity it can handle (*cf.* the work of Gregory Chaitin)[36]. This means that although patterns might be present in the initial data, the program will not identify them, as they will appear "**random**" for the program.

In short, all of the above features are centred around one basic concept: **complexity and how to deal with it**. Essentially, an algorithm is a series of (usually) mathematical operations that are performed on a set of data. Notably, each step in the algorithm is 'blind' (it needs no additional information), each step follows the previous step 'blindly' (no further information is required to determine the next step) and a final result from the process is guaranteed after a *finite* amount of steps. If *any* of these rules are broken, then the process is referred to as a heuristic, i.e. additional, usually expert, information is employed to decide some part of the process. A heuristic is a form of the directed bottom-up approach.

A wide range of data mining techniques exists based on algorithms and heuristics, however, here we shall focus on a selection of these to highlight some of the key differences in their approach. For further elaboration see Appendix, sections E and F.

3.2.3.4 Symbolic approach

The result of data mining process is some sort of classification of the data. In the simplest case, the patterns or trends can be represented by a set of rules. The rules can be of the form:

[36] Chaitin G.J. 1990, *Information, Randomness and Incompleteness. Papers on Algorithmic Information Theory*. London: World Scientific. Chaitin G.J., 1992, *Algorithmic Information Theory*. Cambridge: Cambridge University Press. Chaitin G.J., 1999, *The Unknowable*. Heidelberg: Springer Verlag.

"people having bought the 9th symphony are likely to buy the 8th"
or
"if the user lives in the region defined by the postal code 12101 or earns less than 5000€ per year, then s/he should not be sent a brochure for insurance"

Note that in the first case the rule aims to describe, while in the second case the rule aims to prescribe. Essentially, a rule is composed of a set of properties that can be true or false, called an antecedent, with the result termed a consequent. Rules that prescribe can be represented by the use of a 'Decision Tree'. A decision tree representing the brochure for insurance rules above is shown in Figure 3.

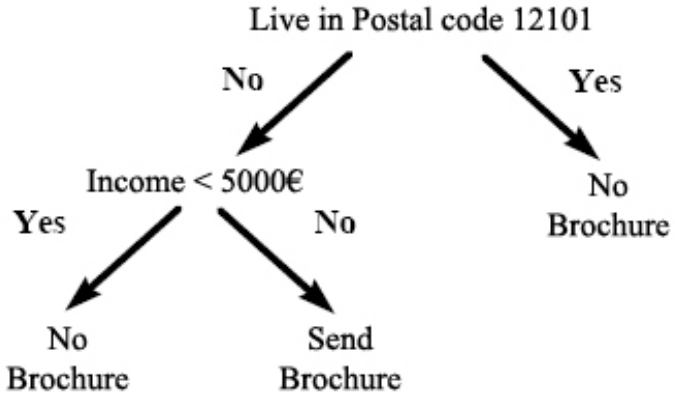


Figure 3: A simple Decision Tree

The hard rules used in such trees are not ideal, for example, someone with an income of €4999 will be excluded in the above example. Also such trees can become very complex, although heuristics can be applied to 'prune' the tree. Various algorithms can be used for building decision trees including CHAID (Chi-squared Automatic Interaction Detection), CART (Classification And Regression Trees), Quest, and C5.0 (Inductive algorithm descended from ID3 and C4.5).

Rule induction is a further technique which produces a set of independent rules that are unlikely to fit a tree structure and may not take every case into account.

3.2.3.5 Connectionist approach

This approach is characterised by the knowledge being contained in weights and nodes. It utilises techniques such as Neural Networks to fit non-linear classification boundaries to data. Such methods offer a potential benefit over simple rule-based approaches as they offer a way of efficiently modelling large and complex problems in which there may be hundreds of variables with many interactions between them. Neural networks utilise a training set of data which is used to configure the structure of the network during a learning phase. Following this phase, the network is able to classify new data based on the training set. Care must be taken however to avoid 'overfitting' the training data since the network is flexible enough to learn the specifics of the training data, rather than generalising it. Often a validation phase, utilising separate data, is used to monitor overfitting and halts training if overfitting is identified. Notably, the training phase can take a prohibitive amount of time, and the resultant networks

are not easily interpreted, that is, there is no explicit reasoning behind the results a neural network may produce.

3.2.4 Distributive and non-distributive profiles

(A. Vedder, TILT)

In the years to come, group profiling through data mining will become a powerful set of techniques of ever-growing importance. Applying these techniques results in generalisations about groups of persons, rather than about individuals. Regarding these generalisations, we must distinguish between distributive group profiles and non-distributive group profiles.[37]
Distributive profiles assign certain properties to a data or information subject, consisting of a group of persons however defined, in such a way that these properties are actually and unconditionally manifested by all members of that group. Distributive generalisations and profiles are phrased in the form of down-to-earth, matter-of-fact statements. *Non*-distributive profiles are framed in terms of probabilities, averages and medians, significant deviancies from other groups, etc. They are based on comparisons of members of the group with each other and/or on comparisons of one particular group with other groups. Non-distributive profiles are, therefore, significantly different from distributive profiles. If every member of a certain group has a chance of 30% of dying before the age of 30, the profile describing the group in terms of this chance is distributive. However, if members of a certain group have an average chance of 30% of dying before the age of 30, the profile describing this average is non-distributive. The properties in non-distributive generalisations apply to individuals as members of the reference group, whereas these individuals taken as separate individuals need not in reality exhibit these properties. For instance, an applicant may be refused a life insurance on the basis of a non-distributive generalisation of certain health risks of the group (e.g. defined by a postal code) to which he happens to belong, whereas he or she is a clear exception to the average risks of his or her group. In all such cases, the individual is primarily judged and treated on the basis of belonging to a group or category of persons and not on his or her own merits and characteristics.
Distributive generalisations and profiles amount to infringements of (individual) privacy, because the properties of the group are automatically properties of all individual members of that group. Of course, in order to count as an infringement of privacy, additional conditions apply, e.g., that the individuals involved can easily be identified through a combination with other information available to the recipient or through spontaneous recognition. In the case of non-distributive profiles, the profile remains attached to the data subject as constituted by a group. Because the properties included in the generalisation do not apply to individual members of the group in any straightforward sense, it is very hard to understand how they could be infringements of privacy. The information contained in the profile envisages individuals as members of groups; it does not envisage the individuals as such. Supposing for the sake of argument that the profile has been produced in a methodically sound and reliable way, it only tells us some "truth" about individual members of those groups in a very

[37] For more details on the distinction, see: Vedder A., 1997, "Privatization, information, technology and privacy: Reconsidering the social responsibilities of private organizations", in: Geoff Moore (ed.) *Business Ethics: Principles and Practice.* Sunderland, Business Education Publishers Ltd, 1997, 215-226. Vedder A., 1999, "KDD: The Challenge to individualism.", in *Ethics and Information Technology*, 1, 4: 275-281. Vedder A., 2001, "KDD, privacy, individuality and fairness.", in: R. Spinello and H. Tavani (eds.), *Readings in cyberethics.* Boston, Toronto, London, Singapore: Jones and Bartlett Publishers, 404-412.

qualified, conditional manner. This means that the information in non-distributive profiles cannot be traced back to individual persons. Therefore, privacy rules, as they are traditionally conceived, do not apply.[38]
This, however, does not mean that non-distributive profiles are morally and legally indifferent. Non-distributive profiles can be problematic from the viewpoint of fairness, distributive justice, equality and non-discrimination.
Some practical problems stand in the way of simple solutions. These have to do with the non-transparency of group profiling, which in turn has to do with the fact that the groups that are the data subjects of non-distributive profiles can often only be identified by those who defined them for a special purpose and not by those who belong to the group involved, and with the possibility of hiding or masking the use of specific sensitive profiles, by connecting them to profiles that refer to trivial properties. Finally, one must be well aware that the normal instruments for data protection that hinge on the control over the data by the individuals involved are not applicable: in the case of group profiles other individuals will be affected when the profile changes because specific individuals opt out or change input data. The locus of control should not only be with the individual that changed her data, because the group as a whole is affected. However, neither can the affected groups be the locus of control, because such groups mostly are nothing more than sets of individuals randomly brought together, were it not for one characteristic that they share.

3.2.5 Automated profiling and traditional social science research methodologies

Traditional social science usually starts with a hypothesis that is then tested by researching a sample of a population. This testing is done by means of surveys and/or participatory observation and/or in-depth interviews. The cost of testing is such that much attention is given to the preparation of both hypothesis and testing. The research aims at explaining situations or phenomena in terms of causes and/or reasons (motives).

Profiling and data mining work from a different perspective, and in a different setting.[39] First of all, the data that are researched have been recorded in databases, their retrieval does not depend on the memory of witnesses. Since the sixties this has already been the case for much social science research, as far as it collected and recorded data by means of surveys, usually based on statements made by 'data subjects'. These statements were the input for databases. Five important difference should, however, be pointed out.

- *First*, data mining often does not depend, or depends only in part, on data explicitly given by data subjects; instead **data are recorded without explicit consent – or even knowledge – of the data subject** (in real time by video cameras; online tracking of web-users; offline tracking of supermarket customers or banking clients, etc.). This also means the data do not indicate what people *say* about themselves but represent what they *do*.

[38] The question is whether the fact that such profiles are in fact applied to an identifiable person turnes them into them personal information, and/or whether this also turnes the data out of which the profiles have been constructed into personal information. In that case any data concerning any person is potentially personal information. See Deadman, S. (2005). *Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation*, Liberty Alliance Project, par. 4.1.2 on identity and identifiability.
[39] Custers 2004, 6-58.

- *Second*, the scope of the 'sample' that can be mined is enormous. The **results are not extrapolated but taken to cover the entire field** (and – hopefully – scrutinised for spurious correlations or low-quality data-input).

- *Third*, the **low cost** of setting up and searching an entire data base, in comparison with the databases filled with the results of surveys and interviews, makes possible **repeated and even continuous searching**. Often data are being collected just because it is possible to do so, without a clear idea (yet) of when or where it will be used. This allows the data controller and the data user to make data subjects seemingly transparent – while the whole process of data collection, storage and processing is usually hardly visible.

- *Fourth*, data mining is **often used to reveal patterns and trends instead of just testing** hypotheses. The techniques employed for validation of the results emerging on interrogation of data originate in the discipline of statistics. However, strictly speaking, data mining differs from traditional statistical methods because data mining relies on the use of software to interrogate the data, whereas in statistics the interrogation of the data is done by the researcher who makes all the decisions at each step of the inquiry.[40]

- *Fifth*, the results that emerge are not taken as proof of causal or motivational links. In fact, the purpose of data mining is not so much the construction of true knowledge for its own sake, but assessment of risks and opportunities in the future on the basis of patterns in past behaviour. **The meaning of the correlations is not sought but created, by acting on them**. Even in the case of genetic profiling, the correlations between genotype and phenotype are used to promote genetic testing, without any knowledge of the causal links between the two.

Evidently, the phrasing of the questions – and the algorithms used to locate correlations – influence the findings. Data users or even data subject may think that because a computer did the job, it must be right. This is not the case. As mentioned earlier, intuition and professional experience play a crucial role that also impacts the interoperability of profiling technologies within and between organisations and national jurisdictions.

3.3 Personalised profiling

3.3.1. Introduction

In this section, we will analyse personalised profiling, that differs from group profiling as far as it is focused on the identification and representation of an individual data subject. As discussed in chapter 2, a personalised profile is a set of correlated data that identifies and represents a single person. If data mining techniques are used to construct personalised profiles, only those data are searched that concern one specific data subject, for instance the

[40] Chan C. and Lewis B., 2002, "A basic primer on data mining.", in *Information Systems Management* 19 (4), 56- 60.

DNA structure of a specific suspect or the data of one specific web user. In the following paragraphs we will discuss user modelling (and user adaptive applications) and biometrics as two types of personalised profiling.

3.3.2 User modelling and user adaptive applications

3.3.2.1 Introduction

(Thierry Nabeth, INSEAD; Simone van der Hof, TILT)

Compared to group profiling, which is mostly based on stochastic approaches (KDD, machine learning or data-mining, see par. 3.2.3), user modelling is mainly characterised by knowledge-based, cognitive and more people-centric approaches (knowledge representation, user modelling, reasoning …). Personalised profiling in the sense of user modelling is principally concerned with the discovery of the individual characteristics of a particular user (rather than the characteristics of an abstracted user, as in the case of group profiling) and it covers all the approaches that can be used to help in the construction of the user model of a particular user.
User modelling can be used to intervene in applications and services that need to be informed about the user's characteristics in order to provide a personalised (or user-adaptive) interaction. Examples of such applications include personalised e-learning systems, that can take into account the previous experience of the user or her learning style to select the learning material that is the most adapted to that user; information retrieval, that can use information on the users preferences and interests to filter information; adaptive AmI application, that may be able to take into account the disabilities of a user and automatically select the mode of interaction that is the most appropriate; or e-commerce applications, that can use information to suggest to customers products that they are more likely to buy.
It is important to notice that few of these adaptive applications have reached the commercial stage, although Amazon, the online bookstore, has used it to enhance the user's experience. Many of these applications still only exist in the form of prototypes in computer labs. Personalised and adaptive systems represent, nevertheless, an important strand of research for the design of intelligent computer-based applications systems.[41] In association with user modelling, these researches aim at enhancing the quality of the interaction and therefore its effectiveness by taking into account the user specificity, such as her cognitive style, or competence, as well as her context of activity of this user. For instance the current tasks in which he is engaged or the organisational context.[42] Adaptive systems may be able to better support the user by:

[41] Fischer G., 2001, "User Modeling in Human-Computer Interaction", in *User Modeling and User Adaptive Interaction*. Kluwer Academic Publishers, 69 – 85. Brusilovsky P., 2001, "Adaptive Hypermedia", in *User Modeling and User- Adapted Interaction*. Kluwer Academic Publisher, p 87 – 110. Stephanidis C., 2001, "Adaptive techniques for Universal Access", in *User Modeling and User – adapted Interaction* 11, 159 – 179, Kluwer Academic Publishers. Kay J., 2000, "User modeling for adaptation", in *User interfaces for All*, Stephanidis (ed), Salvendy (General editor), *Human Factors Series*, Lawrence Erlbaum associates, 271 – 294. Andre E. et al., 2000, "Exploiting Models of Personality and Emotions to Control Behavior of Animated Interactive Agents", in *Fourth International Conference on Atonomous Agents*, 3 – 7, Barcelona. Fink and Kobsa, 2000, "A Review and Analysis of Commercial User Modeling Servers for Personalization on the World Wide Web", in *User Modeling and User Adapted Interaction, Special issue on Deployed User Modeling*, 10, 204 – 209 [Fischer 2001], etc.

[42] Nabeth, Angehrn, and Balakrishnan, 2004, "Integrating 'Context' in e-learning Systems Design", in *IEEE International Conference on Advanced Learning Technologies* (ICALT 2004) Joensuu Finland.

- filtering out the irrelevant information (reducing cognitive load), by delivering this information at the right time (just in time);
- choosing a form of delivery that maximises its impact on this user (taking into account the cognitive style of the user); or
- by proposing very contextualised help (the system is aware of the task in which the user is currently engaged into).

Research on adaptive systems has been conducted for applications in a number of domains such as e-learning,[43] e-commerce[44] or knowledge management.[45]

Personalised (user adaptive) applications generally rely on a user model that is used to represent the characteristic of the user such as name, preferences, location, etc. (all the personal information that can potentially be used to personalise the interaction), and each user is individually represented in the information system by a specific instance of this model. The technologies that are used to represent this use model are often proprietary, although we can observe some effort of standardisation in some application domain (for instance in e-learning, Human Resources, see the Fidis document del. 2.3 models) so as to facilitate systems interoperability and reuse. Of particular interest are the use of ontologies for user-modelling, for their capacity to represent and manipulate complex user models.[46]

The acquisition of user information (i.e. the construction of the profile associated with each user), which is a critical element for the effectiveness of personalised applications, often represent an important challenge. Indeed the direct obtaining of this information by asking the user has many limitations, because it is very inconvenient for the end-user and is not very reliable.

Different options actually exist to build (or acquire) this personal information exist:

- The **direct input by the end user** of personal information (via electronic forms) that we have just mentioned.
- The **extraction from databases**. In this case, the personal data originates from existing databases.
- The **capture of the user's activities**. The different actions and transaction of the user are recorded to be later used for building the user profile.
- The **inference** of this information from other user information. The value of some attributes of the user can be calculated (algorithm) or inferred (intelligent reasoning using heuristics or other means) from the value of other attributes (that are acquired using the other methods).

[43] Diogene 2002, *Survey on Methods and Standards for Student Modelling*, *Diogene Project*, September 2002.to be downloaded at http://www.diogene.org/archive.html.

[44] Kobsa, Koenemann, Pohl, 2000,."Personalized hypermedia presentation techniques for improving online customer relationships", in *The Knowledge Engineering Review* 16, 111 – 155.

[45] Razmerita L., 2004, "User modeling and personalization of the Knowledge Management Systems", book chapter in *Adaptable and Adaptive Hypermedia*, edited by Sherry Chen and G. Magoulas, published by Idea group Publishing.

[46] Razmerita, Angehrn and Maedche, 2003, "Ontology based user modeling for Knowledge Management Systems", in *Proceedings of the 9th International conferentce on User Modeling*, Pittsburgh, USA, Springeer – Verlag, 213 – 217. Dolog and Nejdl, 2003, "Challenges and benefits of the semantic web for user modelling", Paper presented at *the International workshop on Adpative Hypermedia and Adaptive web based Systems* (AH 2003) 20 – 24 May Budapest, Hungary. Heckmann et al., 2005, "GUMO – the general User Model Ontology", to appear in *Proceedings of UM 2005: International Conference on User Modeling*, July 24 – 30 2005, Edinburgh, UK.

- The use of **data mining techniques**. This later method refers to the approach described previously.

As indicated previously, the **direct entering of this information** by the end user (for example for getting coordinates or preferences) is the simplest method, but is an option that can only be used with moderation: people get quickly bored if they have to enter or to update too much information, resulting in poor quality profiles (incomplete or obsolete). People may also be afraid to be asked to disclose too much of their personal information, or simply do not like to elicit information about themselves (because of the frustration it may provoke in some cases). People can also make mistakes unintentionally (originating from simple errors or cognitive bias), or lie in order to fool the system, to get some advantages or to protect their privacy.[47] Finally, in some case, the frequency of update would be too important or too disturbing for the tasks performed to be done by the users, for instance, in the case of mobile AmI applications, asking the users to input their current location would be considered too inconvenient.

The **extraction from databases** (governmental, enterprise resource planning, training systems, or others) depends obviously on the existence of these databases (only partial user information is stored in these databases), but also on the permission that one can have to access these database and exploit their content. Often one of the main barriers associated with the use of databases for getting the user's information is related to privacy, which places limits on its use (purpose, cross-matching data, etc..).

The extraction of personal information from **the capture of user activity** is related to the recording of the actions of the users. Examples of processes that record information include e-commerce systems (such as Amazon) and fidelity programs that capture the history of different transactions associated with each of the customers, or virtual community systems that can capture the history of activities of the different members (such as age in the community, and number of postings). This activity is recorded in databases, or in different log files.

Some user information is profiled via **inferences** that can be performed on other existing information (such as the ones obtained by the previous methods). In this case, the inferred values result from different methods of calculation, such as algorithms, heuristics, or rules. Examples of information that can be profiled in this way include risk assessment of a customer by a banker, or the automatic determination of some user's preferences. For instance Crabtree and Soltysiak[48] (1998) use this method automatically to extract user's interests in an unobtrusive manner through monitoring various office automation systems that they use.

Group profiling, already described in a previous chapter, can also be used to help to determine the value of some personal user attributes. This approach relies on more global analysis, and data-mining or machine learning techniques. Pohl[49] (1997) for an example has investigated an approach that uses machine learning techniques to help in the construction of behaviour-oriented user models. Shearin & Lieberman[50] (2001) have used case-based

[47] Berendt, Günther, and Spiekermann, 2005, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior", in *Communication of the ACM (CACM*), vol 48, no. 3.

[48] Crabtree Barry and Stuart Soltysiak, 1998, "Identitfying and tracking Changing Interest", in *International Journal on Digital Libraries*, vol 2, nr.1, 38 – 53.

[49] Pohl W, 1997, "LaboUr – Machine Learning for User Modelng". in *Proceedings of the Seventh International conference on Human – Computer Interaction*. Amsterdam Elsevier.

[50] Shearin and Lieberman, 2001, "Intelligent Profiling by Example", in *ACM Conference on Intelligent User Interfaces*, Santa Fe, NM, January 2001.

reasoning methods to learn about user preferences in the domain of rental property by observing the user's criticisms of apartment features.

After personalized profiles have been constructed the aim will be to tailor products and services to the wishes and needs of individual customers based on the results obtained during the data analysis stage. This can be done, for instance, by supplying customers with tailor-made information, such as news, weather, and sports reports or by sending them advertisements specifically tailored for them.

Various techniques can be used to make offers to existing and potential customer.[51] For instance, in the case of recommendation systems, a distinction is often made between content-based filtering techniques and collaborative filtering. Sometimes manual rules are distinguished as well. When existing profiles indicate how a certain user values certain products or services, content-based filtering can be used to predict how this user will value brand new, yet similar products or services. According to the value predicted that the user places on these products or services, they can then be offered. The most important drawback to this method is that new products or services that do not fit within a customer's current profile are not filtered. Potentially, a situation of overspecialisation can arise.[52]

Collaborative filtering offers a potential solution to this problem. The idea is that if two users have the same interests and the first one is interested in product *x* then this product can also be offered to the second user. An example of this approach is the 'customers who bought' feature of Amazon.com. A key characteristic of collaborative filtering is that users have to value the products offered them. Therefore, some input from customers is required. If this information is available, 'nearest neighbour' algorithms can be applied to try and detect overlapping interests between users.[53]Collaborative filtering also has some drawbacks, one of which is scalability. As the number of users and of products and services increases, the use of 'nearest neighbours' algorithms becomes more and more laborious. A second problem is that a large number of products or services, combined with a reserve on the part of users to value these products and services, can lead to a situation in which making offers becomes difficult. Products that have not yet been valued by users are not used in new offerings. Finally, collaborative filtering does not take into account the contents of products and services, since only value that users put on them matters.[54] Part of these problems, especially the latter, can be addressed by combining content-based and collaborative filtering. Using these two techniques together appears to bring out the best in both of them, as content-based filtering and collaborative filtering are to some extent complementary.[55] Various techniques exist with which the other drawbacks can, at least partially, be addressed as well.

Hereunder follows a discussion of two examples of user modelling, concerning web users and virtual community environments.

---

[51] For a more detailed discussion see, for instance, Van Barneveld, 2003, *User Interfaces for Personalized Information Systems. State of te Art*. Telematica Instituut, 5-11.

[52] Smyth and Cotter, 2000, "A personalized elivsion listing service. Mixing the collaborative recommendation approach with ntent – based filtering seems to bring out the best in both methods", in *Association for Computing Machinery. Communications of the ACM*, August 2000, vol 43, nr. 8, 107 – 111.

[54] Shahabi and Chen, 2003, *Web Information Personalization: Challenges and approaches*, 3.

[55] Smyth and Cotter, 2000, 109.

3.3.2.2 Profiling of web-users

(Emmanuel Benoist, VIP)

Since the creation of the Internet, people have tried to get a better knowledge of the rather anonymous clients of web sites. First of all, they used the log files, tracing all the requests a server has received, to obtain statistics on the visitors. The evolution of the Internet then gave the possibility following the movements of a single visitor on a web site. This could be done using the technology of cookies. They are a small set of information sent by the server to the client. They are usually used to store a session ID. Such IDs are often used to grant access to a web site. The user with session ID 1234 has given a valid pair of username and password and can therefore access all the subsequent pages without retyping this information. This is also often used to create a virtual basket, the user visits a web site without following any logic, and the site uses the session ID to store all the purchased goods.

