FIDIS

Future of Identity in the Information Society

Title:	"D 2.2 Set of use cases and scenarios"
Author:	WP2
Editors:	Main editor: Thierry Nabeth (INSEAD, France) + see list
Reviewers:	Collective
Identifier:	D 2.2
Type:	[Deliverable]
Version:	1.7
Date:	26 May 2006
Status:	[final]
Class:	[final]
File:	`2005-fidis-wp2-del2.2_Cases__stories_and_Scenario-1.7.doc`

Summary

The objective of this document is to propose a very concrete and multi-disciplinary presentation of identity issues via the provision of a series of cases, stories, scenarios and perspectives.

Each of these cases, stories, etc, has been elaborated by a different member of the FIDIS consortium.

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

Copyright Notice:

Members of the FIDIS consortium

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

Versions

Version	*Date*	*Description (Editor)*
0.1 Initial release	15.11.2004	Thierry Nabeth All the contributors. Revision: contributors + other members of FIDIS
	18.12.2004	LSE: Ana Isabel Canhoto and James Backhouse
	23.12.2004	Claudia Diaz
	5.01.2005	IPTS: Sabine Delaitre
	10.01.2005	VUB: Wim Schreurs
	10.01.2005	ICPP: Christian Krause, Henry Krasemann, Martin Meints
	13.01.2005	VIP: Bernhard Anrig, Emmanuel Benoist, and David-Olivier Jaquet-Chiffelle
0.5 second release	10.01.2005	Thierry Nabeth
	17.01.2005	LSE: Ana Isabel Canhoto and James Backhouse
	18.01.2005	Univ. of Reading: Mark Gasson, and Kevin Warwick
	18.01.2005	TU-Dresden: Sandra Steinbrecher
	18.01.2005	ICPP: Christian Krause, Henry Krasemann, Martin Meints
	18.01.2005	IPTS: Sabine Delaitre
	18.01.2005	VIP: Bernhard Anrig, Emmanuel Benoist, and David-Olivier Jaquet-Chiffelle
	19.01.2005	VUB: Wim Schreurs
	19.01.2005	KU-Leuven: Claudia Diaz,
1.0 Final	19.01.2005	Thierry Nabeth
1.1 Final+minor change	20.01.2005	Claudia Diaz
1.2 Final+minor change	25.01.2005	Thierry Nabeth Fixed a missing reference.
1.3 New version	24.08.2005	VIP: Bernhard Anrig. New version of chapter 3.
1.4 New version	7.09.2005	Claudia Diaz, KU-Leuven. New improved version of chapter 7. (including references).
1.5 New version	13.09.2005	ICPP: Christian Krause, Henry Krasemann, Martin Meints, New version of chapter 2.

1.6 New version	15.09.2005	VUB: Wim Schreurs: • New version of chapter 6. • Worked on improving the legal dimension of the deliverable as a whole. Thierry Nabeth: Conclusion
1.7 New version	26.05.2006	VIP: David-Olivier Jaquet-Chiffelle. Correction of the **definition 3 (subject)** in "Chapter 3. Virtual? Identity".

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. Introduction	INSEAD: Thierry Nabeth
2. Scenarios and a story on Identity, Anonymity and Pseudonymity	ICPP: Christian Krause, Henry Krasemann, Martin Meints
3. Virtual? Identity	VIP: Bernhard Anrig, Emmanuel Benoist, and David-Olivier Jaquet-Chiffelle
4. Tracing at Identity of a Money Launderer	LSE: Ana Isabel Canhoto and James Backhouse
5. Tracing the Identity of a Terrorist Financer	LSE: Ana Isabel Canhoto and James Backhouse
6. Identity and Privacy in the Context of Civil Law: Case law on Recoverable Anonymity	VUB: Wim Schreurs
7. Identity and Privacy	KU-Leuven: Claudia Diaz
8. Ubiquitous Computing Scenario	Univ. of Reading: Mark Gasson, and Kevin Warwick
9. Identity in the Ambient Intelligence Environment	IPTS: Sabine Delaitre
10. The Role of Reputation and Privacy for Identities in Digital Communities	TU-Dresden: Sandra Steinbrecher
11. Identity in Digital Social Environments	INSEAD: Thierry Nabeth

Table of Contents

1 Introduction

1.1 Scope and objectives

"D2.2 Cases, stories and scenarios" represents the second document created in the context of the workpackage 2 of the **FIDIS Network of Excellence**, aiming at better understanding the "Identity and Identification" concepts.

Following the previous document "D2.1 Inventory of Terms", which identified the different terms found in the Identity domain and started to draft some definitions of these terms, D2.2 document consists in a short collection of cases, stories, scenarios, or perspectives in a particular application domain, linking the different Identity terms and concepts together in different contexts and according to a multidisciplinary perspective. The relatively informal form in which this content is presented (as narratives, scenarios, etc.) represents indeed a very effective means to propagate (McLellan, 2002), to elicit (Snowden, 2002), to capture, and to exchange complex ideas, but also to encourage collaboration, to generate new ideas and to ignite change (Denning, 2001; Lelic, 2002) in the FIDIS network.

The first aim of this document is to make the reader aware of the variety of identities issues, via the provision of concrete and comprehensible illustrations. Its focus is not however to indicate how these issues are to be addressed. A second objective is to collect very concrete and comprehensible materials from the different members of the consortium, that will be used later in FIDIS as reference materials helping to illustrate a particularly issue. The third aim is to facilitate inside FIDIS the construction of a common understanding between the partners, facilitating the emergence of collaboration. The final aim is to contribute to the generation of new ideas, and the circulation of these ideas both inside and outside the FIDIS consortium.

Each of these cases, stories, scenarios and perspectives has been contributed by a different member of the consortium that had the opportunity to illustrate an identity issue of its domain of expertise, and each of the contribution has been reviewed by at least two partners. In several cases, the contributions correspond to the follow-up of presentations that were given at the second WP2 workshop that took place at INSEAD, Fontainebleau, France, in December 2004. The contributions come under a variety of forms (short or long contributions, very schematical or only textual), a maximum freedom in this matter having been given to the authors in order not to limit their expressiveness. Finally, it is important to indicate that this set of cases, stories, scenario and perspectives is not supposed to be complete, and in particular it does not cover all the different domains that are concerned with identity issues, but only the few that the members of the consortium have considered to be the most significant.

1.2 A summary of the content

This document first start with two contributions providing a ***process and identity oriented perspective***.

The first contribution "*Scenarios and a story on Identity, Anonymity and Pseudonymity*" from ICPP, uses a story to explore anonymity services in the Internet and then illustrates with a scenario of an idealized web-based shopping system, the use of pseudonyms in various pseudonym domains. The second contribution "*Virtual? Identity*" from VIP, uses practical scenarios as a way to provide a comprehensible illustration of a unifying model for identities for the Information Society.

The next four contributions provide some examples and cases that belong more to the field of ***criminal investigation, law and society***.

"*Tracing the Identity of a Money Launderer*" and "*Tracing the Identity of a Terrorist Financer*" from LSE, provide very concrete examples, illustrating the different issues related to money laundering and the financing of terrorism. The contribution "*Identity and Privacy in the Context of Civil Law: Case law on Recoverable Anonymity*" from VUB, is about some case law related to identity and anonymity, and in the domain of the management of the protection of copyright in the music industry, and about the protection of anonymity and right to freedom of expression on the Internet. The next contribution, "*Identity and Privacy*" from KU-Leuven, provides a more society oriented perspective of anonymity and privacy, and in particular underlines and anticipates the consequences on privacy of the future developments of the Information Society.

The next two contributions explore a probable future of the Information Society with the ***Ambient Intelligent Environments***, and the potentially invasiveness of the technology.

"*Ubiquitous Computing Scenario*" from University of Reading, first describes the scenario of the loyalty cards as it exists today, and the risks that it already put on the privacy of the citizens. It then provides a more futuristic vision, describing the advent and the consequences of RFID on people identity. "*Identity in the Ambient Intelligence Environment*" from IPTS, illustrates very concretely some of the experiences people will have in ambient intelligent environments, and in particular how a bar might look like in 2012 and how people might interact within this environment with "smart objects" and with people.

The last two contributions provide a perspective of identity in the existing ***digital environments*** of today, as well as some outlook about how they will evolve in the future.

"*The Role of Reputation and Privacy for Identities in Digital Communities*" from TU-Dresden, explores the role of reputation (a particular facet of people identity) in digital communities and its consequence on the management of the identity in these environments. It illustrates this with the example of eBay. Finally "*Understanding the Identity Concept in the Context of Digital Social Environments*" from INSEAD, provides the even broader view of concept of Identity in the Digital Social Environments, with a strong sociological orientation. Besides illustrating the different categories of digital social environments and identity issues with examples, it indicates the benefit of integrating social mechanisms in the management of identity.

1.3 Results, conclusion and future work

In this document, we have given to the authors the maximum of freedom and we have tried to avoid imposing them a particular form or a structure for their contribution. Indeed Identity is a domain that is very new (in particular in an online situation) and still subject to important evolutions. We believed it was important not impose constraints, so as to let the "creativity" of the author express as much as possible. The only requirement asked was that the authors provided concrete (even if they are imaginary) illustrations of situations reflecting important aspects related to identity, and to have a descriptive rather than an analytical orientation. This last point was intended to avoid entering into presentations that would become too theoretical and difficult to understand outside an audience of specialists, and would limit its diffusion[1]. Finally, for the same reasons each contribution should be self-contained so that it could easily be diffused separately.

As a result, we have collected in this document a set of contributions that are presenting a variety of Identity issues that cover many dimensions of the Identity domain (societal, legal, social, etc.), principally from an usage/practice perspective. The result of this collection may appear as a patchwork of "things" (concepts, ideas, and issues) related to Identity not necessary very well connected with one another. However, although if we consider that one of the reasons of this "chaos" originates from the method we have employed, we believe that another more profound reason is that this reflects the state of the current situation of the Identity domain: many different things, from many different domains, and a real difficulty to get a global picture and to articulate the different domains with one another.

Yet, this document proved helpful opening the opportunity of creating some bridges between the different disciplines. For instance we were able to assemble in a single document and in a comprehensive way many perspectives which should help us in our goal to build a more global picture of Identity in the Information Society. We believe this is an interesting achievement, even if additional more systematic and more explicit analysis could be beneficial (but with the risk of constructing a "cathedral", and of losing the audience of the more ordinary people). We also put a relatively strong emphasis on the legal requirements & issues (which is an aspect often overlooked in general documents), and more generally the articulation between formal rules (laws, guidelines, etc.), and the way that the world functions effectively (rules may exist, by may not be applied adequately). For instance, in several cases it was shown that law could exist and was adequate, but had some difficulty to be applied into the reality even with the tool managing this identity (for instance in the case study: the City PA presented in chapter 4.5 of the case of the money launderer, the application of the law took some time because the criminal "did not fit the typical money launderer profile"). Still, we have found that the identity "tools", given the transparency that they provide, can represents a formidable means to re-enforce formal laws (sometime with some risks at attainting the privacy of the person as indicated in chapter 7), or the informal rules (for instance chapter 10, "The Role of Reputation and Privacy for Identities in Digital Communities, TUD" indicates the strength of an informal social process such as reputation to enforce rules). The two chapters on Ubiquitous and Ambient intelligence of this document by

[1] Very elaborated documents which are targeted to an expert audience are already largel

giving us a glimpse on the future also proves that we are only at the beginning, and that the new "smart" and identity aware environments promise to transform radically the vision of the Identity in the digital society that we have now.

We do not want to over-analyse here, and do the contrary to what we have preached for this document, and we would like now to invite the reader to discover by himself/herself these different cases, and make his/her own opinion. We hope that this series of case –thanks to the multiple situation that were describes- will be at the starting point of some personal reflections and community discussion on the subject of identity, rather than definitive and closed overview of a subject.

The content of this document will be the starting point of a document (leaflet, etc.) that will be intended to a wider public audience. The main change in the new document (which title will have to be found), will consist in making it even more accessible and enjoyable to a larger audience.

1.4 References

Denning Stephen (2001); "The Springboard: How Storytelling Ignites Action in Knowledge-era Organizations"; *Journal of Organizational Change Management*, Vol 14, No 6, 2001, pp609-614

Lelic Simon (2002); "Fuel Your Imagination. KM and the Art of Storytelling"; *Knowledge Management*, 2001 / January 2002 issue

McLellan Hilary (2002); "Introduction to Corporate Storytelling"; http://tech-head.com/cstory1.htm

Snowden David (2002); "Narrative patterns: uses of story in the third age of knowledge management", *Journal of information and knowledge management*, 1 (1), 2002, pp. 1-6

2 Scenarios and a Story on Identity, Anonymity and Pseudonymity, ICPP

Christian Krause, Henry Krasemann, Martin Meints, ICPP

As Independent Centre for Privacy Protection (Unabhängiges Landeszentrum für Datenschutz) we are especially interested in privacy-protecting aspects of Identity Management and Identity Management Systems. We understand anonymisation and pseudonymisation basically as privacy-protecting mechanisms in Identity Management Functions and Systems. To clarify this we contribute a story on anonymity services on the Internet and a scenario of an idealised web-based shop system using different pseudonyms in various pseudonym domains. The last scenario shows how privacy-invasive GUIDs in the context of a personalised recommendation system could be replaced by a less invasive solution.