Such cookies are also often used by web sites for statistical and profiling purpose. Even without knowing it, the users are tracked, and web sites not only know what they have bought, they also know what they have just visited.
Cookies can also be used to monitor the behaviour of a user in more than one visit. This is useful for remembering the preferences of a user (e.g. preferred language or preferred default page). Such cookies are used to put together sessions that belong to the same person or at least virtual person. Cookies are only sent to the originating server. A client may be known by userID=1234 on website1 and with userID=5678 on website2. It may be very useful to merge information coming from the two sources. In order to do this we need a third web site for the merging of information. The two true web sites insert on all their pages images such as:
<img src="http://site3.com/images/blank.gif?userid=5678&website=website2">
The image is often a 1x1 pixel that cannot be seen. It allows the creation of a third party cookie that can be linked to both user IDs. Using this information it is possible to construct a network of all the web sites visited by a given (virtual) person.
The user can take countermeasures to prevent such abuses. But unfortunately, the degree of awareness of the common consumer concerning privacy hazards on the Internet is almost zero. Users can deactivate all cookies, unfortunately, it does block a lot of web sites and does not prevent those that really want to follow a session to do it, since there exists some turnover (userID in the URLs, IP-tracking or even "fake" DNS entry for each user). The user should nevertheless prevent cookies from continuing once a session finishes. It is possible to only accept session cookies, which protects the user from being followed over a long period. Third parties cookies cannot be used for anything of substantive interest to the user. They should therefore be always blocked.
Recently, these techniques have also been used in e-mails. Since e-mails can be written in HTML, it is possible to include images (visible like banners or invisible like an hidden pixel). Some marketers use the images to mark them with a userID, an address is validated once it has requested the included image.
See further elaboration in the Appendix, section D.

3.3.2.3 Profiling of users in virtual communities environments
(Thierry Nabeth INSEAD)

In this section, we are going to examine how behavioural personal user profiling and artificial agents can be used to stimulate the knowledge exchange process in virtual communities. A more elaborated presentation of this approach, as well as a set of references, is provided in the Appendix, section G: "Using user's Profiling and Artificial Agents for Stimulating the Knowledge Exchange Process in Virtual Communities".

Virtual communities: the participation challenge
One of the main challenges facing designers and operators desiring to build successful virtual communities is the establishment of a sustainable dynamic of participation amongst its members. Indeed, the essential value of a virtual community resides in the activities of its members and in particular is strongly correlated to their willingness to spend time, to interact with others in conversations, or to make available knowledge. The participation of the members of a virtual community in this knowledge exchange process is indeed not spontaneous, but is motivated by a certain number of elements and factors such as: expectation of reward (direct reward, increased reputation), personal satisfaction (altruism, efficacy, friendship), obligations originating in the desire to reciprocate, social imitation, commitment and consistency, etc.
This "mechanics" of the dynamics of knowledge exchange in communities and groups has been the object of numerous researches in different fields of study, such as knowledge management, computer supported collaborative work (CSCW), complexity, and sociology to name but a few, which have tried but never totally succeeded in understanding it, in order to derive some principles that would allow quasi-deterministically to create sustainable and effective knowledge-sharing virtual communities.

Using agents aware of the users' behavioural characteristics to stimulate participation
In this paragraph, we would like to present an approach in which personal behavioural profiling represents a central element for the creation of an intelligent application that could be used for stimulating participation in virtual community environments.
The main principle of this approach consists in the use of artificial agents that are aware of the behavioural profile of the members, and that intervene proactively using this information to stimulate member participation. In effect, this approach relies on two components: (1) the automatic construction (using a set of heuristics) of a behavioural profile of each member related to his knowledge exchange activity. (2) The generation of agent interventions that are the most likely to stimulate the participation of a particular member. The selection of the most effective interventions is based on the behavioural characteristics of the member.
The construction of this profile results from the observation of the actions of the user and the application of a set of heuristics helping to determine the participatory profile. The different actions that are captured and intervene in the determination of the participation profile include events such as: entering digital spaces, posting files, posting messages in bulletin boards, answering to messages, etc. The different behavioural patterns to which a particular user can be categorised include: the level of involvement (is he often present?) and the nature of his contributions (Is he only a lurker? Is he a contributor of knowledge assets? Does he participate in the discussions? Does he initiate discussions? etc.). Example of heuristic rules include: a user that has not connected to the system in the last month can be considered as

inactive. A user that post in discussion at least one time a week is committed in exchanging his knowledge. A user that has posted in the last three months at least a document is an active knowledge contributor.

The importance of personal behavioural profiling
The effectiveness of these different agent interventions depends greatly on taking into account the behavioural characteristics of the user, since it allows an agent to select the intervention that is likely to have the most impact on the user. Intervening in a way that might ignore the current nature and level of the participation would certainly lead to a poor result. For instance, it would be pointless inviting a member of a community to share some knowledge assets with others if this member shown in the past has very little readiness to participate in an interaction. On the other hand, it may be useful just to inform this same member of the benefit people get from interacting more with others. Similarly, understanding the member in terms of his collaboration style (is this member more a "network" person) or his current attitudinal state (is he busy) can help to avoid the selection of an intervention that would be considered a nuisance by the member.
In the approach previously described, the personal behavioural profiling can be used as an essential component to enable the design of a radically new category of (more intelligent) application. In particular, the success of this category of application relies in an important way on our capacity to observe the user, and to extract a relevant behavioural profile.

3.3.3 Biometric profiling

(Angelos Yannopoulos and Vasiliki Andronikou, ICCS)

In recent years biometric profiling has become a heavily researched and very broadly applied technology. The many possible examples of this include how the retinal scans of older science fiction movies can now be applied at surprisingly low cost in a multitude of realistic scenarios, or the 'fingerprint mouse' that can identify a computer user in a way similar to what was once 'high-tech' police technology. Biometrics can be divided into two major categories; *physiological (or passive)* and *behavioural (or active)* biometrics. The first ones refer to fixed or stable human characteristics and individual attributes such as face image, fingerprint, hand geometry, iris pattern and others, whereas behavioural biometrics are based on measurements concerning characteristics represented by those skills, actions or functions performed by an individual at a specific time for a specific reason: for example a person's signature or keystroke dynamics. Behavioural biometrics are less common than physical biometrics, but they are still often used, and it may be harder to apply law and to manage because of their fleeting nature.

A fully designed system might be presented as a simple recognition task where little additional variety could be expected: for instance, measure the timing of a user's typing and match statistics of a remote logon to statistics collected at registration time in order to achieve verification. In fact, however, behavioural biometric profiling can be considered along a number of (fairly) *independent* "axes", sets of activites or requirements whose combination shapes the overall application being considered.

- Type of measurement being made
  - Typing patterns
  - Mouse movements
  - Web navigation

- Access level in order to measure the person's activity
  - Application based on custom hardware
  - Full software access to a person's computer
  - Limited software access to a person's computer
  - Observation of the behaviour of a person's computer as an indication of the behaviour of the person him/herself
- Identification task
  - Identification of unknown person
  - Verification that a person is who he/she claims to be
- Technical method used
  - Standard statistic methods for pattern recognition
  - AI pattern recognition techniques (e.g. neural networks)
  - Knowledge technologies combined with a pattern recognition method

Choosing the trait to measure may seem to be the main inspiration behind the method, while the rest is just a matter of technical implementation; but this is not so. For instance, if attempting to verify user identity remotely (e.g. at a server when a user has logged on), the kinds of patterns that can be measured are different. The client-side application almost always buffers data and sends packets at specific points during an interaction (e.g. when a user presses a "submit" button, rather than sending each character as the user types). Thus, an analysis of the access level available in order to make measurements may be the prime drive for innovation, requiring a reasonably coherent definition of a composite behavioural trait to be arrived at that makes sense to try to recognise, but also can be measured correctly. For instance, we could imagine measuring web navigation patterns, if using hypertext with little information per page, many links and rapid traversal of the information space by the user through a fast connection. Clearly, an important issue is to ensure that adequate data can be collected both for initial profiling (training) and for subsequent recognition.

There is also a huge difference between the tasks of identification and verification. In the latter case, a person claims to have a certain identity, for which data has already been collected. Comparing newly collected data to the specific profile for the given user is a relatively easy task. In comparison, compiling a database that describes a multitude of people and then attempting to find which of these is best matched by an unqualified measurement is a much harder task. In this latter case, the data collected must be far greater in amount and highly accurate. This again reflects on the kind of applications possible. We might be able to recognise a totally unknown user e.g. on a corporate or university network where we have unlimited access and can monitor the user's typing continually throughout the session. However, we cannot identify a totally unknown person just from a login sequence (e.g. if the person is using a pseudonym and we want to match to a database or "real" people).

Finally, the technical tools used in each case need to be customised to the kind of behaviour addressed. If we take the measurements simply to be series of numbers, any range of pattern recognition methods can be tried. However, the raw measurements are not necessarily real "behavioural" measurements: for example, knowing the location of the screen of the mouse pointer for each millisecond during a user's session is not a direct reflection of behaviour; it might, instead, be necessary to model the application domain and estimate indices, from the raw measurements, such as jerkiness of the motion, speed of reaction to various stimuli, etc. Of course, the example would require a high degree of access to the person's computer, while a similar knowledge-based example might be constructed without requiring such access, e.g.

by finding elements of real behavioural patterns of web browsing before using pattern recognition to identify a full browsing session as originating from one user or the other.

Face recognition is a common example of a physical biometric which dates back to the 1960s and is beginning to be applied in a variety of domains, predominantly for security. This technology can be applied in a non-intrusive manner; it allows for human identification in a passive way, without the person's knowledge or cooperation since a person's face is easily captured by video technology. Its applications can be located in many areas, such as in commerce (videophone, teleconference, entertainment, film processing, etc.), industry, security and law enforcement. Typically, facial recognition compares a person's image with a stored template, either real-time or off-line for either identification or verification purposes. However, face recognition can also assist in the construction of the profile of an individual's movements, which can be used for security purposes with the risk, however, of invading the individual's privacy. And what is more, the data collected by this procedure could be combined with other personal information (such as the person's ID) to enrich the person's constructed profile and provide a broader and deeper view of the person's private life.

In the Appendix, section C, face recognition and key-stroke dynamics will be further elaborated as examples of biometric profiling.

3.4 Profiling and interoperability

Personalised profiling involves linkability of different data to one and the same subject. As far as this subject can be identified this may enable extensive personalised profiles to be constructed, that may affect the privacy of the data subject. Several tools have been suggested to limit the linkability of data, especially so called identity management systems (IMS), that enable a user to control access to his or her data. We refer to FIDIS deliverable 3.1 for an overview on such systems and the devices designed for such purposes. In this paragraph we briefly investigate the problems related to the interoperability of such IMS, an issue that will be further elaborated in FIDIS deliverable 4.2.

Interoperability of identity management systems is for the moment an idea rather than a reality. Data contained within an information system that serve to identify, authenticate or just verify a person's identity are bound within that system in a number of ways. In technical terms there will be many problems of exchanging data across systems that spring from format issues, protocol issues and issues of technical standards. The many proprietary systems that currently constitute the range of offerings in the IMS field were not designed to be able to share identity information. There are as yet few common standards on identifiers and registries that can be adopted.[56] Some headway is being made in the e-government area in the shape of the Lisbon Agenda and eEurope 2005, but it is early days yet.
Above the technical level, lies the legal and policy level that enshrines checks and balances that are written into operational systems by different legislatures and regulators. In Europe, the right to privacy is set out in Article 8 of the European Convention of Human Rights and

[56] See Annex 1 of FIDIS deliverable 2.3 for some examples. Public Key Infrastructure is one of the few areas where a range of common standards has been developed for identity and authentication, such as X509 V3 and RFC2527, and yet PKI seems to some of us a graveyard for the hopes of inter-domain interoperation.

Fundamental Freedoms and owners and operators of systems that process personal data will have to have regard to data protection principles before releasing key data to third party systems.

On the social and business fronts, and at the application level itself, while there may be some easy wins to be had in the e-government and e-health areas as far as interoperability of identity goes, it is difficult to see the way forward in e-commerce where merchants, card issuers and aquirers are driven by strong competitive urges. We have already seen how bank cards, both credit and debit cards, are used as make-do identity cards on many occasions, and yet users are forced to amass walletfulls of plastic even though the identity data on each card is largely the same for a given consumer.

Some expect that once such barriers to interoperation are overcome, there will be real benefits in being able to share profiles across databases. In an increasingly technological world, profiling seems the only feasible road to making best use of masses of data to hone products and services for specific types of users, consumers, patients. It would be advantageous to be able to narrow down packages of medical or educational benefits to the precise community that has need of it, say for remedial help or for pre-emptive therapy or treatment. But overcoming the barriers will take some effort if PKI experience is anything to go by and – as will be further developed in subsequent deliverables – sharing profiles across databases raises a number security and privacy issues, considering also the data protection framework that for instance prohibits the use of personal data for other purposes than specified at the moment of collection.[57]

[57] See FIDIS deliverable D7.3, the paragraph on legal issues and D7.4, par. 2.4.3. Also workpackage 5 will focus on issues of privacy and security during the second workplan.

4. Purposes and effects of profiling

4.1 Introduction

Technology in itself is neither good nor bad, but its effects are never neutral. This deliverable does not aim at a comprehensive analysis of possible privacy invasions, caused by profiling practices. Subsequent deliverables within this work package will address such issues in more detail. However some attention should be given to anticipated negative impacts. In this section we will first face the major issue of data surveillance raised by Roger Clarke in his 1994 article on dataveillance. After that the risks and dangers of personalised profiling will be discussed. We will conclude this section with a summary of the purpose and effects of profiling.

4.2 Dataveillance

Profiling functions, intentionally or unintentionally, as a sophisticated assessment of risks and opportunities. It aims at discovering, for example, potential terrorists; criminals; insurance risks; new customers; potentially fraudulent employees; promising students; productive employees. In the case of automated profiling these assessments all depend on data surveillance, or dataveillance: 'the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'.[58]

In a pioneering article of 1994, Clark discussed personal and mass dataveillance, in which he summed up the social impact in terms of dangers to individuals and to society.

As to personal dataveillance, he points to

- low data quality decisions;
- lack of subject knowledge of, and consent to, data flows;
- blacklisting and denial of redemption.

As to the dangers *to the individual* of mass dataveillance, he summed up:

- arbitrariness;
- acontextual data merger;
- complexity and incomprehensibility of data;
- witch hunts;
- ex-ante discrimination and guilt prediction;
- selective advertising;
- inversion of the onus of proof;
- covert operations;
- unknown accusations and accusers and
- denial of due process.

As to the dangers *to society* of mass dataveillance he summed up:

[58] Clarke R., 1994, "The Digital Persona and its application to Data Surveillance.", in *The Information Society*, 10 (2), 2.

- prevailing climate of suspicion;
- adversarial relationships;
- focus of law enforcement on easily detectable and provable offences;
- inequitable application of the law;
- decreased respect for the law and law enforcers;
- reduction in the meaningfulness of individual actions;
- reduction in self-reliance and self-determination;
- stultification of originality;
- increased tendency to opt out of the official level of society;
- weakening of society's moral fibre and cohesion;
- destabilisation of the strategic balance of power;
- and repressive potential for a totalitarian government.

One of the points of this rather loose but penetrating enumeration of the social implications of dataveillance, is the fact that tracking and monitoring the behaviour of individuals and groups has an impact beyond just privacy and security. Due process, weakening of social cohesion, destabilisation of checks and balances, total governance are of a different category than supposed trade-offs between privacy and security. In D7.4 (Implications of profiling practices for democracy and rule of law) and in D7.5 (the publication on profiling and its implications for privacy and security) the impact of profiling technologies on established power relationships will be further elaborated through the question **who is actually profiling who**? Profiling makes persons and groups transparent as correlated data subjects. Large organisations, such as the state, transnational commercial enterprise, healthcare institutions and insurance companies) can afford to invest in profiling technologies. This means that while profiling practices make citizens transparent, individual citizens have few means to profile large organisations. It also implies that one of the most important assets of the democratic constitutional state could become part of a trade-off: the idea that the actions of those in power should be transparent, while citizens should be granted a certain opacity in order to enjoy their freedom.

4.3 Implications of personalization, user information and profiling[59]

(Simone van der Hof, TILT)

This section addresses several relevant considerations with respect to personalisation and the use of user information and consumer profiles, i.e. privacy, inclusion and exclusion, and transparency and quality.

4.3.1 Privacy

The other side of implementing more and more sophisticated personal data collection techniques in online personalised service provision is that the risk to the user's privacy increases. Privacy in general is an important issue in online personalisation, as more collected

[59] This chapter is based on the Research report '*Issues of Online Personalization in Commercial and Public Service Delivery*', TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, June 2004.

user information may imply both better (personalised) service provision and privacy intrusion at the same time. Four main privacy issues related to online personalisation can be perceived:

1. A service-provider approach through which requested user information is not strictly related to the delivery and access of a specific service;
2. User-data collection using invisible methods, which use spy technologies, such as cookies, web bugs, etc. to trace, track and search user profiles;
3. Use of personal data for purposes different from those indicated and without the user's previous and/or informed consent;
4. Lack of effective user access to personal data collected, e.g. at web sites.[60]

However, online personalisation applications, such as recommendation systems, do not always need *personally identifiable* information.[61] The only necessary connection between recommendation systems and users is a consistent pseudonym so the user can be recognised when visiting the website. This kind of user protection is not presently implmented on e-commerce sites, where payment and shipping require personal information that can be connected back to the pseudonym of the user. Because of the importance of privacy protection in online personalised service provision, several different privacy safeguards can be identified in relationships between organisations and users, including:[62]

- Notification by the service provider;
- Opt-in[63] (users must give permission before the service provider can use information);
- Opt-out (users can remove their permission once given);
- Limited access (user information is only used for personalisation of web content);
- User customisation (users can adjust the level of personalisation/profiling to their desires);
- Security (information used to personalise is only accessible by the user or by the authorised organisation);
- Security technology (high level of password/encryption technology is used to safeguard user information).

Personalisation may be a threat to privacy because it provides the companies and organisations using personalisation techniques with a powerful instrument for knowing in detail what an individual wants, who he is, whether his conduct or behaviour shows certain characteristics, and so forth. What increases the problems in relation to privacy is first the potential for further use and sometimes abuse of the detailed and rich knowledge on individuals. Connecting and (re)selling data sources has become a highly profitable business and companies often compromise users' privacy for profits. What is more, several bankruptcy cases have shown that databases with personal data and consumer profiles are a highly valuable asset.[64] Companies may actually believe that they have ownership rights in the

[60] Calenda, 2004, p.11.
[61] Riedl, 2004, "Recommender Systems for Personalization". Paper presented at *the International expert meeting 'Issues of Online Personalisation'*, 5 March 2004.
[62] O'Looney, 2002.
[63] Opt-in and opt-out are sometimes used with a different meaning: as a method e.g., how to declare a consent. Opt-in then means, that I actively have to tick a checkbox to select the consent, opt-out means, that I actively have to tick the checkbox to deny the consent declared by default.
[64] See e.g. the discussion and court proceedings on whether the bankrupt US Internet retailer Toysmart could sell the personal details of its former customers to the highest bidder. See: L. Enos, 2001, "Deal afoot to Destroy Toysmart Database", in *E-Commerce Times*, January 10.

personal data compilations because the law itself offers indications for such a position. In addition to protection under the regime of trade secrets, businesses that have invested in the collection and compilation of personal data are granted exclusive rights under the European Directive on database protection. Another indication can be found in section 55 of the UK Data Protection Act, providing for a criminal sanction for stealing personal data from the *data controller* (i.e. not the data subject).
In the meantime, studies have shown that consumers and citizens are very particular about the type of information they are willing to provide in return for personalised content. Also, they have strong feelings regarding personalisation services that share information about them with other companies: the majority feel that a site that shares their information is invading their privacy.[65] In addition, most consumers hardly understand how personalisation technologies actually work and thus have no opportunity to control the dissemination of their personal or behavioural information. Various personalisation services deploy hidden instruments to track and trace users and thus consumers are unaware that their data and preferences are being collected.

As far as the data that are being used for or generated by personalisation services qualify as personal data[66], legal protection may be available under data-protection legislation. The key European legal regime here is Directive 95/46/EC.[67] The Directive stipulates various fair information practices, mentions among others the grounds for justified processing of personal data and accords data subjects with several rights, among which the right to object to the use of his personal data for direct marketing purposes (absolute right to opt-out, art. 14(b)). Although this provision does not restrict in advance the processing of personal data for direct marketing purposes, an individual may apply this provision to control the use of his data.

4.3.2 Inclusion and Exclusion

A consideration closely related to the use of personal data and privacy protection is the inclusion and exclusion of individuals when it comes to certain personalised services. The use of personalization applications will facilitate the widespread monitoring of what people read, view, or listen to. By using personalisation services, their proprietors will potentially have what Philip Agre has referred to as "God's-eye view of the world".[68] To the extent that personalisation applications allow the user to be tracked easily and thoroughly, it is a simple

[65] See e.g. Mably K., 2000, *Privacy vs. Personalization*, Cyber Dialogue Inc.
[66] See for instance the *Durant case* in the United Kingdom. In this case, mr. Durant sought disclosure of information concerning his complaints in order to re-open his case against Barclays Bank and/or to secure an investigation of this bank's conduct. As part of his activities, Durant asked the Financial Services Authority (FSA) to disclose to him information relating to his complaint, basing this request on section 7 of the UK Data Protection Act 1998. The FSA disclosed some of the information requested, but refused to provide other information as well as 'redacted' other pieces of information (in order to protection the rights of third persons who could be identified on the basis of that information). Durant disagreed with the approach taken by the FSA and took the matter to court. *EWCA, Civ 1746, Court of Appeal* (Civil Division), 8th December 2003. To be downloaded at www.courtservice.gov.uk and http://bailii.org/ew/cases/EWCA/Civ/2003/1746.html.
[67] Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of individuals with regard to the processing of personal data and on the free movement of such data, 1995.
[68] Agre P.E., 1999, "The architecture of Identity: embedding Privacy in market Institutions", in 2 *info Comm and Soc'y* ,1 spring.

matter to limit the scope of certain facilities to a tightly controlled group of consumers. For example, personalisation services will facilitate the selected provision of access to certain services only to consumers who live in preferred postcodes, or have certain levels of income. Also, personalisation services seem well suited as means for choosing who will be allowed to view or read a particular work and who will not. But personalisation is not only about inclusion or exclusion of certain services. It will also facilitate price-discrimination – that is, proprietors of services can ask different consumers to pay different prices.

Is this inclusion or exclusion good or bad? It could be argued that inclusion or exclusion is economically useful, because it will do a better job of getting the right information (commercial as well as public-sector information) to the right persons. Without personalisation techniques, organisations must make wasteful investments in distributing information that may not be appreciated by consumers. Thus, techniques that facilitate inclusion and exclusion may be especially useful for accommodating the changing preferences of consumers and citizens. As such, personalisation is a good way to achieve an efficient market. Personalisation further provides an efficient and effective tool with which companies can monitor who is granted access to certain works and who is not. By using personalisation techniques, content-producers obtain control over the uses of a variety of legally protected works and the techniques will allow providers to manage access rights with respect to particular works.[69] The control facilitated by personalisation techniques will increase the copyright owners' ability to uphold and enforce their copyrights.
One might even argue that inclusion and exclusion of access to certain services is essentially nothing new and as such there is nothing bad about it. Today, consumers' and citizens' behaviour is also predetermined by such matters as their attachment to a group, their cultural or social position or predisposition. Personalisation however provides a new dimension in that it may force individuals into constraining, one-dimensional models, based on the criteria set by technology and by those who own and apply the technology. With commercial personalisation services, the myriad of individual differences may be reduced to one or a few consumption categories, on the basis of which their preferences, character, life-style, and so forth are completely determined.
Also from another perspective, the ability of personalisation techniques to diminish preferences, differences and values seems disturbing. For example exclusion of access to and the use of information and copyrighted works (music, books, films) puts the values of free speech and information under pressure. Personalisation may even have wider societal and political consequences, when it shapes the overall movement of information and expression within society. Free citizens are the cornerstones of democratic constitutional societies. In an doomsday scenario, personalisation services could put cultural and social diversity at stake: one political or religious message dominates the whole discourse. When behaviour is manipulated, freedom of self-determination and personal autonomy are limited and societal freedom is eroded, personalisation may have serious consequences.