In general our view is focused on technologies and processes to show how privacy protection works or could work according to the European Data Protection Directive 95/46/EC. In addition many services are provided in countries where this Directive or European legislation in general does not apply, but privacy is regarded as a human right, and privacy principle such as the Fair Information Practices are spread around the globe. Please refer to chapter 7 (Identity and Privacy, KU-Leuven, scenarios from Claudia Diaz) to get an impression on possible society impacts of existing or missing privacy compliance.

2.1 Introduction

Using the Internet in a traditional way leads to many entries in a lot of log files e.g. at the ISP, proxies and servers. The stored information comprises the IP address, time of login and logout, cookies, headers sent by the used web browser etc. In many cases the storage of these log files is in accordance with the Directive 95/46/EC, for example when the data is needed for accounting purposes[2]. Thus, partial identities (i.e. personal data relating to the user) are stored at least for a certain time and can technically be processed without an additional agreement and the control of the person to whom they belong.

More in particular, three situations occur today: a) There is no agreement at all, the personal data are copied and used without compliance with data protection law: The data subject is not informed that his personal data are processed, does not know for what purposes the personal data are processed and of course did not give consent to process his personal data. b) There are general terms and conditions in a disclaimer that describe which personal data are processed for which purposes, but the data subject does not read these terms and conditions so that we have a hypothetical situation which does not always is in line with what is called the

[2] Often data storage is not compliant with local data protection legislation. Furthermore this data protection legislation in many cases needs interpretation in terms of the Internet. An exemplary issue is the question – maybe depending on the circumstances - whether IP addresses are personal data/personally identifiable information (PII) or not.

'reasonable expectation of privacy' of the user. Whereas situation a) is an illegal situation, situation b) is a legal situation which can be subject to critics. c) Even if the user is informed that his personal data are used for certain purposes (like profiling, transfer to third parties) and even if the user has read the general terms and conditions, he is often confronted with a de facto monopolistic situation in which he can not refuse the use of the data conform the general terms and conditions because, if he refuses, access to the goods and services on the website (or in the ambient intelligence environment) are denied …

These three situations all indicate that the steps described hereafter, should take into account an improvement of the actual situation and therefore, should take into account compliance with the regulatory framework (such as the Data Protection Directive 95/46 and the Privacy and Electronic Communications Directive 2002/58).

Furthermore, the linkability of those log file entries can lead to quite accurate profiles of the person that has used the Internet. On most websites the user loses a lot of functionality by trying to deny the storage of partial identities (i.e. personal data), e.g., via deactivating cookies or java-script in his web browser.

Looking at the physical world, anonymity in many facets of life is a basic right used every day and mostly by instinct. One example for that type of instinctive use of anonymity is a typical purchase: going into a shop, taking the desired goods and paying them with cash. As long as the money is real, the buyer is not asked for his name by the shop staff. The buyer stays anonymous and decides not to actively disclose identifying data[3].

Of course, in real life, people also want to have access to one's real identity under specific circumstances, e.g. in the case of criminal activities (theft, no payment, money laundering, …). In other words: Anonymity in the physical world seems to be no problem for commercial and social communications, but people however will like to have a possibility to revoke this (partial) anonymity if necessary.

We can see that we are de facto confronted with technologies and applications that do always not give the possibility to fully anonymously transact with digital interfaces. The obligatory digital identity card which is being introduced today in Belgium, the use of electronic money, biometrics and other technologies make it very difficult to communicate anonymously. This right to anonymity, which will be described in a further chapter on the basis of examples of actual case law, is in fact at the core of privacy and ICT discussions. Therefore, new models and business cases in ICT and Identity Management often accept the importance of revocable anonymity, indicating that also in a digital world a (technologically) revocable anonymity should be required.

The same purchase on the Internet leads to a lot of traces in databases of the ISP, the web shop, the bank and / or the operator of the payment system. The buyer leaves data related to his person to be able to perform the purchase and wouldn't know (at least in most cases) which data is taken, stored and how it is further used. The balance between the security of access to goods and services on the one hand and the security of access to the identity of the user on the other hand seems very difficult to achieve.

[3] In the off-line world, the physical appearance generally reveals biometric data such as the face or the voice, but these data normally are not stored and interpreted.

2.2 Story: Anonymity services on the Internet

This story shows how important anonymity can be when transferring commercial and e-government services via the Internet.

To use some services and to assert some civil rights, anonymity in the physical world is essentially needed. Examples are

- Some aspects of ballots / votes (especially the voting itself after being authenticated and authorised to vote) and
- Using crisis lines.

To guarantee anonymity, manifold special procedures and legislations are implemented in European countries.

However, by transferring such procedures to the Internet, anonymity often vanishes. By linking some stored data especially from the provider or the browser some essential personal data like the IP address at the time of the use of the services and sometimes even the name etc. can be determined.

To get over the loss of anonymity, some anonymising services on the Internet are being established. At the moment one of the best technical approaches offering strong anonymity is the use of JAP Anon Proxies to conceal the linkability between used IP address and selected website[4]. To anonymise client-related information like browser tags and cookies there are additional solutions available, e.g. the CookieCooker[5].

2.3 Scenario: Shopping using pseudonyms

Another mechanism to avoid profiling and linkability when two parties are involved in a transaction is the use of pseudonyms. This mechanism will be explained in this scenario which is derived from the Identity Management Systems (IMS): Identification and Comparison Study (ICPP, SNG, IPTS 2003)[6].

However, it should be noted that the use of pseudonyms cannot avoid profiling in all situations: The pseudonym, especially when it is (at least temporary) unique, can be profiled itself or used to build a profile. In other words, the right to use a pseudonym does not mean that you automatically have a right to prohibit the use of the movements and actions of the pseudonym to build a profile. On the contrary, there are laws which explicitly allow pseudonym-based use-profiles as long as it is not combined with data on the bearer of the pseudonym.[7] If your pseudonym is "black - 29 years - female – looking for a job", then a) a profile can be applied to the pseudonym and b) your actions and movements under that pseudonym can be recorded (anonymously) to enhance the profile that might apply to that pseudonym. When reading this scenario, one should take this into account.

---

[4] For more information about JAP Anon Proxies see http://www.anon-online.de/

[5] For more information about the CookieCooker see http://www.cookiecooker.de/

[6] Download: http://www.datenschutzzentrum.de/projekte/idmanage/study.htm

[7] See § 6 (3) German Teleservices Data Protection Act (Teledienstedatenschutzgesetz, TDDSG)

This scenario uses different pseudonyms in different contexts (so-called pseudonym domains) related to different steps of the purchase process to guarantee the buyer's anonymity (cf. Figure 1).