4.3.3 Transparency and Quality

[69] Personalization may not only be used to provide customers with better value, it may also be deployed to serve the interests of suppliers. Digital rights management systems are an illustrative example. Suppliers of digital information may use security technologies to limit access to their information, works and services to only those who are willing to pay for these. Depending on the specifics of the measures taken, this may limit the free flow of information as well as consumer choice. Moreover, access to digital works like music files may, for instance, be limited to specific devices, such as the user's own individual registered computer.

The issues of privacy and inclusion/exclusion show that the use of personal data will more and more occur within, and be structured by, social, economic and institutionalised settings. It therefore appears crucial that the legal, technical and organisational mechanisms that determine the ways in which personalisation services are developed must be structured along the lines of control and visibility. To illustrate this point in relation to privacy: in order for individuals effectively to protect personal data that are used for personalisation purposes, they should be given the instruments to know and understand how their social and economic identities are constructed and influenced. This brings us to a fourth consideration: transparency and quality.

Transparency and quality reveal themselves in different aspects and on different levels of personalised services; however, these concepts are also correlated to a large extent in the sense that both contribute to each other. First of all, transparency with respect to the personalisation process itself is of importance, including information as to way the personalisation process works, the different configuration options or features that are included in the service. Moreover, the personalised system has to comply with certain user interface requirements to maximise its usability to the (average) user or large user groups. Preferably, users should be able to operate these systems intuitively, meaning they can find their way within the system without too many instructions. The usage of the personalised service – including its security and authentication options – should not be too complicated for users; otherwise users may walk away from the service before having actually tested it. Right from the start, usability should be part of the design process when developing personalised services in order to forestall implementation difficulties in this respect at a later stage.
When the personalised service provides transaction possibilities, users should be informed of the specifics of the transaction process, such as the point where the transaction is concluded, the general and individual prices of the service in order to prevent customer annoyance with respect to price discrimination,[70] general terms and conditions, payment methods, security of transaction and payment processes etc. The information should be presented in such a way that customers are actually, easily and comprehensively notified, although customers generally do not actually have to read the information. This is relevant legally because many laws provide information duties and rules on general terms and conditions that must be observed in order for transactions to be enforceable.
Moreover, the purpose(s) for which personal data and related information (e.g., log-in information, transaction histories, and localisation information) is used within the personalised service or beyond should be transparent to users. Users should also be aware of the way in which their personalised identity is created and used by the personalised service provider (e.g., what methods are used to create identities and in what context(s) are personal data used and viewed). In addition, users should be informed of the way in which personal data can be accessed, reviewed and updated and the security of this process. Furthermore, users should know if and how (e.g., by sending an e-mail to a clearly specified address) they can restrict or object to (commercial) use of their personal and other data. Such information can be provided in a privacy statement or policy on the website of the service provider. Privacy statements should be complete and easy to access and understand. From a quality perspective, it is also important that the security of personal and other data is adequate and that usability of security and more specifically authentication mechanisms is optimised.

[70] For instance, travel companies may want to inform customers of flexible price programmes where bookings become more expensive when demand increases (see, e.g., www.dfdsseaways.co.uk/).

Usability across different personalised services can, for instance, be addressed by implementing what is called single sign-on authentication mechanisms.
Transparency also demands that users can assess the objectivity, quality and reliability of information provided to them through the personalised process. More than one business or organisation may be involved in providing users with a variety of personalised services and information and, particularly, where there is a lock-in situation in which service providers determine the information to be received by individual users, users should be able to trace the origin of information in order to be (better) able to determine the quality, objectivity and reliability of such information.[71]

Quality of personalised service provision requires that user preferences are closely and adequately matched with the contents of the service, e.g. information. For instance, recommender systems that make recommendations that do not reflect user preferences or tastes will be ignored or rejected by users and will ultimately not be viable. Personalisation should provide users with added value by making the right associations as to their needs; otherwise service providers are likely to be left aside or to forfeit goodwill and reputation.
The quality of personalised service provision is, moreover, dependent on the availability of the service. When the service is (frequently) unavailable because of technical breakdowns, users might lose interest or trust in the service. Personalised service providers must also more generally guarantee adequate security in order to prevent fraud and abuse with respect to the personalised service and (personal) data involved. In order for service providers to test the quality and usability of their personalised services, they can ask for user feedback and involve users in service trials.

4.3.4 Authentication and Identification

Many of the considerations surrounding personalisation come back to issues related to authentication and identification. Personalised services may be equipped with authentication mechanisms that can provide verification of content of data or transactions of the connection between data/transactions and identifiers (which identify an individual) or attributes (characteristics associated with the individual)[72] and of the connection between individuals and identifiers. Authentication largely overlaps the identification concept, since it is the process that actually provides verification of claimed identities (is someone who s/he says s/he is?), however, such mechanisms are not restricted to verifying identities or identifiers; in some cases authentication takes place at the system level when hardware or software (e.g. in case of DRM, a computer on which licensed media files are used) is authenticated. Within the concept of authentication, user authentication and communication authentication can be distinguished.[73] In most cases, the personalised service will also involve user authentication (also called authorisation), which grants certain permissions to individuals (e.g. updating personal data) and can be based upon identifiers and attributes. Single sign-on authentication

[71] See generally on the determination of reliability of information on the internet: A. H. Vedder & R.S. Wachbroit, 2003, "Reliability of Information on the Internet: Some distinctions", in *Ethics and Information Technology*, 5, 211-215.
[72] See on these terms: Camp L J., 2003, *Identity in Digital Government, A report of the 2003 Civic Scenario workshop*, Kennedy School of Government, Harvard University, 5.
[73] Jøsang A.,Patton M., 2003, "User face requirements for Authentication of Communication", in *ACM International Conference Proceeding Series, Proceedings of the Fourth Australian user interface conference on User interfaces* 2003, vol 18, Adelaide Australia, 75.

is, for instance, interesting from a personalisation perspective, because it allows the integration of several authentication processes and providing different personalised (web and mobile) services with a one-time authentication. Furthermore, communication authentication concerns the verification of the identity of the origin of information, e.g., messages and websites that is communicated.

The choice for any mechanism with respect to authentication, identification and/or authorisation depends upon the kind of personalised service (e.g., public versus private, open versus closed network environments) that is provided, the kind of personal data (e.g. sensitive or non-sensitive data) that is involved, and, thus, the level of security that is required. Some systems (e.g., a combination of chip cards and biometrics) may be considered more reliable, yet also more expensive than others (e.g., based upon username/password-protection only). A functional approach to authentication and identification would allow determining the most adequate technology for the purposes of the respective service and the functions necessary to achieve these purposes. For instance, national identity cards may require higher security levels than access to personalised websites, because the assets at stake are more important and the risks are greater. Whereas in the first case, biometric technologies are explored and in some instances already used, these technologies are not considered in the second case which mainly uses username/password mechanisms (although, e.g., banking and payment options again require higher security levels). In this respect, it is also important to point out that a system is as secure as its weakest link. Users of personalised services have to be made aware by service providers in a accessible way to be careful with codes and keys, e.g. passwords, and general terms and conditions will likely contain (a) provision(s) on the liability of careless users. For instance, in the case of single sign-on authentication technologies user carelessness would make the system even more vulnerable, since undermining security affects many different services simultaneously.

Authentication and identification are closely connected with the issue of personal data discussed earlier. Since personalisation in online service provision means individualising online services on the basis of user information, which encompasses personal data, behavioural information, location information, and user profiles, it is necessary to link data on the basis of which personalisation will be performed for an individual person. The identity of individuals for personalisation purposes can comprise different attributes, e.g., personal data such as name, address, or e-mail address, which are connected to the individual's preferences, location, behaviour. Identifiers can be personal when attributes are used that are impossible or difficult to change (e.g., date of birth, fingerprints), but identifiers can also be used in such a way to allow pseudonymous (trans)actions by individuals.[74] In the latter case, identifiers are merely retraceable to non-personal identifiers, which are linked to certain attributes. Identifying an individual for the purpose of personalised service provision does not, therefore, necessarily have to mean that the person's real-life identity (e.g., name, address, appearance) is used to provide the services. In a sense, it is sufficient to know that the service is provided to and individualised for the "right" person, i.e. the person to whom particular preferences and features on which personalisation is based "belong", and – if applicable – is paid for (in time). However, databases with personal data and consumers profiles are valuable assets for businesses (e.g., for marketing and market analysis purposes) and governments (e.g., for the purpose of fraud detection, criminal investigations and national security), so the incentive to restrict the use of data that is retraceable to the actual identity is not very strong. In the light of all this, control and ownership with respect to personal data and identities of individuals are, therefore, important and persistent issues in (personalised) online service provision. These

[74] Camp 2003, 5.

aspects can be built into business models, such that individuals (in this case, i.e. users of the personalised service) can manage personal data and identities within the system. As an example, privacy-enhancing technologies, such as P3P,[75] allow users to control what personal data are disclosed and under what identity and/or identifiers a particular service provider knows the user. Although still in their infancy from an operational point of view, much is also expected from identity management systems.[76] These systems provide an infrastructure for the use and storage of personal information and authentication mechanisms. The public sector may play an important role in the administration of these systems, because they themselves generate important tools for identification of individuals (e.g., driver's licenses, passports) that are often used in private sector (e.g. banking) identification and authentication processes as well.[77] Identity-management systems can be based upon pseudonymous identification processes, meaning that personal identifiers are not disclosed in transactions and, thus, personal data may be more effectively protected, depending on the right amount of security provided.
Standardisation and related to that: interoperability is a critical factor for security and authentication across web services, including personalised services. The standardisation organisations OASIS and W3C, for instance, work together on web services security and related issues. But there are many other initiatives that influence or aim at standardisation of authentication technologies (e.g., certification services), such as the International Standards Organisation (ISO/EN), the American National Standards Institute (ANSI/ABA/X9), ITU (X. 509)[78], Liberty Alliance (identity management, including single sign-on).[79]

4.3.5 Conclusion

The development and use of online personalised services raises a number of questions, dilemmas and fundamental issues. Four relevant considerations have been presented in this paper. Other considerations include issues, such as differences between private and public initiatives, organisation and user-controlled personalisation, and security. All in all, online personalisation is a highly complex development where numerous context-specific aims, ambitions, business-models and conditions may determine the actual development and use of online personalisation services.

4.4 Purposes and effects of profiling: good nor bad but never neutral

[75] See http://www.w3.org/P3P/. Critical notes on P3P: EPIC, Pretty Poor Privacy, An Assessment of P3P and Internet Privacy, June 2000, www.epic.org/reports/prettypoorprivacy.html.
[76] In the terminology of FIDIS deliverable 3.1 we should discriminate between account management IMS (defined as type 1) and user controlled management of identifiers (defined as type 3). This section refers specifically to account management IMS.
[77] Camp 2003, 9.
[78] See <www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.509>.
[79] See also: Kuner C. et al, 2000, *An Analysis of International Electronic and Digital Signature Implementation Initiatives, A Study prepared for the Internet Law and Policy Forum (ILPF)*, September, 2000.

4.4.1 Introduction

In this paragraph we aim to provide a summary of the proclaimed purposes and (un)intended effects of profiling, which should allow us to construct some analytical tools for the evaluation of impacts in subsequent deliverables. *Purposes* are explicit objectives, formulated – in this case – by the data controllers that use profiling technologies. Effects are the visible or invisible, intentional or unintentional consequences on – in this case - the data subjects that are profiled. Following Custers,[80] these effects are described in terms of (1) inclusion and exclusion (2) prototyping and stigmatisation; (3) providing information and confrontation with previously unknown risks; (4) targeted servicing, customisation and de-individualisation. These effects go beyond the often discussed trade off between privacy and security; they rather concern a changing socio-technic infrastructure that will impact the sense of self of those that are being profiled, even if they are not aware of this.
Data Protection legislation emphasises that data should only be used for the purpose for which they have been acquired, but more is at stake. Even *if it were possible* to control the use of data for legitimate purposes, this legitimate use will often have effects that were not intended but are hard to avoid. In deliverable 7.4 attention will be given to the (in)effectiveness of data protection legislation in this regard.

4.4.2 Selection - exclusion

Group profiles are constructed to enable selection. Whether this selection concerns potential customers, employees, insurance clients, persons suffering from a specific disease, offenders or terrorists, the aim is to limit the 'group' of subjects that are the focus of the data user's attention. Thus customers can be serviced in a more personal way - employees can be contracted who fit the company's profile, insurance companies can profile the risk of their clients, and so forth. In performing this task profiling also enables exclusion: customers will not be bothered by advertisements they are not interested in, and those who do not fit the profile of an offender or terrorist will be left in peace. In short, selection aims at either risk-assessment enabling risk-management or providing targeted services, including AmI. In a sense profiling thus allows a refined and smooth functioning of both government bureaucracy and market implementations.
However, the effects of this process of exclusion has two drawbacks: (1) selection and exclusion can be either legitimate or illegitimate, which is not the same as legal and illegal, and profiling provides the tools for massively enhanced selection mechanisms for both legitimate and illegitimate exclusions; (2) as group profiles are often non-distributive some people will be excluded on false grounds, a problem that becomes even more pervasive in the case of non-distributed profiles, meaning that not all individuals in the group share all the same characteristics of the profile (see par. 3.2.4). Levi and Wall conclude that profiling technologies will have a profound impact on access to and participation in the European Information Society, as profiles

> 'could possibly be used against individuals without their knowledge, thus shaping their access to facilities, goods and services, also potentially restricting their movement and invading personal space. In fact, this would regulate their access to, and participation in, the European Information Society'.[81]

[80] Custers 2004: 74-78.
[81] Levi and Wall, 2004, 211.

4.4.3 Prototyping – stigmatisation

A group profile functions like a prototype, enabling an organisation to classify individuals as groups or categories. This makes it possible to deal with massive numbers of customers, clients, patients, citizens while also targeting them in a semi-customised manner. It enables detection by comparison with the prototype.
However, as prototypes become public knowledge, they may give rise to stigmatisation of people or groups of people. While the data user may be aware of the non-distributivity and/or polythetic nature of the group, the public image may not incorporate such complexities. Having visited a certain mosque may be one of the correlated data of a profile that promises to detect potential terrorists; this may lead to stigmatisation of all those that visit the mosque.

4.4.4 Information – confrontation

Profiling provides organisations with information that it can use to target specific persons as potential client, customer, patient, offender, terrorist. When the organisation starts interacting with those it takes to be a member of a certain group, this will entail a confrontation. The individual who is faced with the profile may suffer the consequences of finding out things about herself she was not aware of, while for non-distributive groups this confrontation may be based on wrong inference, or communicated in terms of probabilities. A person who thinks of himself as healthy may find out about a disease he (probably) has or will (probably) develop.[82]

4.4.5 Targeted servicing – customisation

To be targeted with only those advertisements one is likely to be interested in, seems an excellent cure for the spam we are presently confronted with. Who would not want to live in a world that recognises our habits, desires, preferences in products and services? The relationship between targeted advertisement and ambient intelligence concerns this possibility to tune a person's environment in the broad sense to her particular – even unconscious – wishes.
However the result of this custom-made environment may be a very limited perception of the world, that can lead to dangerous types of ignorance and social fragmentation.

4.4.6 Individual targeting – de-individualisation

As seems obvious, profiling enables individual, customised targeting. Problems may occur when a profile applies to the group but not to the targeted individual (non-distributivity; polythetic group): false positives as well as false negatives often cannot be avoided and can cause illegitimate exclusion.

[82] For a discussion of the effects of such disclosure in relation to privacy and the criminal law, see Hudson B. 2005, "Secrets of the Self", in *Privacy and the criminal law*, Antwerp Oxford, Intersentia 2005 (to be published).

But, even more interesting perhaps, profiling will produce normalisation processes:

> 'profiles will begin to normalise the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the patterns; the options reinforce the pattern; the cycle begins again'.[83]

On the one hand, those members of the group that do not fit the entire profile, may be normalised into the profile if constantly approached. This could be called de-individualisation. And worse, when individuals do fall within the profile used to target them, this might result in yet another type of de-individualisation. The limited perception referred to above can cause a loss of diversity, not only between individuals, but also within individuals. If self-identity builds on the permanent confrontation with a diversity of perspectives of others, individual targeting may give rise to the construction of groups that are focused solely on their own profiled characteristics.

[83] Lessig, 1999, *Code and other laws of cyberspace*. New York: Basic Books, 154.

5. Fields of application

After analysing the technologies and techniques of profiling, we will now move into a set of examples of profiling *practices*. These will concern marketing, employment, the financial sector, forensics and e-learning.

5.1. Marketing in general

(Ana Canhoto, LSE)

Commercial enterprise has a great interest in knowing what the behaviour of its customers is or is likely to be. Since, considering the scale of commercial enterprise, it is not always possible for organisations to know each customer individually, they may seek indirect methods to learn about their customers, for instance by aggregating 'records' of transactions. The point is that retailers, for instance, do not want only to understand the behaviour of individual customers, but above all to be able to generalise from observed behaviour in order to make predictions about the behaviour of specific types of customers – that is, organisations want to develop 'community knowledge'.[84]

With this knowledge, the organisation can make informed strategic decisions. For instance, it can organise itself in order to respond in a specific way to exhibited behaviour. If a supermarket identifies the top 20 items bought by a key group of its users – e.g., sandwich-snackers – and stocks the shelves adjacent to sandwich sections accordingly, it can push up sales by this group of users.[85] An enterprise can also use the knowledge about its users' current or expected behaviour to encourage or reward actions that are profitable for the organisation: the objective underlying the introduction of a loyalty card by UK supermarket Tesco.[86] Alternatively, a firm may wish to discourage certain types of behaviour: if it costs more to acquire a new customer than to hold on to an existing one,[87] organisations will take action to increase retention of certain customers. They will try to reduce attrition or churn among certain groups of customers: Chase Manhattan bank decided to reduce the required minimum balance in customers' checking accounts, when it realised that this was a key factor in the choice of banks, for a key segment of Chase Manhattan's customers.[88]

5.1.1 Customer Loyalty Programs

(Martin Meints, ICPP)

Customer loyalty programs became very popular in the last five years in Germany. To gain the loyalty of a customer a certain amount of discount is granted. We observe two types of customer loyalty programs on the German market:

[84] Peppers and Rogers, 1999, *Enterprise one to one: tools for cempeting in the interactive age*. New York, Currency publishing Company.
[85] RetailWeek 2003, "Solutions CRM: Profile shopping.", in *Retail Week*, 22.
[86] Humby et al. 2003.
[87] Peppers and Rogers, 1999.
[88] Fabris P., 1998, "Advanced navigation.", in *CIO Magazine*, 50 - 55.

- Two party relationship programs, where we have a direct contract between customer and vendor
- Three party relationship programs, where we have a more complicated relationship between customer, vendor and system operator granting the discount.

Figure 4 describes the three party relationship:

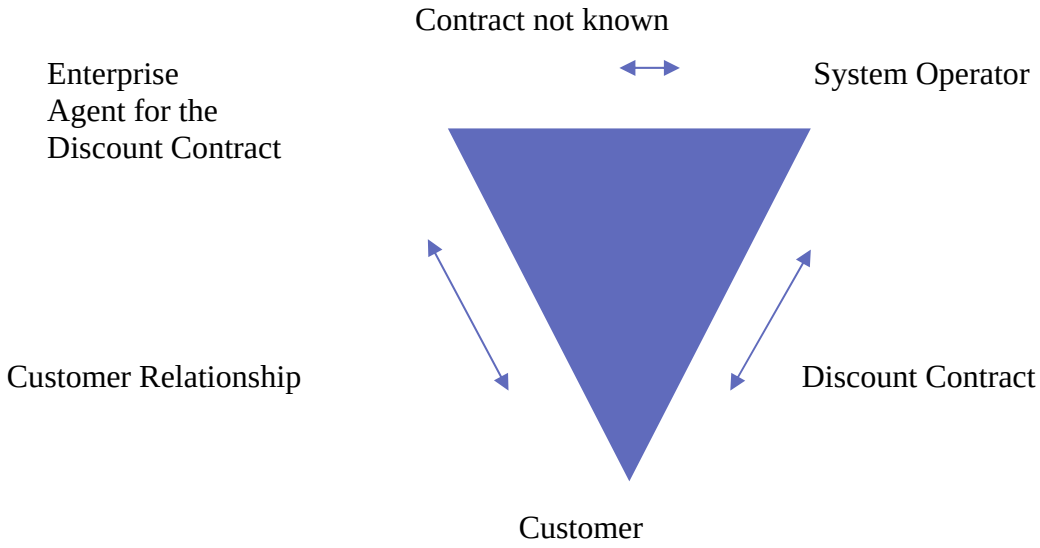


Figure 4: Three party relationship

In most cases in addition to the data needed for discount purposes additional personal data is being collected. In many cases this is e.g.:

- Date of birth
- Several contact addresses (telephone numbers, e-mail etc.)
- Which goods where purchased when and where
- Information on personal circumstances of life (e.g. family status, number of children, income etc.)

These data are mainly used for market research and advertising purposes using profiling techniques. In a study[89] ordered by the "Bundesverband der Verbraucherzentralen e.V." and carried out by ICPP in December 2003, 16 customer loyalty programs were investigated. Against the benchmark of the German Federal Data Protection Act (BDSG) numerous major and minor weaknesses and offences were found. A central weakness of all investigated programs is that because of trade secrecy, the place and time of storage of the data, the way and the purpose of processing was not described sufficiently. On the grounds of insufficient information, a declaration of consent - which has to be based on a free will - is legally not effective.

[89] See http://www.datenschutzzentrum.de/wirtschaft/kundbisy.htm

See the Appendix, section B, for further elaboration of the legal implications.

5.2 Employment[90]

(Martin Meints, ICPP)

German supermarkets use profiling to determine unusual cash flow often caused by embezzlement by cashiers. They analyse cash refund transactions especially. There are some well known techniques for taking money out of a cash till fraudulently. One example is using false certificates for bottle deposits with usually small amounts of money. In the profiles cashiers using this method can be determined by a higher rate of refund transactions than average. Further investigation is necessary, but can be carried out in a targeted fashion. In addition, data mining is used to generate insight on fraudulent techniques as yet unknown.
A retailer chain from Switzerland claims to have caught 50 of their cashiers fraudulently taking money from the cash till. By using profiling techniques, they claim to have saved 200.000 €. For Germany no data are available.

5.3 Financial Sector

5.3.1 Anti-money laundering profiling

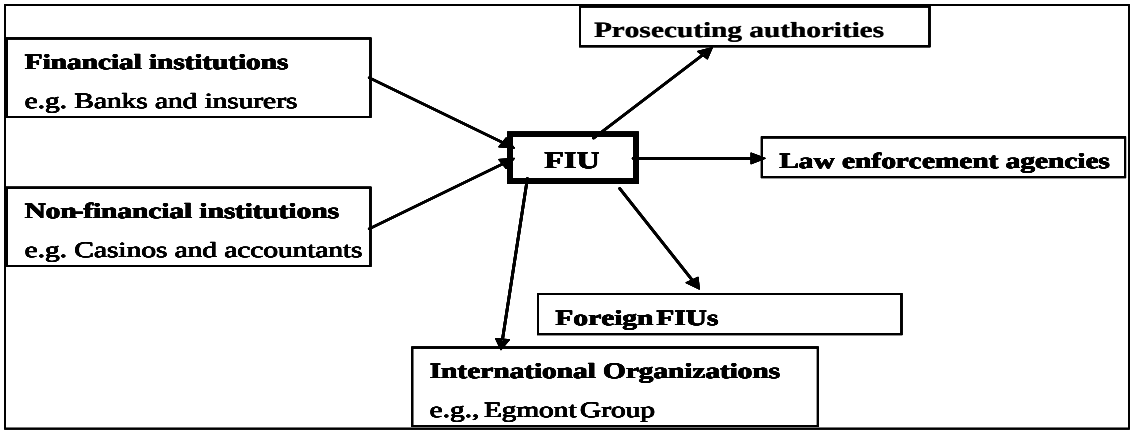
(LSE, Ana Canhoto)

Anti Money Laundering (AML) regulation has gradually increased in scope and depth in recent years and all major jurisdictions require businesses, located within their boundaries, to play their part in its prevention and detection. As well as banking and finance, other sectors, such as accountancy and legal services are required to establish procedures, which facilitate the reporting of suspicious activity to the relevant law enforcement authorities. A number of spectacular fines in such countries as the USA, the UK and Spain, within the last year, have emphasised the degree to which financial regulators are concerned about this particular crime. More recently, terrorist outrages have concentrated attention on how the financial system, in particular, might detect and prevent the funding of such criminal activities.

A critical tool in AML is the Suspicious Activity Report (SAR). A regulated institution must prepare a SAR when it suspects that a customer (either an individual or an organisation) is trying to process financial proceeds from criminal activities through that institution. This report is channelled to the appropriate Financial Intelligence Unit (FIU), a specialised governmental agency in every state created with the purpose of identifying and reducing money laundering activity. The FIU analyses the reports received and forwards a number of cases for further investigation and eventually, prosecution by the competent law enforcement agencies. This process is illustrated in figure 5.

[90] WDR, Quarks & Co, broadcast from 22nd of June 2004, Cologne 2004; see http://www.quarks.de/dyn/18298.phtml

Figure 5: Basic[91] model of FIU's role in AML



The use of automated monitoring systems is often seen as a powerful ally in detecting suspicious activity, justified by the wholesale increase in size of the typical transactional database, and by a desire to keep compliance costs under control. These systems usually consist of powerful algorithms that sweep through the records stored in transaction databases looking for those patterns of financial behaviour that deviate from the norm. Such algorithms tend to be based on rationalist approaches that assume that human behaviour can be modelled through positivist relations of transaction data. This implies that there is a fixed, immutable entity-structure and that behaviour is bivalent (i.e., can only be considered right or wrong, true or false, etc…). Such models take semantics as given and do not question the fundamental notions of individuality and identity. As a result, on top of heavy investments in technology, the organisations intervening in anti-money laundering still need to employ large numbers of people to eliminate the false positives from the large number of patterns of transactions that are deemed to be unusual after automated analysis. Such inefficiency hinders the performance of the system and, ultimately, contributes to the ability of money launderers to operate undiscovered.

An additional problem of the use of automated monitoring tools in AML, is that the profiles typically rely on tried and tested money laundering typologies. They usually lag behind the ever-changing, and increasingly complex, methods of laundering money. Additionally, organisations tend to focus on the "usual suspects" and give more attention to anomalous activity coming from individuals with a given demographic profile – this is well illustrated by the case of a personal assistant who stole nearly £4.5m over two years from her bosses at Goldman Sachs by forging signatures on cheques – the personal assistant's anomalous banking behaviour had been flagged several times by financial institutions but the case took a long time to be investigated because she belonged to a socio-demographic group rarely involved in money laundering activities.[92]

[91] This is a simplified version of the process of reporting suspicious money laundering. In practice, the FIU also provides input (queries and information) to the reporting institutions, and it receives input from the other institutions identified in the figure.
[92] This case is analysed in *D2.2. Cases, stories and scenarios*, WP 2, FIDIS Project 2005.

5.3.2 Fraud prevention

(Martin Meints, ICPP)

In Germany profiling techniques are used to minimise the risk of granting a credit by a bank. For that purpose German banks and other financial service providers (e.g. insurance companies) have founded the so called "Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)". With the consent of customers, required by the Federal Data Protection Act (BDSG), the so called "SCHUFA-Klausel", banks and financial service providers transfer data about all bank accounts and the financial behaviour of German citizen to the "SCHUFA". German citizen cannot avoid the "SCHUFA-Klausel"; no respectable bank or financial service provider offers services to customers who do not consent to the "SCHUFA-Klausel".[93]

The general financial behaviour of reference groups is analysed with massive data volumes about customers of various banks. The profiling gives a so-called scoring value developed from those reference group profiles. Its value lies between 0 points and 1000 points. This value is assumed to express the risk based on past personal behaviour. It is therefore used by banks together with other "SCHUFA"-information (e.g. special person related information like account information) to determine the risk of defaulting on credit and conditions under which someone can obtain credit (e.g. interest rate, maximum amount of credit etc.). The scoring value is used as one instrument to meet the Basel II-requirements by the banks.[94]

The method of calculation of those scoring values is not published in its entirety (trade secrecy) and the customer of a bank cannot obtain all the information, including the scoring value, that is stored at the "SCHUFA". In addition this SCHUFA scoring value is claimed to violate the Federal German Data Protection Act (BDSG), especially § 6a BDSG.[95] There is a risk in this method of excluding people from financial activity (exclusion) for no obvious reason. This can be caused, for example, by mistaken assignment to a profile with a low scoring value. This in turn can lead to severe consequences such as not being able to open any bank account at all.

5.4 Forensics

(NFI, Zeno Geradts)

5.4.1 Current situation

In forensic science, currently there exist many different databases that can be used to link cases and suspects :

- Firearm : Cartridge cases, bullets
- Fingerprint
- DNA
- Face
- Tool mark (e.g. screwdriver)
- Shoe print

[93] http://www.datenschutzzentrum.de/faq/schufa.htm

[94] Petri Dr. B.T., 2003, "Sind Scoringwerte rechtswidrig?", in *Datenschutz und Datensicherheit* (27), 631 – 636, Wiesbaden.

[95] Möller J. and Florax B.-J., 2002, "Kreditwirtschafliche Scoringverfahren", in *Multimedia und recht*, (12), 806 – 811.

- Handwriting
- Paint and glass
- Voice

In practice there is experience with combining those databases for combining evidence; however searching between databases is often not easy, since the data, the data models, and entry of data may be at odds with one another.

If we consider digital evidence on the internet, for example in internet hacking cases, one needs to examine logs and other files. Here too some cases have been submitted. A question that always arises with these cases is who was really behind the keyboard at a given moment. If biometric devices are used more (and spoofing of biometrics is not used), it is also possible to follow persons. The logs of the antenna's mobile service provider can also be used to examine the position of a person at any given time.

5.4.2 Expectation

We expect that in future databases and the data models will become more standardised, in such a way that they can be combined with other databases such as :

- Face and 3D images and other biometrics of everyone (ear, iris, fingerprints, DNA etc)
- Banking and insurance transactions : money laundering
- Telecommunication traffic and interception (location GSM and internet)
- All computer actions and storage
- Records of toll ports / public transportation
- Board computer in private transportation (cars etc.)
- GPS
- Customer loyalty programs (air miles etc.)
- Surveillance cameras (also satellite images)
- Digital traces in domestic applications (e.g. coffee maker, microwave, heater)
- Ambient intelligence

Examination and combination of data is currently possible in Dutch law if there is a severe crime involved; a court order is needed (depending on the kind of information).

For the passport for example it will be possible to track someone if the ICAO-standard is implemented without any protection. The passport will have a wireless chip in it, and information concerning face and fingerprint can be extracted remotely. Currently in trials in the Netherlands, protection is being developed in such a way that one needs more information concerning the machine-readable zone of the passport. However if countries do implement these systems without any protection, then the possibility exists that information concerning the passport they carry can be extracted remotely.

5.4.3 Discussion

The question arises whether the kind of evidence with the combination of many different databases, such as surveillance systems with non-structured data, is feasible. Also the amount

of data that is collected grows very rapidly, and the question is whether it is feasible to store this data in an appropriate way.

Furthermore, it is expected that there will be more false positives when combining different databases. If a 'cold' hit is found in the database, which means that there was no prior information that a certain suspect would be involved in the case, false positives are possible. For example, if DNA were to be collected from all citizens of the world, and the search were against this database, then with current methods around 6 suspects would be found, perhaps more, as family relationships are not accounted for.

The questions also arises whether the databases are inputted correctly. In most databases data entry errors exist. For this reason the standardisation of databases is required before the databases are searched through routinely. In the end, the evidence for some cases might be stronger, since the fact that other data was not found before can also itself be used in certain cases as evidence. How far society wants to go with profiling in (forensic) databases, depends of course on current legislation.

See the Appendix, section A, for further elaboration on forensic use of RFID and biometric profiling.

5.5 E-learning

(Thierry Nabeth, INSEAD)

5.5.1 Personalised profiling and e-Learning

Profiling represents a central element of the **traditional world of education**: student performance is very systematically accessed via series of exams or other similar processes, which aim at evaluating the level of proficiency of a student in a given domain, but also at validating some capabilities that are to be certified officially by a diploma. The discipline of Education (and learning) has also a long tradition of investigating the less tangible factors (such as motivation, desires, learning style, previous experience, or personality) that intervene in student learning performance, and or the likelihood of completing well a particular task. In the latter case, different theories and tools (personality tests or intelligence tests) have been developed in order to "profile" the student, and in particular to identify the characteristics of this students and to assess his ability to "fit" a particular job (for instance the characteristics of a student may make him unable to fulfil a job in which he would have to use manual skills, long period of sustain his attention, and manage a lot of stress).

In the **E-Learning world**, the situation appears however to be significantly different in the way that profiling is considered. Profiling in e-learning systems appears mainly principally under two following forms:

- Student modelling.

Adaptive learning systems.

5.5.2 Student modelling & profiling in LMS (Learning Management Systems)

We have previously seen how user modelling, student modelling in this case, represents an essential element of adaptive systems. However, student modelling also represent on its own a critical component that intervene also in the design of the more traditional LMS (Learning Management Systems).
LMS can be defined as electronic learning environments providing support to the online management, delivery and tracking of learning. Practically, a LMS will give a group of educators the possibility to deliver to students a series of on line courses, to test and to track the achievement of the students, and more generally to manage the educational process.
The student profile represents one of the important components of the LMS, since it is used to centralise all the information that is associated to a particular student, such as his name, coordinates, but also the information that are related to his educational background (such as his different diploma), and the advancement of his work (what are his different assignments, how well did he performed in his previous assignments, etc.). Interestingly, the representation of the student model has been the object of a standardisation, which aimed at facilitating the development of standard component, but also to facilitate the interoperability between e-learning systems. More concretely, the IMS / LIP (Learner Information Package), defines the student according to the following eleven dimensions[96]: accessibility, activity, affiliation, competency, goal, identification, interest, QCL (certifications), relationship (relationship between the attributes), security key and transcript (performance of the learner).
To our knowledge, profiling in LMS is currently not particularly sophisticated, and relies on two ideas that will still need to be fully operationalised in the future: (1) Universal student management & interoperability: LMS are able to manage more centrally a student model and to interoperate with other systems. The profile of the student will increasingly be more complete and will result from a better capture of the actions and the achievements of the students, and from the connections to other databases (for instance between schools) that will be achieved more easily because of increased interoperability. (2) Better global exploitation of the students' information as a whole in order to identify and to exploit some trends in the student population.

5.5.3 Intelligent e-learning applications

User adaptive (or personalised) systems, such as intelligent tutoring systems, represent another field of e-learning application in which user profiling plays an important role.
We have already described in this document how the user model (and the profiling of this information) represents a major component for the design of adaptive applications.
If adaptivity in e-learning applications do not differ fundamentally from adaptivity in other categories of application, it is important to mention that research on adaptive e-learning application has attracted a considerable attention from the research community.[97] Indeed,

[96] For more information about the IMS / LIP standard, the reader is invited to read the document IMS (2001), or the Fidis deliverable "D2.3 models", which provides a summarised version of this model.
[97] Karampiperis and Sampson, 2004, "Adaptive Learning Object Selection in Intelligent Learning Systems", in *Journal of Interactive Learning research, Special issue on Computational Intelligence in Web-Based Education*, vol 15 (4), 389 – 409, nov 2004. Dolog and Nejdl, 2003; "Personalisation in Elena: how to cope with personalization in distributed eLearning Networks", in *Proceedings of International conference on Worldwide Coherent workforce, Satisfied Users – new Services For Scientific Information*, Oldenburg, Germany september 2003. De Croock et al., 2002, "ADAPT-IT: Instructional Design (ID) tools for training design and evaluation.

adaptive systems promise to revolutionise education by providing each student with a personal tutor, addressing therefore the problems of the overcrowded classroom, and of the students that do not get enough attention from the teaching staff.

Educational Technology", in *Research and development*, 50(4), 47 – 58. Brusilovsky P., 1999, "Adaptive and Intelligent technologies for Web-Based Education", in Rollinger and Peylo (eds), *Kunstliche Intelligenz, Special Issue on Intelligent Systems and Teleteaching.*

6. Issues for further clarification

6.1 Commodification of information

One of the most obvious effects of datamining is the emerging trend of viewing information as a product in itself, as data and profiles often have a high market value. Companies that collect valuable data are in a position to become information brokers by reselling the data collected as reports – for instance, reports on television viewing habits.[98] It seems to be the case that, as the process of knowledge discovery (or data mining in a broad sense) is highly automated it becomes more and more dependent on computer technology. As the input to this process is formed by a collection of data objects organised in a database, while the output will be "*pieces* of knowledge *dug* from the database",[99] the temptation to see knowledge as a commodity grows. This also impacts ideas on the protection of (informational) privacy.[100] Interestingly, in the legal field we see different approaches as regards these issues: while the US seems to allow commodification to rule issues of privacy, Europe seems to rather think in terms of personality rights and liberties.[101]

The commodification of information raises many questions.[102] For one, it challenges traditional ideas about property, ownership, privacy and security:

- other than tangible stuff, information can be at many places at the same time;
- limiting access to information can be against the public interest;
- buying and selling information can be against the private interest of a particular person, ànd against privacy as a public interest;
- informational self-determination may be limited due to difficulties to trace the data-controller

In upcoming deliverables the legal and ethical issues of such commodification will have to be adressed, as this concerns the legal and economic infrastructure of our information society. This infrastructure will, in the end, decide who has access to which information and who can or can not employ the knowledge that is generated.

6.2 Privacy, security, trust, usability and equality

As indicated from the start, this deliverable does not focus extensively on privacy, security, trust, usability and equality. It aims to deliver a concise analysis of profiling as technique, technology and practice, with special attention to the effects it produces both intentionally and unintentionally. In later deliverables the issues of privacy and security; trust and usability; and equality, will be explored.

---

[98] Berry and Linoff 1997.
[99] Bruha I., 2000.
[100] Prins J.E.J., 2004, "The Propertization of Personal Data and Identities", in *Electronic Journal of Comparative Law*, 8,3.
[101] Agre P.E. and Rotenberg M., 2001, *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts: MITT.
[102] For the term commodification see: Prins, J.E.J. (2004), "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, 8.3. <www.ejcl.org>.

- D7.3 will focus on the role of profiling in Ambient intelligence with more explicit attention for privacy and security and the legal framework around profiling.
- D7.4 will focus on the implications of profiling on democracy and rule of law, integrating issues such as privacy and security but also posing the question: who is profiling who. This touches on issues such as equality (discrimination; dissymmetry) and transparency (invisibility of data processing; transparency of those that are profiled). The legal framework will be discussed in respect of building in checks and balances: facilitating opacity of individuals and transparency of data controllers/users.
- D7.5 will allow researchers from different institutes and disciplines to integrate their knowledge at the academic level, aiming at a high-profile publication on the subject, including technological, legal and social perspectives.
- D7.7 will shift the focus to profiling of offline behaviour and substance by means of rf-id and biometrics in AmI environments.

Appendix

A Forensic Profiling in the field of RFID and Biometrics

(Zeno Geradts, NFI)

A.1 RFID technologies

Radio Frequency Identification (RFID) tags are expected to be used increasinly in products at retailers and in travel identity cards. Currently the Wal-Mart in the USA, Metro in Germany and Tesco in the United Kingdom are requiring RFID-tags on the products. Also the Department of Defense in the United States is requiring tags on products from suppliers. Tracking and tracing are the most important reasons for this requirement and in the war in Iraq this was convenient for the transportation of equipment and tracking. Losing or misplacing products, parts or equipment will result in higher costs.

It is expected that in 2008 more than 20 billon RFID-tags are used.[103] Most of them will use the EPC-standard (Electronic Product Code). For reading those tags it is expected that 100.000 EPC-readers will be sold. It is expected that the tags will drop to several euro-cents per tag.

RFID-technology

A RFID-system consists of different components :

- One or more tags (transponders), consist of a microchip and an antenna
- One or more reader and writers including the RF-modules
- Application software connected to the reader/writer

RFID-tags exist in two forms :

- Active (with a power supply)
- Passive (need power from the signal of the reader)

Active RFID-tags are somewhat larger and more expensive, however they can be used at a greater distance. Passive tags can be used in consumer articles and are cheap. They can also be used in labels.

Furthermore, RFID-tags can be read-only and read-write. The read-write tags are used with an encrypted identification number, where only authorised users can change the information.

The retailers are requiring their suppliers, to use the Electronic Product Code (EPC). This standard has been developed by MIT's Auto-ID center, and is managed by EPCglobal, which is a non-profit joint venture between two organisations: EAN (European Article Numbering) International and the Uniform Code Council. The second generation of UHF EPC-standard has been ratified in December 2004. In January 2005 this standard is submitted to ISO.

For RFID, the ISO standards concern :

- Technology ISO 18000

[103] TWA Nieuws, 43-2 www.twanetwerk.nl.

- Data content (ISO 15418, 15434, 15459, 24721, 15961 and 15962)
- Device conformance test and performance (ISO 18046 and 18047)
- Application Standards (ISO 10374, 18185, 11785)

A.1.1 Security of RFID

In July an article in Forbes presented a hacker's guide to RFID.[104] It would be easy to hack a tag, and change price information on a tag. There were also privacy concerns for the consumers. The cheap tags are just readable tags, and they cannot be altered easily. Also when using a write-once tag, often the price is not included in the product, since they use a serial number for the product. It is however an aspect that needs attention.

Example of RFID-labels from http://www.bluhmsysteme.com/rfid-etiketten.htm

A.1.2 Forensic aspects of RFID and profiling

RFID tags can be used also in forensic science to track a person using on the RFID-tags one carries in products. For example: there is a unique RFID-tag number on a packet of cigarettes and a person steals this packet in Amsterdam from a store. Theoretically it is possible that within European databases of stolen goods, the person can be arrested in Brussels when they scan the RFID-tags of this person. The same applies, of course, to the previously mentioned passport with a chip. The key elements are RFIDs, in combination with databases and if stored properly, it can be used as evidence.

The use of standards makes it also easier for forensic science to develop tools to read the information in a proper forensic way.

A.1.3 RFID and privacy

Also EPC is worried about privacy aspects. For this reason they have implemented certain privacy guidelines:[105]

[104] http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html
[105] http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

Guidelines

1. Consumer Notice

Consumers will be given clear notice of the presence of EPC on products or their packaging. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

2. Consumer Choice

Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice.

3. Consumer Education

Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarise consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines.

4. Record Use, Retention and Security

The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use.

If they are properly used, and if the consumer can discard the EPC-tag easily from a product, this means that the example above with the package of cigarettes is not feasible, if the thief discards the RFID-tag.

A.2 Biometric Devices

The market of biometric devices is expanding rapidly, since it is convenient to use, and users can not forget their biometric properties. Some examples of biometric properties which are used in commercial systems:

- Face

- Fingerprint
- Handscanner
- Iris
- Voice
- Handwriting

In forensic laboratories also other means of biometric measurement are used for comparison:

- DNA
- Ear prints
- Lip prints

In many countries, DNA databases are built of persons who committed a serious crime and DNA found at the scene of crime, as well as, to determine possible contamination of evidence, databases of employees of the forensic science laboratories. The laws in many countries forbid use of these data for purposes other then that for which they are meant: for serious crimes, by court order or if specified by the law.

In a world where no privacy laws exist, theoretically it would be possible to collect databases of fingerprints, iris scans, voice, hand writing and face. These databases can be combined with one another. If the databases are structured correctly, and there are no errors in names or in the links made, these databases can be used to search by profiling for a person or a group of persons, perhaps leading to more crimes might be solved, and perhaps stronger evidence.

One problem is however that the one-to-many comparison, for example with faces, returns a high error rate. A good example is given at http://www.frvt.org/FERET/default.htm where a methodology has been used to examine different commercial packages and to compare them with a standard database. If we look at the results of FRVT 2002, it can be concluded that on a database of 37,437 individuals which are read in a standardised form, at first 80% are identified, and hence 20% are identified incorrectly. After one year the identification rate drops by 5%. If we had databases of millions of persons, there would be many false hits, as shown in the results :

- 71.5 % true accept rate @ 0.01 % false accept rate
- 90.3 % true accept rate @ 1.0 % false accept rate

Another test by NIST on fingerprints, gives better results http://fpvte.nist.gov/ . We can see here by using single good quality fingerprints

- 99.4 true accept rate @ 0.01 % false accept rate
- 99.9 true accept rate @ 1.0 % false accept rate

When multiple fingerprints and face images (or even 3D-images) become available, the situation improves. In these systems, poor quality images are not used. In practice when filling databases with real images these will also be included, and results will deteriorate.

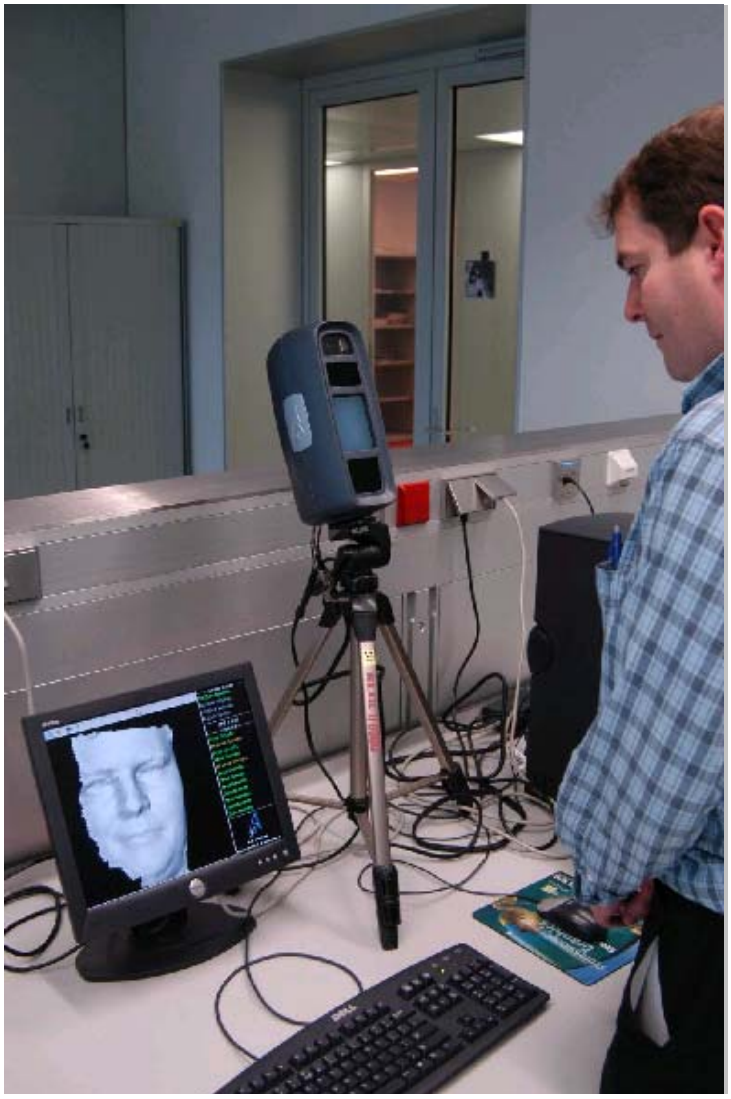


Figure 6: Example of mass market 3D-face scanner

B. Legal grounds for customer loyalty programs

(Barbara Körffer, Martin Meints, ICPP)

Based on European legislation,[106] the German Federal Data Protection Act (BDSG) has several sections relating to customer loyalty programs. They are elaborated in detail in the study "Kundenbindungssysteme und Datenschutz", commissioned by the "Verbraucherzentrale Bundesverband e.V. (vzbv)" and carried out by ICPP in December 2003.[107]

Usually customer loyalty programs employ customer account cards. From a data protection perspective, the contract between the customer and either the discount-granting company directly or an operator of the account card system can be interpreted as two distinct parts:

1. discount related part: rewarding customers' loyalty by granting discounts
2. collection of additional data: collecting and processing additional personal data for different purposes, such as:
    a. advertising
    b. market research

For the first part of the contract, Article 28 paragraph 1 no. 1 BDSG is relevant. This paragraph limits the use of personal data to the purpose of the discount related part of the contract. In detail, this means that the contract partner of the customer only is allowed to store and process the following data:

- Name
- Address
- Year of birth
- One further address information (phone, email etc.)
- Time and place of card deployment
- Price of purchased goods / services and discount amount
- Data related to the purchased goods only if they are necessary for computation of the discount amount.