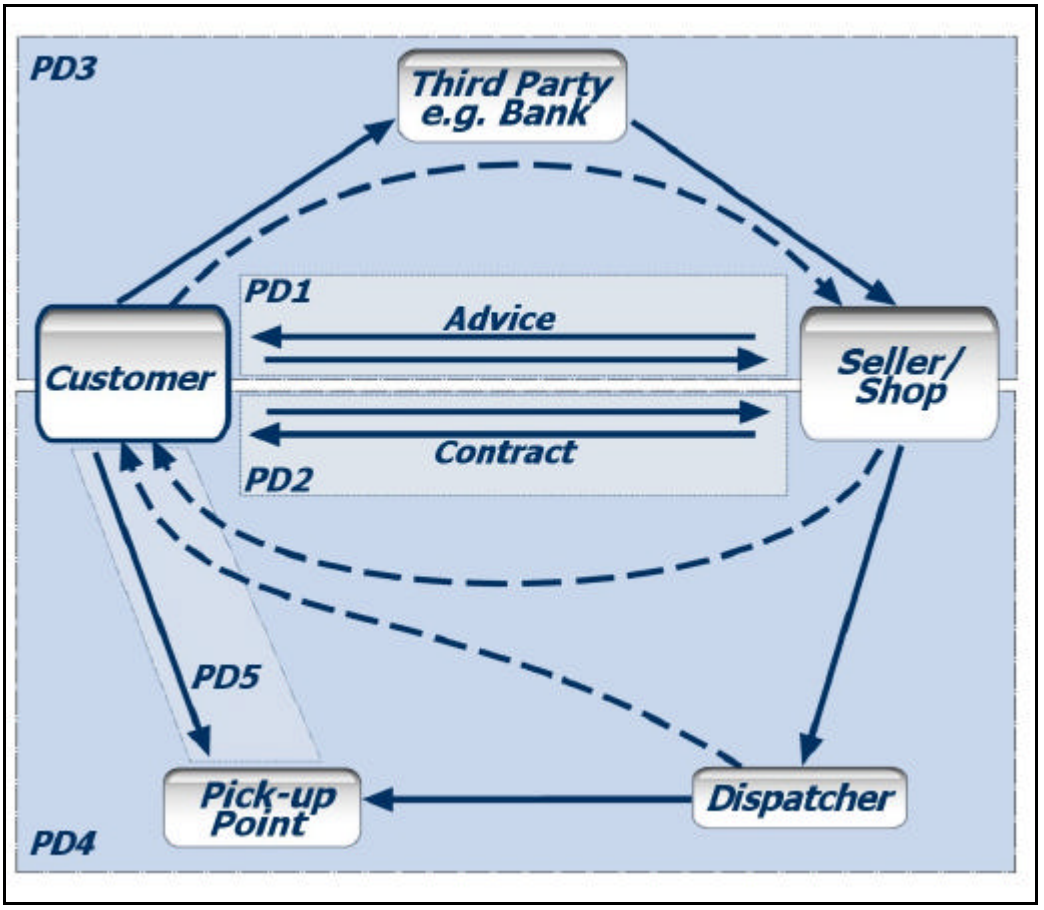


Figure 1: Steps and used Pseudonym Domains (PDs) in the shopping scenario

The first step in the purchase process is the consultation step. In this scenario the customers already use a pseudonym, which cannot be traced back to them (Pseudonym Domain 1).

For the actual purchase (step 2), a different pseudonym is used that cannot be related to the consultation pseudonym (Pseudonym Domain 2). This pseudonym may be linked to a certain reputation to assure the seller that the payment will be made. Alternatively, a special, individual pseudonym might be assigned with respect to each seller: Every time the buyer gets in contact with the seller, the seller-specific pseudonym is re-used in order to establish a reputation and at the same time to avoid the linkage of the customer's data with those at other sellers. As explained in the study, a personal pseudonym or the processing of customer data is not necessary for the demands of warranty services.

Of course, this is not always easy to achieve. When the goal is "to establish the reputation of a regular customer and at the same time to avoid a linkage of the customer's data with those at other sellers", this has to be built with explicitly taking into account actual practices of loyalty cards (see also further the chapter "8.3 *Current Technology: Loyalty Cards*" in this document)

that are often not stand-alone loyalty programs but interconnected programs: The customer can win points in different stores and shops, all part of the loyalty program.

To handle credentials of different sellers and to guarantee and possible perform the payment (step 3), a trusted third party (for payment usually a bank; Pseudonym Domain 3) can be used.

Even the shipment (step 4) can be carried out using pseudonyms. A possible solution could be the use of a pseudonym given by the customer which the seller cannot assign to personal data but which the company can assign to an address (e.g., iprivacy.com) (Pseudonym Domain 4). Alternatively, a pickup point where the buyer can collect the delivered goods after identity verification (password, PIN etc.) could be used (Pseudonym Domain 5).

2.4 Globally Unique Identifiers and databases

Globally Unique Identifiers (GUID) are bit strings (or character strings) which are coded into hardware, software or other data. Usually this bit string either is embedded in digital documents or transmitted during on-line communication. GUIDs can be used for the purpose of identification.

Especially in the private sector hardware and software is mainly used by one person or a small and homogenous group such as a family. Thus GUIDs enable indirect user tracking in many different ways. Therefore, GUIDs are widely discussed as being potentially privacy-violating. Upcoming technologies such as Digital Rights Management (DRM) are planning to make excessive use of GUIDs. Since data collections being associated to a single GUID usually are not known to the user, privacy and data protection regulations and thereby the right to informational self-determination might be violated

In the context of Digital Rights Management an increasing amount of Unique Identifiers is emerging. Documents as well as multimedia files are marked by their respective authors to trace duplication. In this case DRM is used to enforce the right of reproduction.

GUIDs empower others (mainly hardware vendors, software developers and holders of rights of digital documents in general) to accumulate information about users. Latest technologies like RFID (Radio Frequency Identification) even extend the idea of such identifiers: Usually GUIDs are thought of as being linked to on-line services. RFID technology blurs the borders between on-line and off-line world. Like being "tagged" with a cookie while surfing the Internet one may even leave linkable traces in the physical world while visiting a restaurant - provided the visitors wear an RFID chip somewhere in their clothing or accessory. Thus the idea of Unique Identifiers trespasses on the environment of direct computer usage.

Concerning privacy aspects, any identifier should fulfil the following requirements:

- Users must be informed about creation and usage of any identifier that can be connected to personal information (e.g., with respect to "smart dust"[8], the existence and possible design of "decent dust" which should inform the user in a proper way was discussed).
- The usage of the identifier and the correlated database entries must be transparent to the user.