The second part of the contract for collection of additional data can be based on the legal foundation of Article 28 paragraph 1 no. 2 BDSG. This regulation allows the use of data as far as overriding legitimate interests of the customer are not concerned. This includes the name, year of birth and address.
For further data a written consent of the customer is required. Requirements for the consent are regulated in Article 4a BDSG.

In addition, for data processing in general the following legal regulations apply:

- Article 4 paragraph 3 (active information of the customer)

[106] Directive 95/46/EC, 24th October 1995, on the Protection of Individuals with regard to the Processing of personal Data and on the free Movement of such Data.
[107] See http://www.datenschutzzentrum.de/wirtschaft/kundbisy.htm

- Article 34 (provision of information to the customer)
- Article 35 paragraph 1 (right to get data corrected)
- Article 35 paragraph 2 (right to get data deleted)

Consequences especially of Article 4a BDSG are that the customer opting for the further use of his/her personal data has to know details and consequences of the collection and processing of the data. In addition, the decision is not considered to be freely entered into if the participation in the loyalty program depends on an agreement for collection and processing of additional personal data. To gain a legally effective declaration of consent, the customer has to be informed about the following facts:

- Who is responsible for the data and the data processing?
- Which categories of data will be processed?
- For what purpose are they processed?
- How is the processing done (phases and data flows)?
- Whom are data transferred to?
- Information on voluntary decision of consent and the consequences of a refusal
- Information on the ability to revoke the consent at any time

In the aforementioned study, 16 federal and several regional customer loyalty programs were investigated for their compliance with the BDSG. All programs investigated showed defects, some minor, some major.
Examples include:

- More data than necessary for correct implementation of the discount were collected without consent of the customer
- Participation in the discount program depended on consent to further usage of personal data: no freedom of choice given
- The exclusion of personal data from the declaration of consent was not implemented in a privacy-compliant way. An opt-in or opt-out possibility was not implemented in the contract; the customer had to cancel that part of the contract he didn't want to agree with.
- In rare cases, conditions of entry and privacy policies were sent to the customer only after getting his/her consent – this means no consent at all because the customers could not know the conditions in advance
- Information was missing that consent is voluntary
- Consequences of a refusal of the declaration of consent were not pointed out
- Planned processing of personal data was not sufficiently described – therefore declaration of consent was not completely based on a free decision

In some cases, such defects were remedied by the operators of the loyalty programs.

For the LN-Card, a customer loyalty program for the readers of a local newspaper, the "Lübecker Nachrichten" (LN), the privacy seal of "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein" (ICPP) was granted.[108]

[108] See http://www.datenschutzzentrum.de/guetesiegel/register.htm

C. Biometrics profiling

(Angelos Yannopoulos and Vasiliki Andronikou, ICCS)

C.1 Physical Biometrics Profiling : Face Recognition

Face recognition forms part of the general object recognition problem that seeks to differentiate objects which only vary in minor ways from each other and is one of the most challenging computer vision problems. Recognition is achieved through the analysis of certain facial features, such as the upper sections of the eye sockets, or the area around the cheekbones, and their comparison to stored templates. This technology works for both verification and identification. The design, the development and the performance of such a system face many difficulties owing to vulnerability to variations in the operating environment, complex or moving backgrounds, complex foregrounds, occlusion, and in general where the complexity of the system increases in view of real-time operation. The performance of the system can further degrade because of the age of the template. As in every biometric system, in a face recognition system identification of individuals is possible only for those individuals whose images have been enrolled into the system's database. Thus, the first step for the construction of an individual's profile is the enrolment of the person's image (of reasonable quality) into the system's watch list.

A challenging fact which spurs efforts to overcome the technological limitations of such a system and yet raises great concern regarding privacy is that, generally and compared with other biometrics, there is no reasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public, such as facial features or voice. Nevertheless, the people entering a public space where video surveillance is used should be notified, so that they can make an informed choice of whether or not to subject themselves to surveillance. This is the case because the professional analysis of stored facial images or other biometrics (by means of profiling techniques) can reveal certain diseases that a layman in face to face contact could not have recognised.

A simple scenario of the use of such a system could be the tracking of a wanted person by the authorities through the individual's activities; as people are go about their daily tasks, surveillance cameras could be capturing their faces and transmitting these images in order to be compared to the watch list, that contains the people for whom the authorities have issued an arrest warrant. Such a system would be able to track an individual's movements, actions and transactions in real-time and combine this information with respective data from the person's past, stored in databases to which there is access.

When the Super Bowl XXXV was about to take place in 2001, fears of a terrorist attack led to the need for increased security measures. The final system used relied on facial recognition, which involved surveillance cameras continuously scanning spectators' faces and capturing images of their faces processed in real-time in order to produce a "faceprint" (set of measurements of facial features). This "faceprint" was then compared against each record in a computerised database of well-known criminals and suspects of terrorism and was classified as either matching or differing from each of them. An alert to the police was to be triggered in case of a match.

Nevertheless this "super surveillance" could be very easily abused. For instance, what if the watch list does not only include people wanted by the authorities. Should the authorities be allowed to add to the watch list a particular individual simply to track their moves or is the approval of a judge required? Another scenario involves the capturing of images of all the faces included in the videos captured by the cameras, the only technical restriction of which being the required volume of storage. This information could be then maintained for future use, as a record for the particular person. Moreover, increased police attention on previously convicted persons identified in public areas by the system would make their rehabilitation harder.

Questions arise such as who should be entered into the watch list, whose approval (and in which cases) is essential for such an entry, how long are these records maintained, whether they should be accompanied by information, such as when the entrance of each person's image took place and at whose request. It is thus obvious that abuse can be eliminated though official procedure to some extent by establishing legal measures controlling the administration, management, use and maintenance of such systems, whereas citizen committees and public boards could monitor government use of the system. However, existing measures taken to handle related privacy issues emerging from other types of surveillance technology could be taken into account.

C.2 Behavioural Biometrics Profiling: Keystroke Dynamics

We will now briefly address the issue of whether and how behavioural biometrics can be exploited in a malicious manner.

A simple example of a behavioural biometric that can be abused in a way that is extremely difficult to track is the measurement of keystroke dynamics. The classic application is to protect passwords: a password system logs the timing taken by a user to enter his/her password, as well as the password itself, and then uses a pattern recognition system to classify a newly entered password as matching or differing from the logged timing patterns. Since computer users constantly use the keyboard, any application that can reliably measure the timing of a user's typing can also try to perform identification or verification of the user.

Given the basic idea, it is quite easy to engage in various flights of fantasy that involve behavioural biometric systems violating the privacy of computer users by inexorably tracking their identity no matter how they try to achieve anonymity. For instance, one might consider a chat programme which measures users' typing patterns and identifies them regardless of whether they use multiple accounts, identify themselves with pseudonyms otherwise unrelated to their personal data, use different computers such as those available at internet cafes each time they log on, and so on. Or, perhaps, imagine a browser that monitors how a user moves the mouse and can thus always identify its users.

Clearly, the ability of such malicious software to create a centralised collection of identification data needs to be discussed when considering such scenarios, not to mention the possibility of making the measurement at all: a trivial example is that we need not worry that a web server might realistically make such measurements, as the mouse is obviously handled on the client side by the browser and hence the server of a web page never receives useful

timing data about mouse movements – nor, in fact, about typing, since the client sends batches of data at relatively large time intervals, e.g. when a user hits 'enter'). However, scenarios will arise when such measurements are possible.

The ability to make measurements does not necessarily imply an ability to extract meaningful conclusions. Pattern recognition systems often fail at tasks where there is an unconstrained ability to make measurements, because of difficulties in the task of recognition itself. Obviously, pattern recognition systems do perform well in many cases, so it is important to study what kinds of problems they can resolve. Whether recognition is possible depends on intrinsic characteristics of the task, and also on the data available.

We are currently considering a variety of possible behavioural biometrics and how such data can be abused for the task of identifying an unknown user, as opposed to verifying an identity already claimed by a user, which is generally relatively easy, given adequate data. This is still ongoing work, but we can summarise some results that are emerging. There are a number of different parameters of such a malicious effort, and if all of them are handled well, the task is solvable. We tabulate these parameters and table how their combinations affect the possibility of malicious activity.

complete access to user's computer (could be virus)	yes	yes	yes	no	no	no	Basic Parameters
initial training period possible: measuring user when identity is known	yes	no	no	yes	no	no	
known, fairly limited user group (e.g. 100s of users)	-	yes	no	-	yes	no	
(malicious) recognition task	easy	possible	very hard	very possible	hard	hopeless	
+use multiple biometrics	easy+	quite possible	hard	almost easy	still quite hard	hopeless	Modified Situation
+low processing power (e.g. local) or little data	very possible	hard	hopeless	possible	very hard	hopeless	
same application situation but imagining extremely powerful pattern recognition algorithms	easy+	easy	still quite hard	easy	quite possible	may become possible	

D. Profiling of web-users

(E. Benoist, VIP)

There are a lot of ways to gather information concerning web users. Sometimes the user is indeed aware that he is providing information to others, but sometimes he does not want to give any information and it is simply stolen.

D.1 Log files analysis

Since ever the web existed, there have been log files. This means that a server (such as Apache Httpd or Microsoft Internet Information Server IIS) stores a lot of information concerning each of the requests they deal with in a file (or several) which is then often used to compute statistics for a site, amongst other tasks.
Such a file is always generated by the server. It can either be stored for future use or otherwise be deleted if it is only used for debugging purposes. Log files contain a lot of information, and the user is usually unaware of this. Here is an example of an entry in an apache server log file, corresponding to a request for the page f.html originating from the IP address 62.2.135.157.

```
62.2.135.157 - - [23/Dec/2002:00:29:12 +0100]

"GET /Icons/70x1.gif HTTP/1.1" 200 54

"http://www.isbiel.ch/A/f.html"

"Mozilla/5.0 Galeon/1.2.5 (X11; Linux i686; U;) Gecko/0"
```

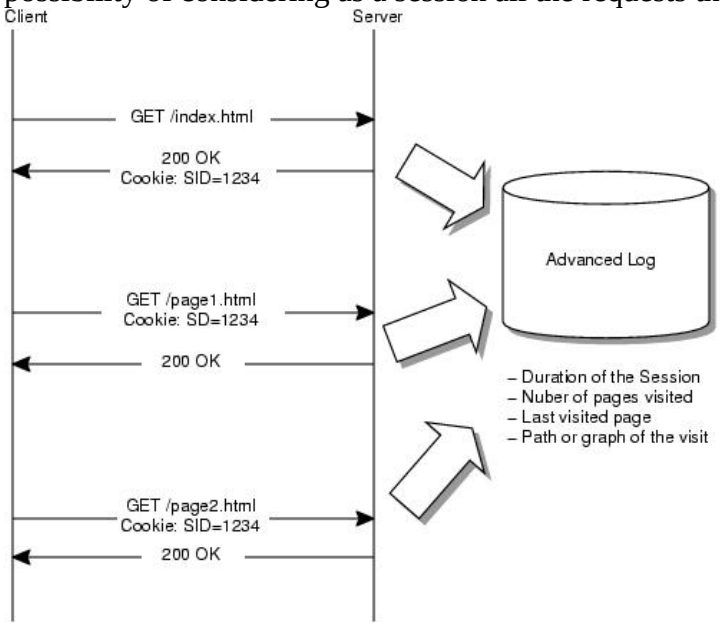
This entry contains the following information: IP address, Date of the request, HTTP Request (the first line), the return value (200 means OK, 404 document not found), the size of the information, the URL-referrer (the previously visited page), and the user agent (which browser or spider sent the request).

D.2 Session tracking

Since the Internet protocol for the web (HTTP) does not include session handling, developers have been forced to simulate this feature. In many circumstances, it is very important to follow the session of a user to see that different requests belong together. This is useful for instance in recognising whether a user has been granted access to the server with a username and password. It is also used to gather the elements of a virtual basket, such that the user can visit a web site and keep track of what s/he has bought.

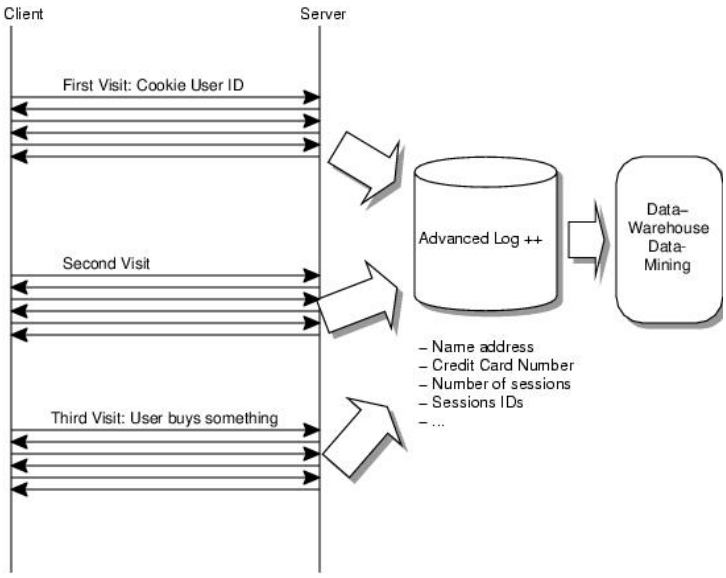
One method for tracking a session of a user is to send a cookie. Cookies are small pieces of information that are added inside the HTTP header, i.e. the first part of the source code of a web page, usually not visualised by a browser. The server sends this information with a statement of its validity, and as long as the cookie is still valid, it will be resent to the server each time the client sends a request to the same host.
Sessions can also be tracked for people that do not accept cookies. It is possible to insert a session ID in all the URLs of the requests for pages on the server. Such a method can be

detected by the user. But there exists another more complicated method. Since DHCP servers rarely dynamically change the IP address of a client during a session, one can expect that all the requests occurring from the same user have the same IP address. This offers us the possibility of considering as a session all the requests that originated from the same client.



D.3 User Tracking

Session tracking is useful for attacking privacy, but one can go further. If the user can be linked to all his sessions, a lot of information can be gained by this "total history" of a user's visits.
So-called user tracking can be achieved using cookies. But with such cookies, the validity must be set to one month or one year. Such a cookie contains a user ID that is stored in a database on the server such that the server can recognize the client the next time he visits the site. This is being done for example at www.amazon.com where the user receives advertisement and special offers corresponding to all the pages he has visited and all the item he has bought so far.



Again, such a tool may be dangerous for privacy. For instance if the user is not only known by his/her ID, but as a human being with a name, an address, and a credit card number. Then these pieces of information once entered by the user may "propagate", while the client may have expected that the site would have “forgotten” them.

maurus.frey@chaosnet.ch

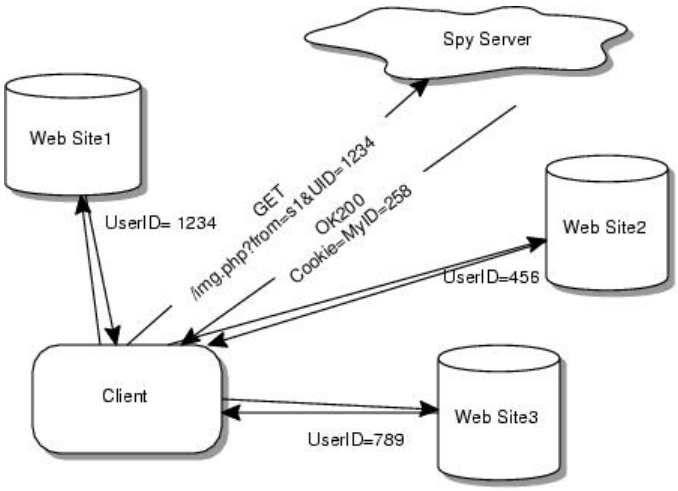
Messgs:	1
Visits:	26
First Visit:	2004-05-18 16:02:06
Last Visit:	2005-02-11 15:27:29

	Start	End	Total
1.	2005-02-11, 14:43:25	2005-02-11, 15:28:20	00:44:55
2.	2005-02-08, 21:08:01	2005-02-08, 21:08:33	00:00:32
3.	2005-02-05, 14:35:32	2005-02-05, 14:38:21	00:02:49
4.	2005-01-30, 17:38:23	2005-01-30, 17:38:23	00:00:00
5.	2005-01-17, 09:38:43	2005-01-17, 18:08:23	08:29:40

D.4 Multi-server user tracking

The next level in user profiling deals with the profiling over multiple hosts. Since cookies can only be sent to the site that created them, it is not possible to have the same cookie for more than one web site. That means that the user has different user IDs on different sites. The same person may be seen as ID=1234 on site1, ID=5674 on site2 and ID=007 on site3.
A solution to this problem is to have a central site that serves all the pages. This is clearly not usable in general, since it would not be efficient at all. Yet there is a simple efficient solution. We just have to insert a request for the same web site in all the pages of the different sites. This is possible, and indeed often done, using a small image. When a web page is

downloaded, the browser usually asks for all images that are contained in the page in order to display them in the same page. Usually, images are located on the same web site and are just static files. The idea however is to reference inside the web page an image that is stored on another server. This reference points indeed to a program that generates an image (for example using PHP) which is sent as the answer to the request. Such a program can use its own cookie and this cookie will be the same for all the web sites, since the image comes from the same server.



Such an image must not harm the design of the web page. There are two solutions: first it can be a banner that contains an advertisement and can centralise all the information. But it can also be a hidden pixel. That means an image with a height and a width of 1 pixel. If the pixel has the same colour as the pages that contain it, the user will never see it.

D.5 Protection measures

Disable Cookies
The protection can be on various levels. First one can simply disable the cookies in the browser. This means that the browser will never accept or send any cookie. Such protection is quite efficient, since one can not easily treat sessions and it is not possible to reference a user as a recognized client. Yet, a lot of web sites require cookies to handle sessions, and without enabling cookies users are unable to use many web sites that might be interesting.
Moreover, it is possible, using IP address, to retrace the session of a user using only the IP address (which does not change inside a session).

Disable persistent cookies
One can allow cookies to be used for one session only: it is possible to prevent them being stored on the hard disk and thus used as user ID for many transactions. This is quite harmless, since the only permanent cookies that are interesting concern language specifications.

Disable third parties cookies
This is used to prevent the information passing from one site to another. This is a good idea, since such information use always has negative connotations for the user. We cannot find a valuable program that uses this feature.

Define a policy for the use of cookies

Some web sites declare how they use data collected about users. Based on such information, it is possible to decide whether or not to supply information to this site.

E. Mathematical Tools for Data Mining

(Emmanuel Benoist and Bernhard Anrig, VIP)

The CRISP-DM process model contains 6 phases: Business Understanding, Data Understanding, Data Preparation, Modelling Evaluation and Deployment. We will focus here on the two steps depending on the machine: Modelling and Evaluation.
Modeling can be done with a very large set of algorithms and tons of heuristics. We present hereafter two rather simple modelisation technics, first the regression analysis and then a simple algorithm for constructing decision trees.

Since there exists no unique modelling technique that would work for any problem, we have to evaluate the accuracy of an algorithm and its configuration. This is done during the evaluation step. As an example, we present the cross-validation protocol for testing the quality of a method on a given set of data.

E.1 Regression Analysis

Suppose we have one set of data containing two variables (x and y) that seem to be correlated. We can test if the x's and the y's are linearly correlated with the following formulas. We try to build a formula for computing the y's knowing the x's, y=f(x). The same type of strategy works also if y is dependent on many different parameters (for instance y = 5.93 x + 1.87 z - 0.98 t).
Suppose we have a set of data containing for each record two parameters x and y. When we plot a graphical representation of the two parameters, they seem to form a line. We can have the intuition that the two parameters are linearly correlated. That is what we can compute.
Suppose we have some children with the age of 6, and we want to find an equation for modelizing the relation between size (in cm) and weight (in kg). We want to compute the weight knowing the size of a child.

Child number	Size (x)	Weight (y)
1	121	25
2	123	22
3	108	19
4	118	24
5	111	19
6	109	18
7	114	20
8	103	15
9	110	20
10	115	21

We first plot this set of points in a graphical representation. We remark that the points almost form a line. We will try to model the value of y as a linear function of x. This can be noted $y = ax + b$. The problem is now to find the values of the constants a and b.

We want to find a and b such that the line is a good approximation of the values. This will be done by minimizing the differences of the very value of y and its respective computed value.

To prevent that negative and positive differences could compensate, the sum of the squares of the differences is minimized.

$$S = \sum (y - ax - b)^2$$

This sum is minimal for two values of a and b (using derivation and the 0 of the derivate) to be obtained with the following formulas:

$$a = \frac{\sum xy - n\bar{x}\bar{y}}{\sum x^2 - n\bar{x}^2}$$

and

$$b = \bar{y} - a\bar{x}$$

In our example the mean value for x ($\bar{x}$) is 113.2, for y ($\bar{y}$) is 20.3. The results for the coefficients are therefore:
a = 0.42 and b = -27.38
This results in the equation:
weight = 0.42 height - 27.38
We can hence predict that a child of age 6 which has height 125cm will probably weight 25.27kg.

Such a method can easily be extended for attributes that are linear functions of many parameters. The mathematical concepts remain the same, the equations just have to be written in a matrix way.

Nevertheless this method is only available for numeric attributes that behave linearly. The equations have to be redesigned if the relation is not linear but quadratic ($y = ax^2 + bx + c$). More about linear (and non linear) regression can be found in any book on statistics.
However, such a method can not be applied to symbolic attributes, like city, profession, education grade, or ability to pay back a loan. Nevertheless, some numeric attributes can also not be used in such a method: the Zip code is normally difficult to be correlated with other values whereas it can be very informative regarding to the academic level or the average income for instance.

E.2 Constructing Decision Trees

The algorithm presented hereafter is known as ID3. Together with a lot of improvements, it has formed the widely used system C4.5 and its new release is called C5.0. Nevertheless, this is not the place to present all the possibilities offered by such systems. We will only focus on the main mechanism for building decision trees, the gain of information in a divide and conquer algorithm.
The algorithm we present here can only deal with Boolean attributes. One of the more complex steps in data mining is to find a way to discretise continuous variables. Transforming any attribute in a set of Boolean attributes can be done using algorithms (such as clustering), but is often made using ad hoc heuristics, that need to be precisely configured to work fine.
Suppose we want to build a decision tree. The algorithm works top-down, seeking at each stage an attribute to split on that best separates classes, and then recursively processing the subsets resulting from the split individually (a divide and conquer algorithm).
Suppose we have the following table:

Number of the person, Earns more than EUR15000(A), Married (B), University degree(C), Had problems to pay back a loan(D)

Number of the person	Earns more than EUR15000(A)	Married (B)	University degree(C)	Had problems to pay back a loan(D)
1	T	T	F	F
2	T	F	T	F
3	F	F	T	T
4	F	T	T	T
5	F	F	F	T
6	F	T	F	T
7	F	F	F	F
8	T	F	F	T
9	T	T	F	T
10	T	F	F	F
11	T	T	T	F
12	T	F	T	F
13	F	T	F	T
14	T	T	T	F
15	F	F	F	T

Consider that we have four attributes "Earns more than EUR15000" (A), "is Married" (B), "Received a University degree" (C) and "Had problems to pay back a loan" (D), each of which being Boolean, and we want to predict D. D is called the class. There are three possibilities for the attribute to be used at the root of our decision tree, i.e. A, B, or C. We examine the three cases. If we choose A, for A=true, we have 8 cases and there is 25% D=true and 75 % D=false (noted [2,6]) for A=false we have 7 cases which makes [5,1].
We have to measure the information contained in such a tree (or of any subtree). This will be done using its purity, which is the weighted mean of the purity of the leaves. The purity of a leaf is measured using its entropy. The formula is based on the probabilities pi of the class value (D in our example). The formula for the entropy is entropy ([p1,p2,p3,...,pn])=-p1 log(p1)-p2 log(p2) - ... -pn log(pn). In our case the entropy of the node [2,6] is -0.25*log(0.25)-0.75*log(0.75)=0.811 and the entropy of the node [6,1] is -0.86*log(0.86)-0.14*log(0.14)=0.592. Hence the value for this tree is the weighted mean of the two entropies, which makes:
(0.811*8+0.592*7)/15=0.709
We do the same for all the possible classes for the root of our tree. This means that if we take B as the root we have two leaves in our tree: [4,3] (for B=True) and [4,4] (for B=False). The information needed to order this tree is the weighted mean of the entropies and is 0.993. The last case is when the root is C, we have two leaves [1,4] and [6,3] this needs an information of 0.848 to be sorted. The higher the value is, the less information is gained by using the respective node as root for the decision tree. Hence we see that for example using the information whether someone is married or not (attribute B) does not influence very much (at least in our dataset) the ability of paying back a loan.
So we select the one attribute whose tree has the smallest entropy (where the purity of the nodes is the best). For our case, this means that the root for our tree is A. The same process described so far is then recursively done with the created leaves that are expanded into

subtrees independently. The tree grows until it has only pure leaves, or no other attribute can be used. There exists also heuristics to deal with almost pure leaves and to stop developing the branches, but this process is beyond the scope of this paper.

E.3 Neural Networks

The neural network domain is an involved, complex and evolving one, and detailing its mathematical derivation and implementation is out of the scope of this document. See http://richardbowles.tripod.com/neural/neural.htm for more information.
The main difficulty with neural networks is the interpretation of the results. Data Mining techniques provide a way to gain information about the data. The knowledge discovered can be understood and used. But neural networks work as black boxes. There is no way to understand how a pattern has been learnt, what sort of deduction has been done. The translation into a humanly understandable language is not possible. Moreover, in order to "learn" the way to answer a new question, a neural network needs a huge training set, which is probably not available.

E.4 Cross-Validation

Usually the amount of data which is available for processing is quite restricted, hence one has to develop concepts for testing the quality of the results gained so far with only the small amount of data. One well-known concept for this purpose is called "cross-validation". It consists mainly in choosing a number of folds in which you partition your data. So for example say we will use ten folds and therefore split our data into ten partitions p1 to p10 of approximately equal size. Then, nine of them, say p1 to p9, are put together and used for the training (the Modelling step of the CRISP-DM process) and the last one, p10, for testing the Evaluation step of the CRISP-DM. This is then repeated exactly ten times so that each partition (pi) is once used as a set for training while all others (p1, p2, ... p10 but not pi) are then used for testing. In this case we speak of ten-fold cross-validation.
Usually together with cross-validation, one uses stratified folds of data, that is one wants to make sure that in each of the folds the classes are represented approximately in the same proportion as in the union of all the ten sets.
The overall error rate of such a cross-validation is then computed as the average of the ten error estimates.
Note that depending on the application, one has to introduce different costs for different errors depending on their impact. So for example classifying an A as a B might cause much more damage than classifying a B as an A.

E.5 Products for data mining

A lot of products are available on the market for dealing with data mining problems: C4.5, C5.0, See5, Fair Isaac, Insightful Miner/ S-Plus, Mineset (PurpleInsight), SAS Enterprise Miner, SPSS Clementine, Statsoft Statistica ThinkAnalytics etc.

Weka is an open source framework intended to test algorithms for data mining that can be freely downloaded. [109]

[109] http://www.cs.waikato.ac.nz/ml/weka/

F. On Algorithms

(Jean-Paul van Bendegem, VUB)

In this section of the Appendix we will run through each one of the five topics mentioned in 3.2.3 under the heading "algorithms". The main purpose is to provide some examples that clarify the concise description in the main text of this report.

F.1. The choice of language in which to express the procedure can have a tremendous effect on the "success" of the algorithm in terms of efficiency (computer space and time required). As an example consider a (formal) language that accepts as a logical rule modus ponens – A and "If A, then B", therefore B – and suppose that we are dealing with a numerical problem, say, we are checking whether a property P holds for a particular number, say 100. The information we have is that 0 has the property P and that, for all numbers n, if n has the property, then so does n+1. If one wants to formally prove that 100 does indeed have the property, there is only one option: start with 0 and apply modus ponens over and over again to go from 0 to 1, from 1 to 2, …, from 99 to 100, thus the rule is applied a 100 times.

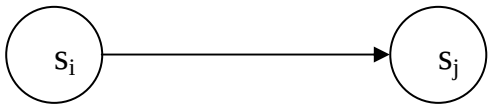
However, suppose that we make the language a bit more expressive. Suppose that we allow ourselves to "contract" repeated steps. To give a concrete example: on the basis of the language given, it is possible to give a general proof (i.e., not restricted to particular numbers) that if the property holds for n, so it holds for 2n, the double of n. In that case one gets a "speed-up" effect. Starting from 1, one runs through the powers of 2, i.e., 2, 4, 8, 16, 32, 64, and, because the next step gets us beyond 100, we will have to make 36 one-step moves, starting from 64, to reach 100. This means that we now need 6 + 36 = 42 steps to complete the same process. (Note incidentally this curious phenomenon, well-known to mathematicians, that proving a general case is often easier than proving a particular case, although, of course, the general case is far more informative than a special case. The implication is straightforward: there is no simple relationship between the complexity of a (logical-mathematical) proof and the scope of the content of the statement proven).

It seems a straightforward extension of the above idea to make languages as expressive as possible. However, this is not the case, since expressivity entails complexity issues and problems. A classic example in the area of formal logic is the problem of the choice between first-order and second-order logic. In rough terms, if we are talking about objects and their properties, first-order logic only allows quantification over objects ("For all things x, so-and-so"), whereas second-order logic allows quantification over objects *and* properties ("There is a property P, such that for all things x, so-and-so"). Second-order logic is obviously far more expressive, but, to give just one example, there is no proof theory, meaning, informally, that a satisfactory definition of what constitutes a proof cannot be produced.

(George S. BOOLOS, John P. BURGESS & Richard C. JEFFREY: *Computability and Logic, Fourth Edition*, Cambridge: Cambridge University Press, 2003, is still considered to be the best introduction).

F.2 The choice of support or carrier for the algorithm. In the logical-mathematical literature the standard conception of a computing device is still the concept of a Turing machine **T**. **T** consists of a tape and a reading-writing machine. The tape itself is divided in

squares and each square may contain a symbol taken from a (usually minimal) alphabet, viz. 0 and 1. The machine itself is described in terms of (a finite number of) states s_1, s_2, …, s_n and (a finite number of) movements, usually moving left (L), moving right (R). Thus a typical program instruction would be <0, s_i, s_j, 1>, i.e. if **T** reads a 0 on the tape and is in state s_i, then it changes into a state s_j, and writes 1 on the tape. Often a diagrammatic approach is preferred (this obviously bares a connection to the choice of language!) to represent a basic action of **T**, i.e., the execution of one instruction:



0 : 1

Amazing as it sounds, but nearly the whole of mathematics can be translated in terms of such machines. It is an extremely powerful tool, because of its simplicity and its scope. It allowed Alan Turing to show that a machine that would be able for any other machine to decide whether that machine will or will not stop when given a specific input, cannot exist. Thus there is *no universal mechanism or algorithm* to decide whether arbitrary problems have or have not solutions.

However, at the same time, it is clear that a Turing machine **T** is quite independent of any support whatsoever, it is typically a "paper" computer; the physical basis, i.e., how **T** is implemented, is of no importance (or, at least, assumed to be). More specifically, no issues of (underlying) causality have to be dealt with. Recent advances in computer technology are rapidly changing this picture:

- Quantum computing requires the preparation of quantum mechanical systems in very specific states to make the computation possible; in this case the physical system is of primordial importance and the limits of the quantum mechanical system co-determine the computational limits. (Related to this topic is the discussion whether quantum mechanical Turing machines can do "more" than classical Turing machines - still an open question at this moment),
- Organic computers require a biological support and here too, the inner workings of, say, a cell need to be well understood in order to get a grip on the computation itself. Biochemical processes are involved, such as DNA-RNA interactions, that determine what the computational possibilities are. Hence the support is primary.

This raises the interesting discussion whether or not one can consider the underlying physical system itself as the algorithm and not necessarily a symbolic representation of that system (comparable to the phenomenon that time is defined presently, not by any artificial man-made object but by a "natural" object, viz. pulsars). It relates to the *John Lucas-Roger Penrose* discussion whether the human brain can be considered to be a classical Turing machine, or to be seen as such, or none of these.[110]

[110] see Penrose R. ,1989, *The Emperor's New Mind*, Oxford University Press where nearly all topics in this paragraph are dealt with at length and also its sequel of 1994, *Shadows of the Mind*, Oxford University Press.

F.3 Program verification is a separate issue is that is often ignored in actual practice: it concerns the question whether the program or algorithm really does what one expects it to do. Of course, in simple cases there is not much of a problem, but, as soon as complexity reaches a certain level, it becomes a difficult task *to prove that* the program is correct. Usually the proof verifying the program or the algorithm is more complex than the algorithm itself (often measured in terms of length, how many symbols are needed to write down the algorithm or program and the verification). An example to illustrate this point:

Consider a "simple" program for division for positive numbers, x and y:

((r := x; q := 0); while y ≤ r do (r := r – y; q := 1 + q))

Note that the program not only produces q, the quotient, but at the same time r, the remainder. In order to prove that this program does indeed do what we claim it should do, a formal language to talk *about* programs is necessary. Related to topic 1, a language is required, in this case, we will need statements such as:

- P{Q}R (informally: "given the input described by P, after execution of Q, R results"),
- x := f (informally: "replace x everywhere by f").

In addition we will need axioms as we want to *prove* that the program is correct:

- P_0{x := f}P, where P is P_0 with x replaced everywhere by f, (D0)
- If P{Q}R and "If R, then S" is provably the case, then P{Q}S (D1)
- If P{Q}R and "If S, then P" is provably the case, then S{Q}R (D2)
- If P{Q_1}R_1 and R_1{Q_2}R, then P{Q_1;Q_2}R, (D2)
- If (P and B){S}P then P{while B do S}(not-B and P) (D3)

This is the formal proof of correctness of the above program, illustrating the complexity issue (the two lemmas are merely arithmetical truths that are assumed to be correct; the example is taken from one of the early great "classics" in program verification, viz. C.A.R. Hoare's 1969 paper:[111]

1	$\mathbf{true} \supset x = x + y \times 0$	Lemma 1
2	$x = x + y \times 0\{r := x\}x = r + y \times 0$	D0
3	$x = r + y \times 0\{q := 0\}x = r + y \times q$	D0
4	$\mathbf{true}\{r := x\}x = r + y \times 0$	D1 (1, 2)
5	$\mathbf{true}\ \{r := x; q := 0\}x = r + y \times q$	D2 (4, 3)
6	$x = r + y \times q \wedge y \leqslant r \supset x = (r - y) + y \times (1 + q)$	Lemma 2
7	$x = (r - y) + y \times (1 + q)\{r := r - y\}x = r + y \times (1 + q)$	D0
8	$x = r + y \times (1 + q)\{q := 1 + q\}x = r + y \times q$	D0
9	$x = (r - y) + y \times (1 + q)\{r := r - y; q := 1 + q\}x = r + y \times q$	D2 (7, 8)
10	$x = r + y \times q \wedge y \leqslant r\{r := r - y; q := 1 + q\}x = r + y \times q$	D1 (6, 9)
11	$x = r + y \times q\{\mathbf{while}\ y \leqslant r\ \mathbf{do}\ (r := r - y; q := 1 + q)\}$ $\neg y \leqslant r \wedge x = r + y \times q$	D3 (10)
12	$\mathbf{true}\ \{((\mathrm{r} := \mathrm{x}; \mathrm{q} := 0); \mathbf{while}\ y \leqslant r$ $\mathbf{do}\ (r := r - y; q := 1 + q))\} \neg y \leqslant r \wedge x = r + y \times q$	D2 (5, 11)

[111] Hoare CA.R., 1969 , "An Axiomatic Basis for Computer Programming", in *Communications of the ACM*, 12, nr. 10, 576 – 580.

(Note that this topic is of importance to society: there have been court trials to decide whether a (commercially available) program was indeed sufficiently verified or not, as the program malfunctioned and a "guilty" party had to be identified.[112]

F.4 Conflicting data and inconsistencies. To illustrate the problem the title is referring to, consider a database containing data, expressed in terms of statements or properties, represented by p, q, r, … Reasoning with these data involves the use of rules in the format of A ← B, meaning that, if B (often referred to as *the head of the clause*) is the case, then A (often referred to as *the body of the clause*) will result. Consider now the following rather simple case:

- q ← p
- r ← p
- (s and t) ← r
- not-p ← s
- p ←

This set of conditions is inconsistent, since the last clause states that p is a fact, but then q is a fact, r is a fact, but then s and t is fact as well, and hence also s, but then also not-p. How to deal with this situation? It is definitely the case that, because of the size of actual databases and because of the permanent, often "real-time" updating of databases, inconsistencies will and do result. The question then becomes: what to do?

The most common strategy underlying a number of proposals to deal with inconsistencies is to look at maximally consistent subsets. Thus in the above example, it is obvious that by dropping the clause "p ← ", the problem is solved, although not much can be said now, except that not-p is the case. Therefore, it seems more interesting to delete the fourth clause, because then we can assume (though not necessarily) p, q, r, s and t to be the case. This raises the important issue: how to detect the maximally consistent subsets? Perhaps not entirely unexpectedly, this problem, although in principle solvable in the finite case, is of (at least) NP-complexity (see the next topic for a definition), in short, a "hard" problem.

An alternative is to work with preferences, e.g., defined on the clauses. If we prefer not-p over p, for whatever reasons, then it is obvious that in the example given, we will drop the last clause, because that is compatible with accepting not-p. However, other problems appear: what if the preferences are such that no clause can be satisfied? Then one needs to rearrange the preferences. Of course, one might think about trying out all preferential possibilities, but that problem again is NP-hard.

A next step – but that, to our knowledge has not really been made in computer science today – is to analyse the contradiction itself, to reason with it, and, on the basis of that analysis, to make a choice one way or another. This requires a move that both logicians and computer scientists are not all that willing to make: to abandon or, at least, to adapt classical logic. Without going into too much detail, here is the crux of the matter. In classical logic a

[112] See Mackenzie D., 2001, *Mechanizing Proof. Computing, Risk and Trust.* Cambrigde, Mass, MIT for an excellent report of this affair.

contradiction is a disaster, because of the classically valid argument "If both p and not-p are the case, then anything, q, is the case", the infamous "ex contradictione sequitur quodlibet". To reject a logical rule, one must find a counterexample to it, in this case, one must find a situation wherein both p and not-p are the case, and, at the same time, not anything is the case, i.e., q can be false. The latter part is easy, enough things are not the case, but the first part requires a curious move: to accept that there are situations wherein a statement and its negation can be both true. However, the reward is phenomenal: one can now reason with contradictions.[113]

F.5 Complexity and randomness is perhaps the most intriguing topic. Looking at problems that are solvable, i.e., there is a program that will execute the program in a finite time, requiring a finite amount of space, and produce an answer, one way or another, it soon became apparent that some problems are easy to solve, some difficult to solve. The imprecise notions "easy" and "difficult" equally soon became translated in formal terms. Any problem is characterised by some parameters k, l, m, n, … If a problem is solvable in time or space expressible as a polynomial of some parameter of the problem, then we have a P-problem. E.g., given n books, to sort these books alphabetically is a P-problem. (Take the first book, that requires one step, take the second book, see if it comes before or after the first book, this involves two steps, take the third book, see if it come to left, to the right or in the middle of the two books already sorted, in short, one needs 1 + 2 + 3 + … + n steps, or, n(n+1)/2 steps, and that is a polynomial). Other problems require an exponential amount of space and time to solve the problem (putting together a schedule for train traffic is such a problem). A special subgroup are those problems for which an exponential solution is known, at the same time it is not known whether a P-solution exists, and, in addition, it is always possible to make a guess for the solution, a guess that can be checked in P-time. Such problems are NP-problems (see the above topic). In fact, at the present moment, there is a quite complicated hierarchy of complexity measures.

However, even more intriguing, is the fact that, given a program, given sets of data, there will always be structures or patterns, present in the data, that the program will not recognise as such. In other words, to the program the structure will appear *random*, although there is structure present. The core of the argument is this: if a given set of data has a structure or contains some pattern, then it must be possible to describe that pattern, and, obviously, this description must be shorter than a simple enumeration of all the data. What we are doing in a sense is to compress the data. If this compression is to be reliable, then we must able to prove so (compare with topic 3). If we succeeded in proving the compressions in all possible cases, then any data set can be compressed and that runs counter to the idea that there are genuinely random sets. There will therefore always be data sets that contain patterns that will not be detected and hence will appear as random.

Excellent guides in these matters are the works of Gregory J. CHAITIN: *Information, Randomness and Incompleteness. Papers on Algorithmic Information Theory*. London: World Scientific, 1990; *Algorithmic Information Theory*. Cambridge: Cambridge University Press, 1992; *The Unknowable*. Heidelberg: Springer Verlag, 1999. Here one finds the formal counterparts of the informal arguments presented above.

[113] See Priest G., Routley & Norman (eds.), 1989, *Paraconsistent Logic. Essays on the Inconsistent*. München, Philosophia Verlag, for the "bible" of paraconsistent logic.

G Using user's Profiling and Artificial Agents for Stimulating the Knowledge Exchange Process in Virtual Communities

(Thierry Nabeth, Albert A. Angehrn and Pradeep Kumar Mittal, CALT - INSEAD)

In this section, we are going to examine how artificial agents relying on personal behavioural user profiling can be used to stimulate the participation in the knowledge exchange process in virtual communities.

G.1 What are Virtual communities?

G.1.1 Defining the virtual community concept

Howard Rheingold, the person who popularised the term "virtual communities", has defined this concept as "social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace".[114] In a later review of literature aiming at understanding why people are joining virtual communities, Ridings and Gefen[115] (2004) have found that the concept of virtual community has been characterised more generally as (1) people with shared interests or goals for whom electronic communication is a primary form of interaction, (2) groups of people who meet regularly to discuss a subject of interest to all members, (3) and groups of people brought together by shared interests or a geographical bond. We will define ourselves a virtual community as an "electronically-supported" social structure holding together a set of people sharing a common culture, set of interests, values, goals or norms.
In the last few years, virtual community has emerged as one of the more important actionable paradigms for supporting the circulation of tacit knowledge in our digital societies.

G.1.2 Virtual community environments

In this context, virtual community environments are the techno-sociological infrastructures that have been specially elaborated to support these virtual communities. Virtual community environments include all the systems, such as forums or bulletin boards, that provide explicitly shared dedicated spaces for supporting the discussions of communities or groups of people. The communication in these spaces can be asynchronous (bulletin board) or real-time synchronous (chatrooms). People interact mainly with others by posting messages in (public or restricted) shared spaces, but can also sometimes communicate directly and more privately with one another. The control of what can be posted in the public spaces (specified in an explicit or implicit code of conduct) can be enforced by a moderator or by some social regulation mechanisms (social pressure, norms, etc.). Recent forms of virtual community systems are enhanced with technical mechanisms and features aiming at better supporting and stimulating the social process, via the visualisation of people activities (with the whole line of research dubbed as *social transluscence*)[116] or the provision of matching mechanisms helping the forming of groups or the establishment of relationships.

---

[114] Rheingold H., 1993, *The virtual community: Homesteading on the electronic frontier*, Reading MA Addison – Wesley.
[115] "Virtual Community Attraction: Why People Jang Out Online", in *Journal of Computer – Mediated Communication* 10 (1), art 4, Nov. 2004.
[116] Erickson T. et al., 2002, "Social translucence: Designing Social Infrastructures that Make Collective Activity Visible.", in *Communications of the ACM (Special issue on Community*, ed. J Preece), vol 45, no. 4, 40 – 44.

G.2 The challenges of participation

G.2.1 Virtual communities: the participation challenge

One of the main challenges facing designers and operators desiring to build successful virtual communities,[117] is the establishment of a sustainable dynamic of participation amongst its members. Indeed, the essential value of a virtual community resides in the activities of its members and in particular is strongly correlated to their willingness to spend time, to interact with others in conversations, or to provide knowledge assets. The participation of the members of a virtual community in this knowledge exchange process is indeed not spontaneous, but is motivated by a certain number of elements such as: direct rewards, increased reputation, internal satisfaction (altruism and efficacy), or reciprocity. [118]
Understanding the "mechanics" of the functioning of the participation in a knowledge exchange in virtual communities or in groups has been the subject of numerous researches in different fields such as: knowledge management and organisation[119] [120] [121]; CSCW[122] [123]; complexity[124]; social computing[125]; sociology and communication,[126] or psycho-sociology [127], to name a few.