[8] For more information about smart dust see http://robotics.eecs.berkeley.edu/~pister/SmartDust/

- Terms and conditions of usage of identifier-generated database entries must be documented; restrictions have to be enforced.

2.4.1 Scenario: Identity on your own - GUIDs, customer data and informational self-determination

The usage of GUIDs creates partial identities. They are based upon database entries that the user usually has no access to. Linking such GUID-based partial identities leads to more comprehensive data collections about the user. Users that are confronted with decisions made upon profiles generated from database entries may be surprised to learn what conclusion e.g. a company has drawn from these profiles.

Privacy-compliant use and building of profiles must primarily be transparent to the user. Traditionally the user transmits his GUID to the server, thereby revealing personal data. The server then delivers content personalised according to the user profile linked to this partial identity. Furthermore it adds information gathered during the actual session to the profile. From a privacy point of view the transmission of the GUID must not happen in the background without the user's knowledge. Also the linked profile should be in the domain of the user. In an idealised model, the profile would be stored on the user's computer or digital device. This way the information gathered is visible and even editable to the user. Technically there are some obstacles in this model:

- Stored data must be processed to derive actions from it. This data processing would have to be done on the user's device. Therefore program code would have to be transmitted to and run on the device. This is highly undesirable.
- Data processing can only be done when the user is on-line and enables services to access the stored data. The sending of a newsletter e.g. based upon specific user profiles would virtually be impossible.

Storage and processing of the complete user profile on the user's digital device therefore seems impractical.

Scenario: Download and usage of MP3 files

To illustrate how a privacy-compliant usage of GUIDs could be achieved, we'll take a look at some imaginary multimedia software that can play MP3 files. Therefore we assume that the vendor of the software provides a service to suggest commercial MP3 downloads based on the user's preferences. Playback of the MP3 files is done locally. The software gathers information about what is played, what is skipped and when playback is started and stopped. This leads to a user profile saved on the local machine. Whenever the user visits the vendor's website to download MP3 files, the stored usage profile is needed for recommending songs. The service provider specifies which specific data are needed, e.g., songs played and songs skipped, but not the postal address or the real name.

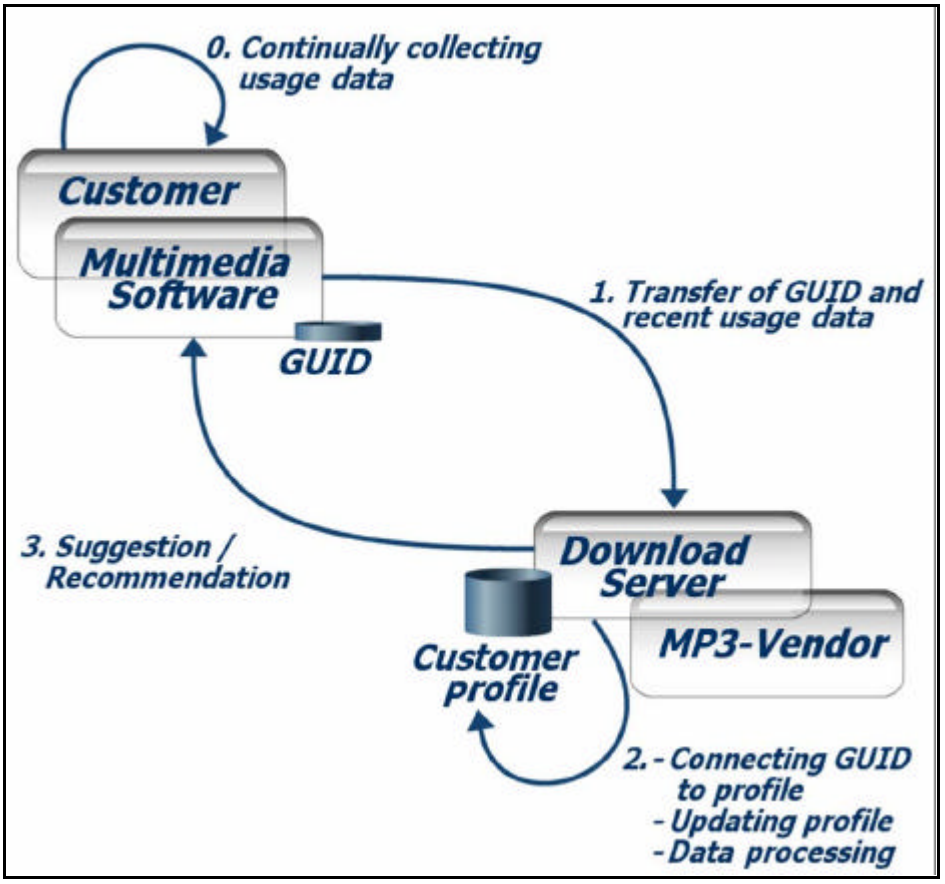


Figure 2: Current processing and storage of profiles using MP3 files

At this point, the user can decide if the data that are to be transmitted comply with his preferences. This can possibly be decided automatically via P3P-compliant declarations. After confirmation either by the user or by a P3P agent, the required data are encrypted and transmitted.

Digital Rights Management nowadays is widely understood as technology to enforce rights of authors to prevent unauthorised duplication and/or editing of digital documents in general. Taken literally, these technologies can also be used to defend the user's (digital) right of informational self-determination. Provided that service providers comply with privacy legislation in general and their own privacy policy in particular, profile transmission for data processing can be tagged for one-time usage. Other possibilities include permission for a limited time or limited amount of data.

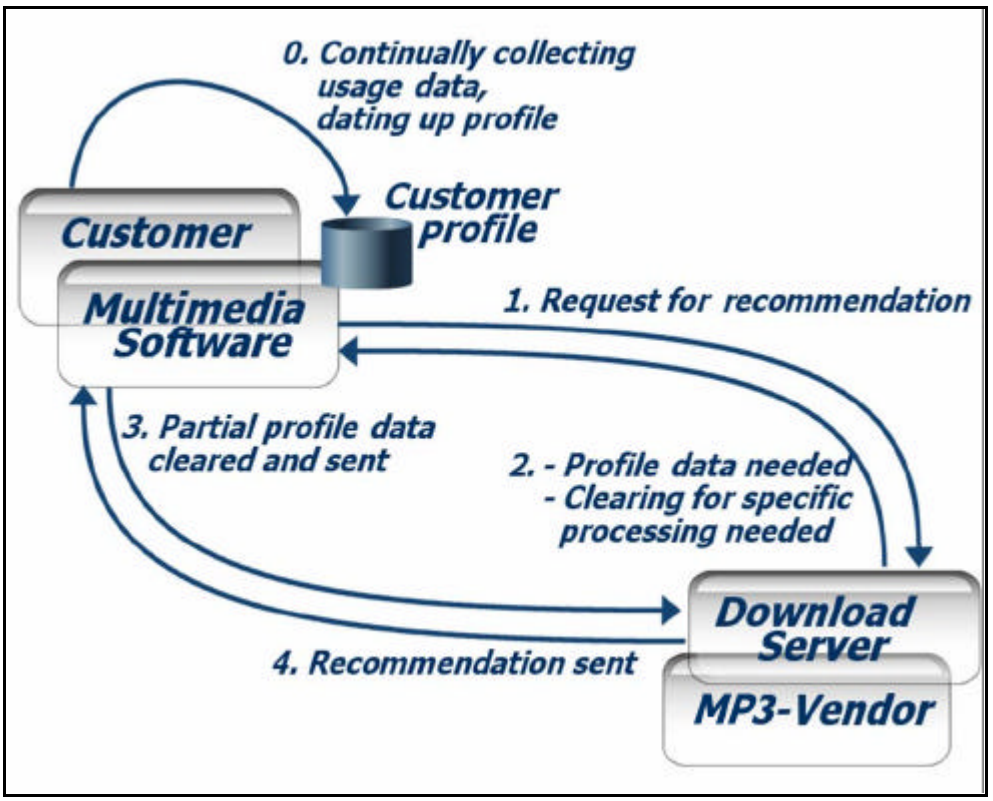


Figure 3: Privacy-aware processing and storage of profiles using MP3 files

So data collection is done entirely on the user's device, processing is done remotely by the service provider.

2.5 Conclusion

A central problem of the use of Internet is the storage of personal data in log files and databases. In many cases this is done in accordance with the Directive 95/64/EC basing on consent of the user or for specific purposes such as accounting purposes. A problem arising with this kind of storage of data is linkability and an increased possibility to profile persons.

Also in many cases it is debatable if a legally effective consent for storage and processing of personal data is given by clicking an "I agree" button on a web page.

The presented story and the two scenarios show how this situation can be improved using anonymity services or changed processes. Anonymity services can prevent linkability between data stored by an ISP and a different service provider on the Internet. The use of Pseudonym Domains when shopping could establish anonymity as it is usual when shopping in the physical world. And the usage of GUIDs for example in the area of DRM is not always necessary. Most GUID-based systems could operate much more privacy-respecting if user profiles were stored and controlled locally. The effort for changing the process to achieve more privacy compliance in our eyes seems to be acceptable. In addition this could be interesting for the suppliers of the services as well; privacy-respecting products today already

have a unique selling proposition in several markets, such as certain types of Identity Management Systems[9]. This could be extended to further markets and products.

[9] For an overview of Identity Management Systems, see: Matthias Bauer, Martin Meints, Marit Hansen (Eds.) (2005), "Structured Overview on Prototypes and Concepts of Identity Management Systems", FIDIS Deliverable 3.1, Version 1.1, September 2005; available on at the FIDIS web site: http://www.fidis.net/.

3 Virtual? Identity, VIP

Bernhard Anrig, Emmanuel Benoist, and David-Olivier Jaquet-Chiffelle VIP[*]

This chapter deals with two concepts that are linked together: identity and identification.

The aim is to present a unifying model for identities in the Information Society. This model is driven by practical applications: identification, authentication and authorization schemes. It provides unifying tools that allow a better description and understanding of the elements involved in these schemes.

We apply this model to some typical identification, authentication and authorization schemes in order to illustrate our approach.

3.1 Introduction

Many concepts evolve around the one of identity: identification, anonymity, pseudonymity, (un)observability, (un)tracability[10].

The aim of this chapter is to present a unifying model for identities in the Information Society. This model is driven by typical applications: identification, authentication and authorization schemes.

As a model it is not supposed to be definitive or universal; however, it fits very well with the current diversity of these schemes and we hope it to be broad enough to evolve and adapt itself when new schemes appear.

Our goal is not to cover all aspects of identity, this would be too ambitious. But we will present a set of unifying concepts and then use them to better understand and solve practical scenarios.

We will provide new definitions for these unifying concepts and we will illustrate these definitions with typical examples. For example, in our approach, pseudonyms are reduced to a special case of identity.

In this model, we attempt to define "identity" in the Information Society. Here, the identity clearly does not refer to the entire person anymore, but only to part of it. We should remember that, etymologically speaking, "person" comes from the Latin word "personae" which is derived from the Greek word "prosoopon" which means "mask". In a way, we will refer to the mask instead of the whole person itself. This approach will lead to a new core concept: the virtual persons.

In doing so, we do not cover existential questions like the ones related to the soul for example. We consciously restrict our view to the Information Society. The existence of a soul, feelings, etc. for people, animals or even programs is beyond the scope of this article.

---

[*] V.I.P – Virtual Identity and Privacy research center
Berne University of Applied Sciences, CP 1180, CH-2501 Bienne http://www.vip.ch; contact@vip.ch

[10] See FIDIS D2.1 (2005) for a description of the terms used in the Identity domain.

The same set of concepts is used to modelize the identity of a human being or the identity of a legal entity.

3.2 Virtual Persons

The goal of this section is to provide the basic definitions used in the next section to clarify the meanings of identity, identification and the like.

3.2.1 Definitions

In many countries, the law distinguishes two types of personalities: the physical persons and the legal persons. First we characterize both and then we present a unifying concept: the so-called "subject".

Definition 1 (Physical person) *A physical person is the physical mask of a human being.*

Note that we explicitly do not restrict our definition to living human beings as even dead people may have some rights, as for example the right to a decent funeral.

Definition 2 (Legal person) *A legal person is any personality which is recognized by the law of a country; it has rights and duties. It is often recorded in registers and has a legal status.*

A legal person can be for example a company, an organization or a community.

The next definition gathers together physical and legal persons, as well as everything that can —in some given context— be mistaken with such persons: for example *the wind* closing a door, or *the program* ejecting a member of a forum for using forbidden words, or *the dog* opening the door and breaking the plates.

Definition 3 (Subject) *A subject is any set of physical or legal entities having –in a given context- some analogy with a physical person.*

Here subject is not opposed to object. Indeed, physical objects can satisfy our definition of a subject. In our definition, subjects typically play a role; they look like the grammatical «subject» in a sentence as has been pointed out by Sarah Thatcher[11]. Our subjects *are*, they *have*, they *do* (or *behave*) or they *know something* just like physical persons.[12]

[11] Sarah Thatcher intervention at the Second FIDIS WP2 Workshop: "Theme: Relating the Identity Issues to the Real World", Fontainebleau, France, 10th December 2004, Url: http://www.calt.insead.edu/fidis/workshop/workshop-wp2-december2004/

[12] In contrast to (Pfitzmann and Hansen 2005) we require the analogy of a subject to the physical person.