G.2.2 Some directions for addressing the participation challenge

From these theories, we could try to derive a set of principles that could be used to address this participation challenge. One of these principles could consist in working on the establishment for the members of these communities a climate of trust,[128] a sense of community,[129] and a feeling of recognition for the actions of their members.[130] Other principles could be derived from the Social exchange theory,[131] which proposes an economic

[117] see Cothrel and Williams, 1999, "On-Line Communities: Helping Them From and Grow", in *Journal of Knowledge Management*, 3 (1), 54 – 65, March 1999, for the main success factors.
[118] Hall, 2001, "Social exchange for knowledge exchange". Paper presented at *Managing Knowledge: conversations and critiques*, University of Leicester Management Centre, 10-11 April 2001.
[119] Wasko and Faraj, 2000, "'It is What One Does', Why people participate and Help others in electronic Communities of Practice", in *Journal of strategic Information Systems*, 9, 115 – 173.
[120] Cothrel and Williams, 1999.
[121] Sharratt and Usoro, 2003, "Understanding Knowledge-Sharing in Online Communities of Practice", in *Electronic Journal of Knowledge Management*, 1 (2), dec 2003.
[122] Majchrzak et al, 2003, "Computer Mediated Inter-Organizational Knowledge Sharing; Insights from a Virtual Team Innovating Using a Collaborative Tool", in *Information resources Management Journal*, vol 13, nr. 1.
[123] Brock and Kim, 2003, "Exploring the Influence of Rewards on Attitudes Towards Knowlegde Sharing", in *Advanced Topics of Information Resources Management* (2), IDEA Group publishing, PA.
[124] Reed, 1999, "That Sneaky Exponential: Beyond Metcalfe's Law to the Power of Community Building", in *Context Magazine*, spring.
[125] Erickson et al., 2002.
[126] Ridings C., and Gefen D., 2004, "Virtual Community Attraction:Why People Hang Out Online", in *Journal of Computer-Mediated Communication* 10 (1), Article 4, November.
[127] Beenen et al., 2004, "Using social psychology to motivate contributions to online Communities", in *Proceedings of ACM CSCW 2004, Conference on Computer Supported Cooperative Work*, Chicago, IL.
[128] Tung et al., 2001, "An Empirical Investigation of Virtual Communities and Trust", in *Proceedings of the 22nd International Conference on Information Systems*, 307 – 320.
[129] Blanchard and Markus, 2002, "Sense of Virtual Community-Maintinging the Experience of Belonging", in *35th Annual Hawaii International Conference on System Sciences* (HICSS '02), vol 8. Koh and Kim, 2003, "Sense of Virtual Community: A Conceptual Framework and Empirical Validation", in *International Journal of Electronic Commerce*, vol 8, nr. 2, winter 2003 – 04, 75.
[130] Chan et al., 2004, "Recognition and Participation in a Virtual Community: A Case Study", in *Proceedings of the 37th HICSS Conference* Hawaii 2004.
[131] Thibaut & Kelly, 1959, *The social psychology of groups*. New York, Wiley.

model of rational choice to explain participation. More concretely, a virtual community designer could set up mechanisms supporting the factors that make people participate,[132] such as: (1) anticipated reciprocity; (2) expected gain in reputation and influence on others; (3) altruism and perception of efficacy; (4) direct reward. Cognition and psycho-sociology also have some theories on influence that could be applied to "orient" people in their desire to contribute to a knowledge exchange process. For instance to stimulate participation one could try to exploit some of the six principles of influence of Robert Cialdini of: (1) reciprocity (felt obligation to "reimburse"); (2) social validation (social conformance); (3) commitment / consistency (tendency to act in a similar way as in the past); (4) friendship / liking; (5) scarcity; (6) authority.[133] Finally, an interpretation of the laws of Metcalfe and of Reed on the importance of critical mass effect could lead to putting more effort to reach a critical mass, and making more visible the perceived value of the virtual community for the user. [134]

G.3 Using Behavioural profiling and Intelligent Agents to Stimulate People Participation

G.3.1 Using intelligent agents to stimulate people participation

One of the most interesting approaches found to stimulate social participation in digital community platforms consists in implementing mechanisms that contribute to make the activities of their members visible. This approach has attracted an important attention in the research community via the concept of *social transluscence.*[135]

Another promising approach that we would like to present in this section would be to start from a similar idea of behaviour-based cognitive profiling suggested by Kinshuk and Lin (2004) for the design of adaptive learning communities, and to apply it for stimulating members' participation in the knowledge exchange in virtual communities.

The main principle of this approach consists in the use of artificial agents that are aware of the behavioural profile of the members, and that intervene proactively using this information to stimulate members' participation. This approach relies on two components: (1) the automatic construction (using a set of heuristics) of a behavioural profile of each member related to his knowledge exchange activity; (2) the generation of agent interventions that are the most likely to stimulate the participation of a particular member. The selection of the most effective interventions is based on the behavioural characteristics of the member.

The construction of this profile results from the observation of the actions of the user and the application of a set of heuristics helping to determine the participatory profile. The different actions that are captured and intervene in the determination of the participation profile include events such as: entering digital spaces, posting files, posting messages in bulletin boards, answering to messages, and so forth. The different behavioural patterns to which a particular user can be categorised include: the level of involvement (is he often present?) and the nature of his contributions (is he only a lurker? Is he a contributor of knowledge assets? Does he participate in the discussions? Does he initiate discussions? etc.). Examples of heuristic rules include: a user that has not connected to the system in the last month can be considered inactive. A user that posts in discussion at least one time a week is committed in exchanging his knowledge. A user that has posted in the last three months at least one document is an active knowledge contributor.

---

[132] Hall, 2001.

[133] Cialdini and Sagarin, 2005, "Interpersonal influence", in Brock T. and Green M. (eds.), Persuasion: *Psychological insights and perspectives.* Newburry Park, CA Sage Press, 143 - 169.

[134] Reed D.P., 1999.

[135] Erickson et al., 2002.

These agent interventions aim at different objectives: (1) To create awareness. For instance the agent may inform the member about a knowledge exchange practice he may not be aware of. (2) To raise interest. For instance the agent may present a knowledge exchange practice under an angle that makes it particularly meaningful and useful to this member. (3) To stimulate action. For instance, the agent may suggest an action and encourage the member to try this action. (4) To reinforce the practice. For instance, the agent may congratulate the member and provide him with feedback demonstrating the value and the impact of his contributions.

G.3.2 The importance of the personal behavioural profile

The effectiveness of these different agent interventions depends greatly on the exploitation of the user personal information, and in particular on the level and nature of user participation.
For instance, Everett Rogers (1995) theories of innovation diffusion states that people do not adopt straightaway a new attitude but go through a series of phases of adoption (awareness, interest, trial, and adoption).[136] The agent therefore needs to know about the current participatory level of the user (for instance is the member already familiar with some of the knowledge exchange practices or is he totally unaware?) when selecting the most effective intervention, in order to avoid proposing to the member something that is too crude, or on the contrary too sophisticated for this particular user. For instance it would be useless to invite a member of a community to share knowledge with others, if this member has shown in the past very little readiness to participate in an interaction. On the other hand, in may be useful just to inform this member of the benefits people get in interacting more with others.
Similarly this theory of innovation diffusion distinguishes different category of people (from the innovator, to the laggards) in regard to their attitude towards innovation. For instance, the innovators are principally driven in their action by their curiosity, whereas the late adopters are very sensitive to social pressure and will change their practice when they realise that they are isolated in their behaviour. An intervention that is likely to have the most affect on an innovator will be one that emphasis novelty, whereas the interventions that will have the most effects on a late adopter will be one that emphasis the social conformance ("everybody does it that way").
We can imagine many other sorts of usage of the behavioural profile information (level and nature of participation, personality traits, cognitive style or attention state) of a member for stimulating people participation in a knowledge exchange. In particular, it could be an interesting exercise to try to derive from the different theories addressing the participation challenge that we have mentioned previously (knowledge management, psycho-sociology, sociology, etc.) a set of agent interventions that would make use of this information to increase the level of participation in a community. For instance, some interventions would be directed to increase the climate of trust, the belonging (sense of community) or the feeling of being recognised. Some other intervention could even function more surreptitiously and rely on the psycho-sociological theories of influence,[137] and play on factors such as social imitation, commitment, reciprocity, to increase the impact of the interventions.

[136] Rogers E., 1995, *Diffusion of Innovations* (fourth edition). New York, Free Press.
[137] Cialdini & Sagarin, 2005.

G.4 Many promises, but still a long way to go

The approach that we have presented previously looks very promising since it provides an outlook on radically new categories of applications that personal behavioural profiling can make possible.
However, beyond the ethical questions that are features of the manipulation and the exploitation of behavioural information, the empirical validation of these approaches still need to be done, even if some preliminary work in this direction has already begun.[138] In particular, several questions are still open, such as the reliability of personal behavioural profiling (heuristics and machine learning techniques have limitation), complexity of operationalisation of the solution (artificial cognitive agents still have a long way before going out of the laboratory) and acceptance (how will the users integrate in their work the use of intelligent mechanisms).

H The Profiling Game Riezlern[139]

(Claudia Diaz, COSIC)

H.1 Introduction: The Game

This document describes a profiling competition that took place in January 2005 as part of the program of the First FIDIS PhD Event.[140] The competition was organised as follows: fifteen PhD students, divided in three groups of five people, had to collect as much information as possible about three target subjects, using for this purpose information publicly available on the Internet. The participants had a few hours to complete the task.
The purpose of the game was to use this simple experiment to get an idea on the amount of data available on the Internet, as well as to explore approaches to collect and combine these data. The participants were given freedom to decide how to proceed with the collection and

[138] Kinshuk and Lin, 2004, "Cognitive profiling towards formal adaptive technologies in web-based learning communities", in *International Journal Web Based Communities*, vol 1, nr. 1, 103. Angehrn, 2004, *Designing Intelligent agents for Virtual Communities*, INSEAD CALT Report 11. Roda et al., 2003, "Using conversational agents to Support the Adoption of Knowledge Sharing Practices", in *Interacting with Computers, Special Issue on Intelligence and Interaction in Community –based Systems*, Elsevier, vol 15, issue 1,januari, 57 – 89. Razmerita, Angehrn and Nabeth, 2003, "On the role of user models and user modeling in Knowledge Management Systems", in *Proceedings of the 10th international Conference on Human – Computer Interaction*, Greece, vol 2, 450 – 456.

[139] For a reference of a similar initiative, see also Personal data for the taking by Tom Zeller Jr., The New York Times, via CNET News.com, May 18, 2005. As part of a computer science and security project (Johns Hopkins project) and working with a strict requirement to use only legal, public sources of information, groups of three to four students set out to vacuum up not just tidbits on citizens of Baltimore, but whole databases: death records, property tax information, campaign donations, occupational license registries. Several groups managed to gather well over a million records, with hundreds of thousands of individuals represented in each database. http://news.com.com/Personal+data+for+the+taking/2100-7348_3-5711761.html

[140] This is a report of the first PhD training event of FIDIS, January 2005: "How much information on someone can you find in the Internet?" This question motivated a profiling game in which 15 PhD students participated. This report describes how the game was conducted, the tools that were used to obtain information on the profiled subjects, the information that was found, the methodologies followed by the participants in order to build profiles and discussion and conclusions on the game.

combination of data, as far as only publicly available data was collected. In order to be able to verify the correctness of the collected data, the target subjects were among the participants (one per group), and each group had to collect data on the two target subjects who belonged to the other groups. As a disclaimer, it is worth nothing that the specificity of the profiled subjects (German PhD students with active Internet lives), does not (yet) make these results generalisable to the information available on an average citizen.
At the end of the game, the groups had to present the profiling information of the target subjects they had studied. Each piece of data had to be linked to the web address or resource where it had been obtained. Groups obtained points for the data that was found exclusively by them. When a group had mistakenly added to the profile information that was not related to the subject (e.g., data belonging to someone else with the same or a similar name), points were lost.
In the following sections, we describe the tools used to collect the information, the type of information that was found, the strategies used to build the profile, the main issues addressed by the discussion that took place after the game and the conclusions we have extracted from this experiment.

H.2 Tools to collect data

The most heavily used tools for the collection of data were search engines. They were used to get the basic information, that was later complemented with other search tools. The participants reported having used the following tools:

- Google was extensively used. The keywords searched were initially name and surname. Later on, as more information on the subject became known, other keywords such as town or email address were used in order to refine the search or obtain additional information.
- Other search engines, such as Altavista provided complementary information. Search engines for a specific type of content, such as images.google.com or groups.google.com also provided complementary data (like pictures) on the profiled subjects. Google News was used to find newsgroup posts from student times.
- National and local phone books. As the nationality of the three profiled subjects was German, the German phone book proved to be useful to provide the home address, the phone number and sometimes even the profession of the subjects. Searches for people in the same town with the same surname led to the discovery of relatives.
- Home pages proved to be a rich and reliable source of information, they typically provide a CV that describes many of the activities developed by the subject and the places and institutions in which he or she has worked. Moreover, it usually contains some indications of the preferences and interests of the subjects, as well as a publication list. Once the subjects were linked to other people, the home pages of co-authors, friends, colleagues and relatives provided additional information.
- Archived sources such as google's cache or www.archive.org provided information that was no longer available in the original site, either because it had been removed or because the website was no longer active.
- Various messenger accounts were used to obtain information; for example ICQ, Skype.com, MS Messenger and Jabber. Orkut and Open BC Membership provided information on the social network and the interests of the subject.
- OpenBusinessClub provided information about membership in organisations.
- Key servers provided the PGP key and information on the social network of the subjects (by looking at the people who had cross-signed their key with the subject).
- School pages, once the schools the subject has attended become known (typically mentioned in the CV).
- Domain's owners search (www.denic.de) and search for home pages in web domains that contain the name or surname of the subject. This provides additional home pages the subject may have or maintain.
- Citeseer, DBLP and other publication search engines provided the publications of the subject and links to coauthors and related researchers.
- Newspapers, mainly local newspapers from the home
- town of the subject provided information on their public activities. Some groups also searched for events that were reported on the birth date of the subject.
- Newsgroups on topics of interest for the subjects provided information on the technical activities and knowledge of the subjects, as well as relationships.
- Well known stores, such as Amazon.com, were looked into in order to find information on the books, films, ior other articles the subject buys on the Internet.

Some participants proposed a list of additional tools that could be used to further enhance the profiling, but which were not used due to the limitation of time for the exercise. Additional data gathering tools include:

- Buying the financial record from Schufa.
- Buying the consumer profile from Informa.
- Run a password guessing tool for web form logins on Amazon and eBay with the subject's e-mail-addresses to harvest the business histories these sites keep.
- Inquire the subject's highschool, university and employer to ask about certificates, graduation etc.
- Check the many find-your-classmates web pages.
- Write him/her an email to get one back to see the IP-address and the Mail-Client.
- Try to sniff the communication of the subject in order to monitor his or her Internet activity.

H.3 Results of the search

The first goal of the participants was to find personal homepages. These were easily found by searching the names in Google, as they appeared on top of a list of a few hundreds of hits. The home pages were used to collect a basic set of information such as:

- Work place, position, professional activities, work location
- Contact information: town, address, phone, fax, email address
- CV, which typically contains educational and professional history of the subject (name of previous companies, schools, universities, etc.)
- Publication list, which provides information on the research interests and co-authors
- Picture (a picture of the subject is often available)

From this basic information, and using the tools listed in the previous section, the participants were able to obtain for one or more of the profiled individuals additional information such as:

- Personal phone, address, alternative email addresses
- Languages spoken
- Political affiliation, and participation in political activities or discussions
- Religious affiliation, and participation in religious groups
- Participation in public awareness campaigns in the local town
- Multiple alternative email addresses that served as pseudonyms in certain domains. These email addresses could have been further investigated in order to find additional information related to the subject under the pseudonym
- Pictures of the subject and taken by the subject
- Military membership and grade
- Date and place of birth
- Name, address and phone numbers of relatives
- Sports, hobbies and miscellaneous interests (photography, philosophy, etc.)
- Social network: names of the co-authors, colleagues,
- friends (including the name and picture of an *Internet fan)* and relatives of the subjects were easily found
- Places the subject has been to and dates of the stays
- Personal diaries full of personal details (in some cases travel diaries) revealed daily patterns of activity

- Opinions posted in a variety of Newsgroups
- An image of the (physical) signature

The amount of misleading data (which was unrelated to the subject) found was minimal. However, it is expected that searchs on subjects with more common names than the profiled ones in this particular game would generate larger amounts of misleading information (or would require more effort in order to separate the information that refers to the subject of interest and that belonging to other, unrelated subjects).

H.4 Building a profile

The limited duration of the game, and the large amounts of data to be gathered, left little time for sophisticated profiling of the subjects. Most groups presented the collected data, classified as belonging to distinct areas of identity. This organisation of the data led to some preliminary conclusions on meta-data, which is not directly available but inferred by the combination of several sources of data.

The subjects were naturally implementing identity management mechanisms, as the information they provided varied according to the topic and environment of the hosting web site. For example, one of the subjects had provided an informal picture for his student website, and a formal one for his profile in a business website. However, all these data could be linked together with simple searchs in the Internet (as had been made obvious by the first part of the exercise). The distinct profiles that could be built on each of the profiled subjects were:

- The **educational** and **professional** profiles were easily available for any of the subjects. Detailed and complete information was provided in the personal homepages. This is consistent with the idea that it is in the interest of the subject to have a publicly available professional identity, because it is useful to improve his or her professional career. Even more, we could say that a public professional profile is today required in the research field in order to conduct daily working activities.
- Several aspects of the **personalised profil**e were also easily available. In particular, there was extensive information related to hobbies, sports and other interests (some somehow related to the professional activity, like participation in Newsgroups on topics related to their work; and some totally unrelated, like photography or philosophy). Much of this information was made available through the homepages (or pages linked to it), and other was easily linkable to the subject, as it usually contained his or her name and other verifiable information. From this observation, we could say that users often like to make public these details, possibly as means to be reachable for people who share similar interests. More sensitive information, like sexual orientation, religious beliefs or attitudes towards drugs could also be extracted from the available data.
- Unfortunately, there was no psychologist among the participants. However, a draft **psychological, behavioural** and **ideological** profile could be built, both based on the opinions (and the websites in which opinions were posted), language use, pictures (face, expression, clothing, background) topics discussed, and personal experiences described in Newsgroups, posts and online diaries (which proved to be a very rich source of information for building a psychological profile). Some of the groups selected some personal details for their expositions in order to give a feeling on the degree of detail of some data that can be found and linked to a person.
- Most of the groups presented names of people who appeared to be related to the studied subjects. Participants highlighted that, if more time was available, it would be easy to

build the **social network** of the subject. Names and addresses of relatives were found in the phonebooks; names of colleagues and co-authors were available in the homepages; some groups tried to google the address or phone number to look for other people living with the subject; Membership accounts provided social contacts of the subjects; descriptions of trips or events often included names of other people; and key servers provided the trusted relationships with other PGP users.

- One of the aspects that proved harder to find with the available tools was the **consumer** profile. Some groups could withdraw conclusions on items of interest for the subject from the description of personal interests or experiences, as well as from the available pictures. However, a more detailed search may reveal the consuming patterns of users who have an account in eBay, Amazon, or other e-commerce websites. Moreover, it is worth noting that this information is not available to the Internet user, but it is to the companies with which the subject has made transactions (and to all those other companies that buy the date share information with the original company). In this sense, the data is in fact available to those who are interested in exploiting it in order to build –valuable consumer profiles.
- No **financial** information was available through search engines. More sophisticated techniques (possibly involving social engineering or hacking activities) may be required in order to access this sort of information. However, the financial status of the subjects could be roughly estimated from the data. Similarly, no **health** related information was found. Nevertheless, assumptions could be made on the general health condition and the lifestyle of the subject by examining the available information (for example, someone involved in hard sport activities could be assumed as being in a healthy condition).

The combination of information related to a subject, belonging to different contexts, opened the possibility of sophisticated profiling, When many different identities of the profiled individuals were put together (combination of professional, personal, and leisure activities), the result was a rather detailed and complete picture of the subject. Even though this was only outlined by the participating groups, the large amounts of data gathered (which could not be thoroughly analysed) suggested that building a sophisticated profile, which included most important aspects of a person's life, was possible.

H.5 Discussion

A short discussion followed the presentations of the profiles. One of the issues that was raised was the very question of the meaning of profiling. While some argued that the fact of putting together facts relative to a subject which comes from different sources is effectively building a profile, others argued that the gathering of information should be understood as *data mining* and that *profiling* consisted in inferring meta-data from the row data (i.e., interpreting the available data in order to classify the subject according to abstract models or categories).
The freedom given in the definition of the game *"build a profile as complete as possible"*, led to different interpretations. While some groups looked for as many details as possible, others focussed on more general information that could give a "big picture" of the subject. Similarly, not every group used the same searching tools. Some focussed on the social network, some others on the professional and educational profiles, some on the social activities, and some on their writings. This led to another relevant question: What is relevant to build a profile? In order to answer this question, we need to know what is the purpose of

building a profile. Clearly, a company wanting to sell a product is interested in profiles which provide the information of how likely is a customer of buying a certain product; while a potential employer will be interested in the educational and professional profile.
Given that the profiled individuals were among the participants, we could ask the question of whether they were really aware of the amount of information related to them that was publicly available in the Internet. They acknowledged that, although much of the information had been made public by themselves, they were not aware of the existence (or linkability to their public identity) of certain data (in some cases, such as contact details of relatives, the data could seem scary).
What are the potential threats a person could face due to the exposure of personal information? It is clear that an adversary wanting to harm the reputation or even the physical life of a subject, could use the Internet as a source of valuable information. In another level, companies can use this information in order to sell their products or services to the subject, organisations seeking to extend their membership (e.g., religious sects) may use this information in order to target individuals who are more likely to be converted, and public powers may also profile their citizens in order to exercise more control on the populations (e.g., anti-system individuals could be easily monitored and controlled).
Why do people provide information on themselves? The main advantage and motivation for making personal data publicly available is that having a persistent identity in the Internet is a necessary condition to develop professional, personal, commercial and leisure activities. Offering a public profile enhances accessibility for other people who share interests. Keeping a public profile is also a tool to build reputation (e.g., providing the CV and the list of publications). A public identity is, in short, necessary to develop enhanced professional and personal activities, as well as a tool to extend the social network beyond traditional territorial borders.

H.6 Conclusions

Here we summarise some of the most important conclusions extracted from the experiment:

- For individuals who develop activities in the Internet, large amounts of information linkable to their identity are available. This information includes professional, educational, personal and psychological data, as well as enough information to build (at least) a partial social network.
- Sensitive data such as financial, consumer and health information, religious and political beliefs or sexual orientation are harder to find, but it either can be found with more sophisticated search tools or inferred from the available information.
- Internet users have a clear interest in making public their educational and professional profile in order to widen their professional opportunities. Regarding the personalised profile, some aspects are also made public, possibly to share information or stablish communication with people who share similar interests.
- There are certain aspects of the personalised profile for which the subjects do not have an interest in making easily linkable to their professional profile. Yet, this information is easily linkable with simple search tools (due to the fact that it shares an identifier, e.g., the name, with the professional profile).
- Profiled subjects found most disturbing the public availability of data they had not introduced in the Internet and which referred to their *offline* lives (for example, the home phone number or address), mainly that available in public indexes as phonebooks. Also,

subjects seemed to be surprised by the possibilities of constructing a social network, which ranged from names and locations of relatives to an extensive network of social and professional relationships which could hardly be denied.

- Subjects were performing some identity management when interacting with different parties and in distinct contexts. Yet, many of these partial identities could be traced and linked to a natural individual for which extensive information on his work, life, interests and location was available.
- People (including technically educated people) do not seem to be fully aware on the information on themselves that is publicly available in the Internet and easy to find and link. When they realise the degree of public exposure to which they are subject, there is often a feeling of vulnerability.
- The exposure of personal data may constitute a security problem. On the other hand, it is used as a tool to build reputation, enhance the professional and personal network, and share information with people with similar interests.
- Once information has entered the Internet, it cannot be removed. Web pages which are no longer available can still be retrieved from archives and chaches. Therefore, once the data has been introduced in the Internet, it is no longer under the control of its owner.
- Human intelligence was behind the search strategies and profiling methods. Although automated searches could be helpful in the collection of data, complex decisions need to be taken in order to discriminate relevant from irrelevant (and even misleading) information. This high cost in time and human resources for building just one profile may discourage massive sophisticated profiling.
- The intervention of human intelligence may explain the minimal amount of misleading information that was presented as part of the profiles.
- Social networks, on the other hand, are easier to build in an automatic way. A program could easily search for links in webpages and appearances of identifiers such as names, email addresses or locations in order to construct a social network.
- The results provided by the search engines were much better for language dependent content. Regarding the language issue, it also seems that people (at least Germans), even if they have good knowledge of English, tend to write in their mother tong.
- Finally, there is clearly a need for identity management tools that allow for pseudonymous, unlinkable management of information that belongs to separate contexts in order to empower the user in the management of his or her data and identity.