Three basic classes of authentication technologies (cf. FIDIS D2.1 (2005)) are commonly considered

1. something you **know**
2. something you **have**
3. something you **are**

We want to introduce a fourth one:

4. something you **do**

Something you

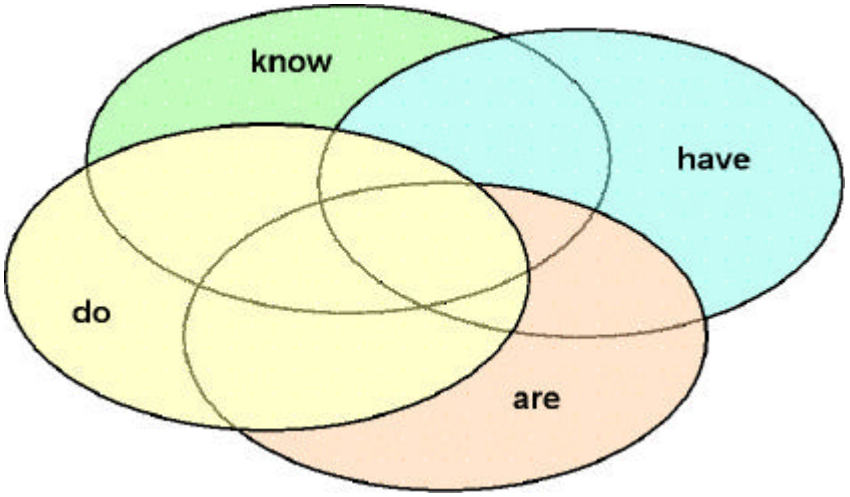


Figure 1: Classes of authentication technologies

We propose the following Cartesian representation to classify these four classes[13].

Table 1	*Attribute*	*Ability*
Role	**Are**	**Do**
Acquisition	**Have**	**Know**

[13] Thierry Nabeth, INSEAD, (http://www.insead.fr/~nabeth/) reviewed this paper and suggested to use a Cartesian representation.

In this table, the four classes of authentication technologies are characterized using four categories: attribute, ability, role and acquisition.

We present also the dual table, where labels and contents (i.e. categories and classes of authentication technologies) are exchanged.

		External	
	Table 2	*Have*	*Do*
Internal	*Are*	**Attributes**	**Role**
	Know	**Acquisition**	**Ability**

This puts into evidence two types of classes:

- internal classes (are, know)
- external classes (have, do)

The relations between these classes, their categories and their type are summarized in the following diagram:

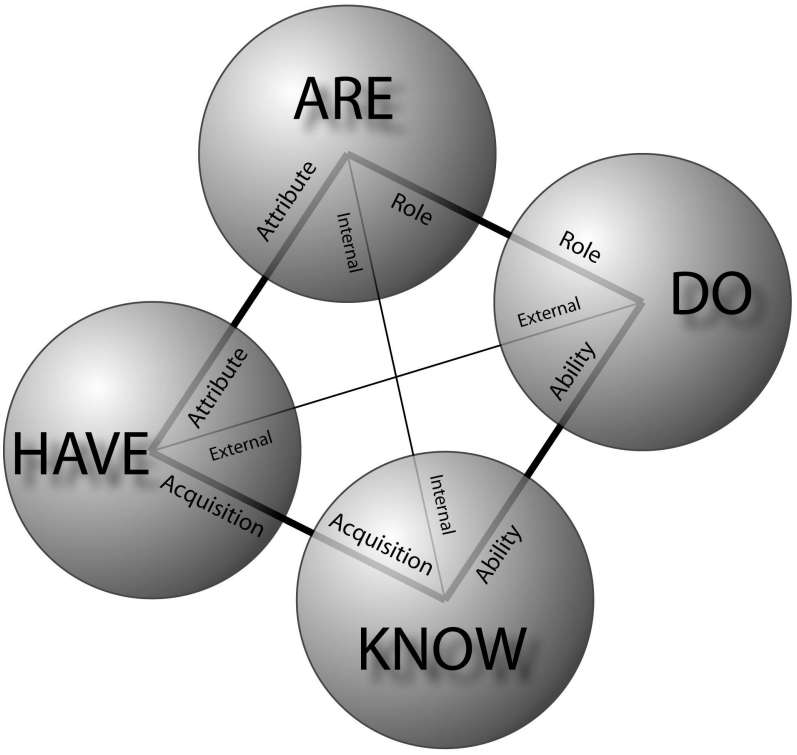


Figure 2 : Relations between authentication technologies

We will define the concept of *virtual person* while keeping in mind these authentication technologies. Indeed our definitions are "application oriented".

We observe that from a practical point of view, in most situations, a subject is accessed through a mask it is wearing. One subject can have many masks: one at work, another at home, with friends or with its banker. One mask can also be worn by many subjects: two people sharing the same computer have the same IP address. In some situations, the mask is transparent and the link between the mask and the subject is almost trivial. On the other hand, in other situations, it is difficult (or even impossible) to link a mask and the subject behind it.

However, from a practical point of view, it is enough to work with those masks, instead of the subjects, to achieve most of the tasks related to identification and/or authentication.

This is the main motivation to create and develop the concept of *virtual person.*

Definition 4 (Virtual Person) *A virtual person is a mask defined by its attribute(s), and/or its role(s), and/or its ability(-ies), and/or its acquisition(s). The entity behind the mask, if it exists, is a subject.*

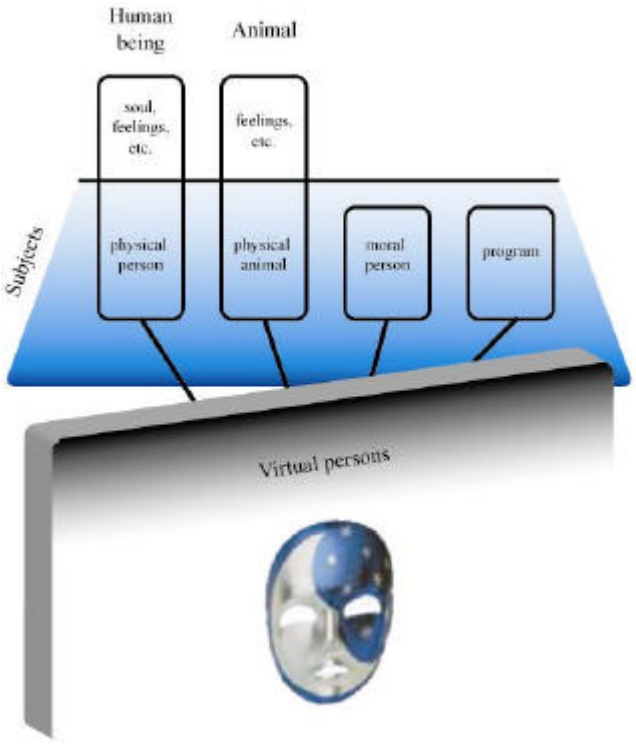


Figure 3: Virtual Persons

Fig.3 illustrates the fact that we often access a mask without any knowledge of the entity behind it. Do I talk to a single person or to a group? Is it a program or a person? Who/what did indeed close the door?