Glossary:

correlation
*general***:** a reciprocal relation between two or more things
in statistics: a statistic representing how closely two variables co-vary; it can vary from -1 (perfect negative correlation) through 0 (no correlation) to +1 (perfect positive correlation);
a statistical relation between two or more variables such that systematic changes in the value of one variable are accompanied by systematic changes in the other
*non linear***:** any correlation in which the rates of change of the variables is not constant; also called curvilinear correlation
see http://www.elook.org/dictionary/correlation.html

data controller: the subject (person or organisation) that determines the purposes and means of the processing of data

data mining: data processing using sophisticated data search capabilities and statistical algorithms to discover patterns and correlations in large pre-existing databases; a way to discover new meaning in data
see http://www.elook.org/dictionary/correlation.html

data subject: the subject (human or non-human, individual or group) the data refer to

data processing:
computer science: a series of operations on data by a computer in order to retrieve or transform or classify information
see http://www.elook.org/dictionary/correlation.html
legal: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
Directive 95/46 EU on Data Protection, concerning processing of personal data, art. 2 sub b

KDD: knowledge discovery in data bases, comprising the whole process of recording, storing, tracking of data, including discovery of patterns by means of data mining techniques and interpretation of the correlated data

ontology: In computer science, **an ontology** is the product of an attempt to formulate an exhaustive and rigorous conceptual schema about a domain. An ontology is typically a hierarchical data structure containing all the relevant entities and their relationships and rules within that domain (eg. a **domain ontology**).
see: http://en.wikipedia.org/wiki/Ontology_(computer_science)

profile: set of correlated data that identifies and represents a data subject. If the data subject is a group/a category/or a cluster we speak of a group profiles, when the data subject is a single person we speak of a personalised profile

profiling: the process of constructing profiles (correlated data), that identify and represent a data subject (either a person or a group/catogory/cluster), and/or the application of profiles (correlated data) to identify and represent a person as a specific person or as member of a specific group/category/cluster, aiming at the assessment of risks and/or opportunities for the data user (inferred from risks and opportunities concerning the data subject)

semantic web: Although the term 'ontology' has been used very loosely to label almost any conceptual classification scheme, among practising computational ontologists, a true ontology should besides the subsumption relation (also: 'is a', 'subtype' or 'subclass'), also describe entities by other 'semantic relations' that specify how one concept is related to another.
see:
www.en.wikipedia.org/wiki/Ontology_(computer_science)#Semantic_web

(end) user: the profiled data subject using a certain device (web, customer loyalty card) that facilitates the recording of data to be stored and processed for the data controller

References:

Agre, P.E. (1999), "The Architecture of Identity: Embedding Privacy in Market Institutions", in 2 *Info. Comm. And Soc' y* 1 (Spring). To be downloaded at: http://www.infosoc.co.uk/00105/feature.htm

Agre, P. E. (2001), "Beyond the Mirror World: Privacy and the Representational Practices of Computing.", 29-62, in *Technology and Privacy: The New Landscape*, edited by P. E. Agre and M. Rotenberg. Cambridge, Massachusetts: MIT.

Agre, P.E. and Rotenberg, M. (2001), *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts: MIT.

Andre E., Klesen M., Gebhard O., Rist T. (2000), "Exploiting Models of Personality and Emotions to Control the Behavior of Animated Interactive Agents", in *Fourth International Conference on Autonomous Agents*, pp. 3-7, Barcelona.

Angehrn, Albert A. (2004), *Designing Intelligent Agents for Virtual Communities*; INSEAD CALT Report 11-2004.

Armstrong, S. J. (1970), "How to Avoid Exploratory Research", *Journal of Advertising Research* 4, p. 27-30.

Beenen, G., Ling, K., Wang, Xiaoqing, Chang, K., Frankowski, D., Resnick, P. and Kraut R.E. (2004), "Using Social Psychology to Motivate Contributions to Online Communities", in *Proceedings of ACM* CSCW 2004 Conference on Computer Supported Cooperative Work, Chicago, IL. 2004.

Berendt, B., Günther, O., Spiekermann, S. (2005), "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior", in *Communication of the ACM (CACM*), vol 48, no.3, 2005.

Berry, M. J. A. and Linoff G. (1997), *Data mining techniques: for marketing, sales, and customer support*. New York.

Blanchard, A., Markus A.L. (2002), "Sense of Virtual Community-Maintaining the Experience of Belonging", in *35th Annual Hawaii International Conference on System Sciences (HICSS'02)*-Volume 8.

Bock, G.W., and Kim, Y.G. (2003), "Exploring the Influence of Rewards on Attitudes Towards Knowledge Sharing", in *Advanced Topics of Information Resources Management*, (2), IDEA Group Publishing, PA.

Bonnet, M. (2001), "Personalization of Web Services: Opportunities and Challenges", in *Ariadne*, 22 June 2001, Issue 28. To be downloaded at: www.ariadne.ac.uk/issue28/personalization/intro.html.

Bruha, I. (2000), "From machine learning to knowledge discovery: survey of preprocessing and postprocessing", in *Intelligent Data Analysis* 4: 363-374.

Brusilovsky, P. (1999), "Adaptive and Intelligent Technologies for Web-based Education", in C.Rollinger and C.Peylo (eds.) *Kunstliche Intelligenz, Special Issue on Intelligent Systems and Teleteaching.*

Brusilovsky, P., (2001) "Adaptive Hypermedia", *User Modeling and User- Adapted Interaction*. Kluwer Academic Publisher, vol. 11 p 87 – 110.

Calenda, D. (2004), "Social Implications of online personalization", *Paper presented at the international expert meeting 'Issues of online personalisation'*, 5 March 2004, Oxford Internet Institute.

Camp,L.Jean (2003), *Identity in Digital Government, A Report of the 2003 Civic Scenario Workshop*, Kennedy School of Government, Harvard University.

Canhoto, Ana and Backhouse, James (2004), *'Constructing categories, Constructing signs - analysing differences in Suspicious Transaction Reporting practice'*. Information Systems Integrity Group, London School of Economics, London.

Chaitin, G.J. (1990), *Information, Randomness and Incompleteness. Papers on Algorithmic Information Theory*. London: World Scientific.

Chaitin, G.J. (1992), *Algorithmic Information Theory*. Cambridge: Cambridge University Press.

Chaitin, G.J. (1999), *The Unknowable*. Heidelberg: Springer Verlag.

Chan, C. and B. Lewis (2002), "A basic primer on data mining.", in *Information Systems Management* 19(4): 56-60.

Chan, Calvin M. L., Bhandar, Mamata, Oh, Lih-Bin, Chan, Hock-Chuan (2004), "Recognition and Participation in a Virtual Community: A Case Study", in *Proceedings of the 37th HICSS Conference*, Hawaii, 2004.

Chung, H. M. and Grey P. (1999), "Special edition: Data mining", in *Journal of Management Information Systems* 16(1), 11-16.

Cialdini, R. B., & Sagarin, B. J. (2005), "Interpersonal influence", in T. Brock & M. Green (Eds.), *Persuasion: Psychological insights and perspective*s (pp. 143-169). Newbury Park, CA: Sage Press.

Clarke, R. (1994), "The Digital Persona and its Application to Data Surveillance", in *The Information Society* 10 (2).

Cothrel, Joseph and Williams, Ruth (1999), "On-Line Communities: Helping Them Form and Grow", in *Journal of Knowledge Management* 3 (1) March, 54-65.

Crabtree, Barry and Soltysiak, S. (1998), "Identifying and Tracking Changing Interests", in *International Journal on Digital Libraries*, Vol. 2, No. 1, pp 38-53.

Crossley, M., Kings N.J., Scott J.R. (2003), "Profiles - Analysis and Behaviour", in *BT Technology Journal*, vol 21, nr.1, Januari 2003.

Custers, Bart (2004), *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epideminology.* Nijmegen: Wolf Legal Publishers.

Darlinski J., *Wissen ist Macht*. To be downloaded at http://datenschutz.in-berlin.de/rasterfahndung.pdf.

De Croock, M.B.M., Paas, F.G.W.C., Schlanbusch, H., & van Merriënboer, J.J.G. (2002), "ADAPT-IT: Instructional Design (ID) tools for training design and evaluation", in *Educational Technology, Research and Development*, 50(4), 47-58.

Diogene (2002), *Survey on Methods and Standards for Student Modelling; Diogene project*, September 2002. To be downloaded at: http://www.diogene.org/archive.html.

Dolog, P. and Nejdl, W. (2003), "Challenges and benefits of the semantic web for user modeling". Paper presented at the *International Workshop on Adaptive Hypermedia and Adaptive Web-based Systems (AH 2003*), 20-24 May, Budapest, Hungary.

Dolog, Peter and Nejdl, W. (2003), "Personalisation in Elena: How to cope with personalisation in distributed eLearning Networks", in *Proceedings of International Conference on Worldwide Coherent Workforce, Satisfied Users - New Services For Scientific Information*, Oldenburg, Germany, September 2003.

"Durant M. v Financial Services Authority Case" (2003), *EWCA, Civ 1746, Court of Appeal* (Civil Division), 8th December 2003. <www.courtservice.gov.uk> and <http://bailii.org/ew/cases/EWCA/Civ/2003/1746.html>

Enos L. (2001), "Deal Afoot to Destroy Toysmart Database", in *E-Commerce Times*, January 10, 2001.

Erickson, T., Halverson, C., Kellogg, W. A., Laff, M. and Wolf, T. (2002), "Social Translucence: Designing Social Infrastructures that Make Collective Activity Visible.", in *Communications of the ACM (Special issue on Community*, ed. J. Preece), Vol. 45, No. 4, p. 40-44.

European Parliament and of the Council, (1995), "Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of individuals with regard to the processing of personal data and on the free movement of such data", in *Official Journal* L281/31, 1995.

Fabris, P. (1998), "Advanced navigation", in *CIO Magazine*, 50-55.

Fayyad U. et al.(1996), *Advances in knowledge discovery and data mining.* Menlo Park, California: AAIPress / The MIT Press, p 6.

Fayyad, U., Djorgovski, S. G. et al. (1996), "From digitized images to on-line catalogs: data mining a sky survey.", in *AI magazine* 17(2), 51-66.

Fayyad, U., Piatetsky-Shapiro G., et al. (1996), "From data mining to knowledge discovery in databases.", in *AI magazine* 17(3), 37-54.

Fayyad, U., Piatetsky-Shapiro G., et al. (1996), "The KDD process for extracting useful knowledge from volumes of data.", in *Communications of the ACM* (11): 27-34.

Fink, J., Kobsa, A. (2000), "A Review and Analysis of Commercial User Modeling Servers for Personalization on the World Wide Web", in *User Modeling and User Adapted Interaction, Special Issue on Deployed User Modeling*, 10, p.204-209.

Fischer G. (2001), "User Modeling in Human-Computer Interaction", in *User Modeling and User Adaptive Interaction*, Kluwer Academic Publishers, vol. 11, 1-2, 65-86.

FIDIS (2005), *Del 2.2 Cases, stories and Scenarios* WP 2, FIDIS Project.

FIDIS (2005), *Del 2.3 Models of identity* WP2, FIDIS Project.

Funsten, D. M. (1998), "Helping your customers behave themselves.", in *Bank Marketing* 30(10): 22-27.

Hall, Hazel (2001); "Social exchange for knowledge exchange". Paper presented at *Managing knowledge: conversations and critiques*, University of Leicester Management Centre, 10-11 April 2001.

Hand, D. J. (1998), "Data mining: statistics and more?" in *The American Statistician* 52(2), 112-118.

Hand, D. J., H. Manila, et al. (2001), *Principles of data mining*. Cambridge, MA, MIT Press.

Hoare C.A.R.(1969), "An Axiomatic Basis for Computer Programming", in *Communications of the ACM***,** 12, nr. 10, 576 - 580.

Hardy Q. (2004), "Data of reckoning", in *Forbes*, 173, 151-153.

Heckmann, D., Schwartz, T., Brandherm, B., Schmitz, M. and Von Wilamowitz-Moellendorff, M. (2005), "GUMO - The General User Model Ontology", to appear in *Proceedings of UM 2005: International Conference on User Modeling*, July 24 -30, 2005, Edinburgh, UK.

Hildebrandt, M. (2005), "Privacy and Identity: a reply to Archard's *The value of Privacy"*, in *Privacy and the criminal law*, Antwerp Oxford: Intersentia 2005 (to be published).

Hildebrandt, M. (2005), "Are profiles justiciable?". Paper presented at the *Conference Is Knowledge justiciable*? Essen, Germany 21-23 March 2005.

Hudson, B. (2005), "Secrets of the Self", in *Privacy and the criminal law*. Antwerp Oxford: Intersentia (to be published).

Humby, C., T. Hunt, et al. (2003), *Scoring points: how Tesco is winning customer loyalty*. London, Kogan Page.

Ihde, Don (1993), *Philosophy of Technology: an Introduction.* New York: Paragon House.

IMS (2001), "IMS Learner Information Packaging Information Model Specification; Final Specification,Version 1.0", in *IMS Global Learning Consortium*, March 2001. To be downloaded at: http://www.imsglobal.org/profiles/lipinfo01.html.

Jackson, J. (2002), "Data mining: a conceptual overview.", in *Communications of the Association for Information Systems* 8: 267-296.

Jøsang A., Patton M.,(2003), "User Interface Requirements for Authentication of Communication", in *ACM International Conference Proceeding Series, Proceedings of the Fourth Australian user interface conference on User interfaces 200*3 - Volume 18, Adelaide Australia, 75.

Karampiperis P., D. Sampson (2004), "Adaptive Learning Object Selection in Intelligent Learning Systems", in *Journal of Interactive Learning Research, Special Issue on Computational Intelligence in Web-Based Education*, vol. 15(4), 389-409, November 2004.

Kay, J, (2000), "User modeling for adaptation, in User Interfaces for All", in Stephanidis (ed), C, Salvendy, G, (General Editor), *Human Factors Series*. Lawrence Erlbaum Associates, 271—294.

Kinshuk, Taiyu Lin (2004), "Cognitive profiling towards formal adaptive technologies in web-based learning communities", in *International Journal of Web Based Communities*, Vol. 1, No. 1, 2004 103.

Kobsa, A., Koenemann, J., and Pohl, W., (2000), "Personalized hypermedia presentation techniques for improving online customer relationships", in *The Knowledge Engineering Review*, 16, 111-155.

Koh Joon and Young-Gul Kim (2003), "Sense of Virtual Community: A Conceptual Framework and Empirical Validation", in *International Journal of Electronic Commerce*, Volume 8, Number 2, Winter 2003-4, 75. To be downloaded at: http://www.soc.napier.ac.uk/publication/op/getpublication/publicationid/321908.

Kuner C., Barcelo R., Baker S., Greenwald E.(2000), *An Analysis of International Electronic and Digital Signature Implementation Initiatives, A Study Prepared for the Internet Law & Policy Forum (ILPF)*, September. To be downloaded at: <www.ilpf.org/groups/analysis_IEDSII.htm>

Lenzen, R. (2004), "Customer Analytics: It's all about behavior", In *DM Review*.

Lessig L. (1999), *Code and other laws of cyberspace*. New York: Basic Books.

Levi, M. and Wall, David S. (2004), "Technologies, Security, and Privacy in the Post-9/11 European Information Society", in *Journal of Law and Society* 31 (2), 194-220.

Manago, M. and M. Auriol (1996). "Mining for OR.", *ORMS Today Special Issue*: 28-32.

Nabeth, T., Angehrn, A.A. and R. Balakrishnan (2004), "Integrating 'Context' in e-Learning Systems Design", in *IEEE International Conference on Advanced Learning Technologies (ICALT 2004)*, Joensuu, Finland.

Nash, K. (2001), "Casinos hit jackpot with customer data", in *CNN.com*.

Mably, K. (2000), *Privacy vs. Personalization.* Cyber Dialogue Inc. To be downloaded at: <www.cyberdialogue.com>

Mackenzie D.(2001), *Mechanizing Proof. Computing, Risk, and Trust*. Cambridge, Mass.: MIT, 2001.

Majchrzak, Ann, Ronald, E. Rice, Nelson, King, Arvind Malhotra; Sulin Ba (2003), "Computer-Mediated Inter-Organizational Knowledge-Sharing: Insights from a Virtual Team Innovating Using a Collaborative Tool", in *Information Resources Management Journal*, Vol. 13, No. 1.

Mobasher, B., Cooley, R., Srivastava, J. (2000), "Automatic Personalization Based on Web Usage Mining. Web Usage mining can help improve the scalability, accuracy, and flexibility of recommender systems", in *Communications of the ACM, Association for Computing Machinery*, August 2000, 142 – 151.

Möller, J. and Florax, B.J. (2002), "Kreditwirtschaftliche Scoringverfahren", in *Multimedia und Recht* (12*)*, 806-811, München.

O'Looney, J. (2002), "Personalization of Government Internet Services". To be downloaded at:
http://www.digitalgovernment.org/lobrary/library/dgo2001/DGOMAC/MEDIA/OLOO.PDF

Paternoster, C. & Searby, S. (2002), "Personalise or Perish?", White Paper in *BT Exact Technologies.*

Peacock, P. R. (1998), "Data mining in marketing: part 1.", in *Marketing Management* 6(4), 8-18.

Peppers, D. and M. Rogers (1999). *Enterprise one to one: tools for competing in the interactive age*. New York, Currency Publishing Company.

Petri, Dr. T. B., (2003), "Sind Scoringwerte rechtswidrig?", in *Datenschutz und Datensicherheit* (27), p. 631-636, Wiesbaden.

Penrose, R.(1989), *The Emperor's New Mind.* Oxford: Oxford University Press.

Penrose, R.(1994), *Shadows of the Mind*. Oxford, Oxford University Press.

Piatetsky-Shapiro, G. (2000), "Knowledge discovery in databases: 10 years after.", in *SIGKDD Explorations* 1(2): 59-61.

Prins, J.E.J. (2004), "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, 8.3. <www.ejcl.org>.

Pohl W. (1997). "LaboUr - Machine Learning for User Modeling". *Proc. of the Seventh International Conference on Human-Computer Interaction.* Amsterdam: Elsevier.

Razmerita, L. (2004), "User modeling and personalization of the Knowledge Management Systems", book chapter in *Adaptable and Adaptive Hypermedia*, edited by Sherry Chen and George Magoulas, published by Idea Group Publishing.

Razmerita, L., Angehrn, A.A. and A. Maedche (2003), "Ontology based user modeling for Knowledge Management Systems", in *Proceedings of the 9th International Conference on User Modeling*, Pittsburgh, USA, Springer-Verlag, 213-217.

Razmerita, L., Angehrn, A.A. and Nabeth, T. (2003), "On the role of user models and user modeling in Knowledge Management Systems", in *Proceedings of the 10th International Conference on Human-Computer Interaction*, Crete, Greece, Vol. 2, 450-456.

Reed, D., P. (1999), "That Sneaky Exponential: Beyond Metcalfe's Law to the Power of Community Building", in *Context Magazine*, spring. To be downloaded at: http://www.contextmag.com/archives/199903/digitalstrategyreedslaw.asp

Rheingold, Howard (1993), *The virtual community: Homesteading on the electronic frontier.* Reading, MA: Addison-Wesley.

Ridings, Catherine and David Gefen (2004), "Virtual Community Attraction:Why People Hang Out Online", in *Journal of Computer-Mediated Communication* 10 (1), Article 4, November. To be downloaded at : http://jcmc.indiana.edu/vol10/issue1/ridings_gefen.html.

Riedl J. (2004), "Recommender System for Personalization". Paper presented at the *international expert meeting 'Issues of online personalisation'*, 5 March 2004, Oxford Internet Institute.

RetailWeek (2003). "Solutions CRM: Profile shopping". *Retail Week***,** 22.

Roda, C., Angehrn, A.A., Nabeth, T. and L. Razmerita (2003), "Using Conversational Agents to Support the Adoption of Knowledge Sharing Practices; Interacting with Computers", *Special Issue on Intelligence & Interaction in Community-based Systems*; Elsevier, Vol. 15, Issue 1, 57-89, January.

Rogers Everett M. (1995), *Diffusion of Innovations* (Fourth Edition). New York, Free Press.

Shahabi C., Chen Y. (2003), *Web Information Personalization: Challenges and Approaches* 2003. To be downloaded at: http://infolab.usc.edu/docDemos/DNIS2003pdf.

Sharratt, M; Usoro, A. (2003), "Understanding Knowledge-Sharing in Online Communities of Practice", in *Electronic Journal of Knowledge Management*, 1(2), December.

Shearin Sybil, Henry Lieberman (2001), "Intelligent Profiling by Example", in *ACM Conference on Intelligent User Interfaces*, Santa Fe, NM, January 2001.

Smyth B., Cotter P., (2000), "A Personalized television listings service. Mixing the collaborative recommendation approach with content – based filtering seems to bring out the best in both methods", in *Association for Computing Machinery. Communications of the ACM*, August 2000, vol. 43, 8 107 – 111.

Stephanidis, C. (2001), "Adaptive Techniques for Universal Access", in *User Modeling and User-Adapted Interaction*, Kluwer Academic Publishers, vol.11, 159-179.

Priest G., Routley, Norman (eds.) (1989), *Paraconsistent Logic. Essays on the Inconsistent*. München: Philosophia Verlag.

Thibaut, J. W., & Kelley, H. H. (1959), *The social psychology of groups*. New York: Wiley.

TILT – Tilburg Institute for Law, Technology, and Society (2004), *Research report 'Issues of Online Personalization in Commercial and Public Service Delivery*'. Tilburg University, June 04.

Tung, L., Tan, P., Chia, P, Koh, Y. and Yeo, H. (2001), "An Empirical Investigation of Virtual Communities and Trust", in *Proceedings of the 22nd International Conference on Information Systems*, 2001, 307-320.

Turow, J., Feldman, L., and Meltzer, K.. (2005). "Open to Exploitation. American Shoppers Online and Offline." Annenberg Public Policy Center of the University of Pennsylvania. To be downloaded at: http://www.annenbergpublicpolicycenter.org.

Van Barneveld, J. (2003), *User Interfaces for Personalizes Information Systems*. *State of the Art*. Telematica Instituut.

Van Brakel, J. (1999), "Telematic Life Forms.", in *Techné: Journal of the Society for Philosophy and Technology* 4 (3). To be downloaded at: http://scholar.lib.vt.edu/ejournals/SPT/v4_n3html/VANBRAKE.html

Vedder, Anton (1997), "Privatization, information, technology and privacy: Reconsidering the social responsibilities of private organizations". In: Geoff Moore (ed.) *Business Ethics: Principles and Practice.* Sunderland: Business Education Publishers Ltd, 215-226.

Vedder, Anton (1999), "KDD: The Challenge to individualism", in *Ethics and Information Technology*, 1, 4, 275-281.

Vedder, Anton (2001), "KDD, privacy, individuality and fairness". In: R. Spinello and H. Tavani (eds.) (2001), *Readings in Cyberethics.* Boston, Toronto, London, Singapore: Jones and Bartlett Publishers, 404-412.

Vedder, A.H. & Wachbroit, R.S. (2003), "Reliability of information on the Internet: Some distinctions", in *Ethics and Information Technology*, *5*, 211-215.

Warntjen, M. and Kissler, D.(2002), "Die Schlechten von den Guten trennen", in *Forum und Recht* (2). To be downloaded at http://www.forum-recht-online.de/2002/202/202warntjen_kissler.htm.

Wasko, M. and Faraj, S. (2000), "It is What One Does': Why People Participate and Help Others in Electronic Communities of Practice.", in *Journal of Strategic Information Systems*, 9, 155-173. To be downloaded at http://www.ejkm.com/volume-1/volume1-issue-2/issue2-art18.htm.