Note that the duality of tables 1 and 2 shows that we can also define a virtual person by what it knows, and/or what it has, and/or what it is and/or what it does.

3.2.2 Examples of Virtual Persons

In this section we present several examples of virtual persons. Note that a virtual person can be defined by one or more criteria.

Virtual persons can be defined by *roles*:

- **"Are"** (role & attribute) the President of the United States, the Pope, the Driver of the bus number 8, the first owner of a given car or the buyer in a given transaction.
- **"Do"** (role & ability) the person who opened the door, what has caused the door to close, the one who ejected you from the IRC forum, the person who killed JFK or the first man to walk on the moon.

In the last example, the virtual person did have some existence even before it was linked to an existing human, since it was already possible in the 50s to talk about him without knowing who he would be.

- **"Are & Do"** The instigator of a crime is defined both by it ***is*** and it ***does*** (or have done). So is the actress playing the role of catwoman.

Virtual persons can be defined by *acquisitions*: in particular, we can define a virtual person by its knowledge or what it has.

- **"Know"** (acquisition & ability) The one who knows my credit card's PIN code, the one who knows the private key corresponding to a given public key, the one who knows who killed JFK.
- **"Have"** (acquisition & attribute) The holder of my cell phone, the shareholder of 51% of the shares of a given company, the one who holds some token, the holder of your credit card...

Any *attribute* can also be used: the owner of a fingerprint, the person in front of whom I stand, the tallest person in the world.

The same is true for any *ability*: the one who can break the system, etc.

3.3 Identity and Identification[14]

3.3.1 Identity

In the following we refer to a community of reference. Such a community *C* is either a set of subjects or a set of virtual persons.

Definition 5 (Identifier) *An identifier* I *is a set of information.* I *is an identifier w.r.t. a community* C *if and only if there exists a unique element in* C *that is compatible with* I.[15]

[14] See FIDIS Deliverable 2.1 for a discussion on the relations between identity and identification.

For example:

- *Dad* is an identifier in my family,
- *Fingerprints* are supposed to be identifiers w.r.t. the world population,
- *BIE1* is an identifier w.r.t. the people working at the Berne University of applied Sciences and
- A *pseudonym* can be an identifier w.r.t. the virtual persons active in a chatroom; it may not be relevant outside of it (where other people use the same pseudonym).

Definition 6 (Identity) *An identifier* I *with respect to a community* C *is an identity of* P *with respect to the community* C *and according to an observer if and only if this observer can link* I *to the element* P *of* C.[16]

Note that according to these definitions, an identifier is independent of any observer whereas an identity always depends on the observer.

For instance, a valid 4-tuple containing name, first name, date of birth and address is an identity of some physical person living in Switzerland for almost any observer in Switzerland. On the other hand, BIE1 is an identity with respect to the employees of the BFH only according to the observers knowing the abbreviation scheme. A so-called Cookie on the Internet is an identity of the virtual person «the one using this browser on this machine» with respect to the users of a web site, according to the administrator of this web site. For most other observers this might be just an identifier.

3.3.2 Identification

Definition 7 (Identification) *Identification is a process done by an observer; identification means the process of linking a virtual person to another virtual person or to a subject.*[17]

In the identification process, the observer must answer two questions

- Do I trust the *existence* of a link?

---

[15] This definition of an identifier is compatible with the one from (Kent and Millett 2004), but we think that it is necessary to require identifiers to be defined with respect to communities.

[16] The definition of identity has some parts in common with (Pfitzmann and Hansen 2005) and (Kent and Millett 2004), yet we stress the necessity of an (explicitly defined or implicitly known) observer with respect to this very definition, in the sense that the observer must create, verify, etc. the link. In (Pfitzman and Hansen 2005), the term "attacker" is used for a subject interested in monitoring communications etc.

[17] This is in the sense of the attribute-based definition of (Kent and Millett 2004): "Identification is the process of using claimed or observed attributes of an individual to infer who the individual is". Again, we think that the observer is a key concept in the process of identification.

- Do I trust the *non-existence* of a link?

There are three[18] cases (Fig.4):

- *yes / no* I am convinced that both entities are linked
- *no / no* I don't know
- *no / yes* I am convinced that both entities are not linked

The thresholds used in this process to make a decision depend on the application.

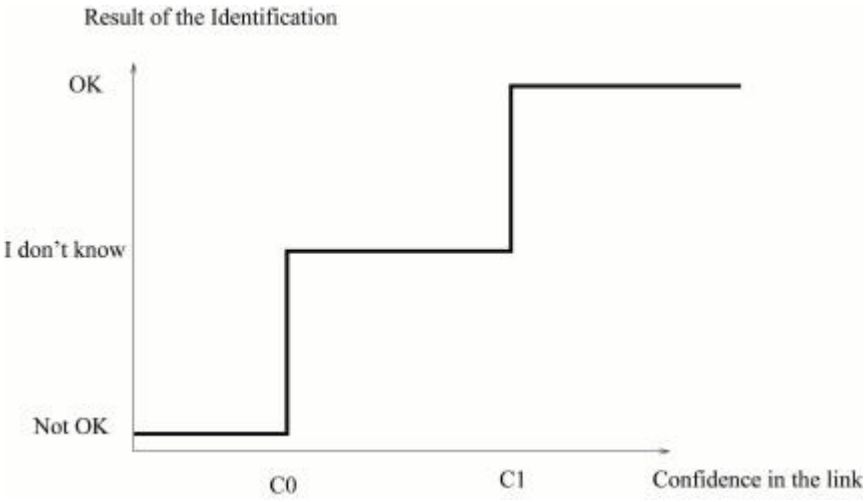


Figure 4: The three cases

For the identification of a client by the doorkeeper of a bar, C1 is quite low. On the other hand the confidence in the identity of the person launching a nuclear rocket has to be much higher.

The identification as introduced above leads to two generic cases:

- validation of a claimed link (verification of an identity)
- search for existing links (search for matches)

3.3.3 Use Cases

3.3.3.1 Verification of an Identity

We present two typical examples for such a process; of course many more can be thought of.

[18] Note that answering yes to both questions is nonsense.

Login on a System Consider the classical problem of the identification of a user by a server. The user wants to have access to a computer system and tries to identify itself with its username (FRODO) and its password. Let's consider this situation from the point of view of the server (here the actual observer), which has to grant the access (or deny it), cf. Fig. 5.

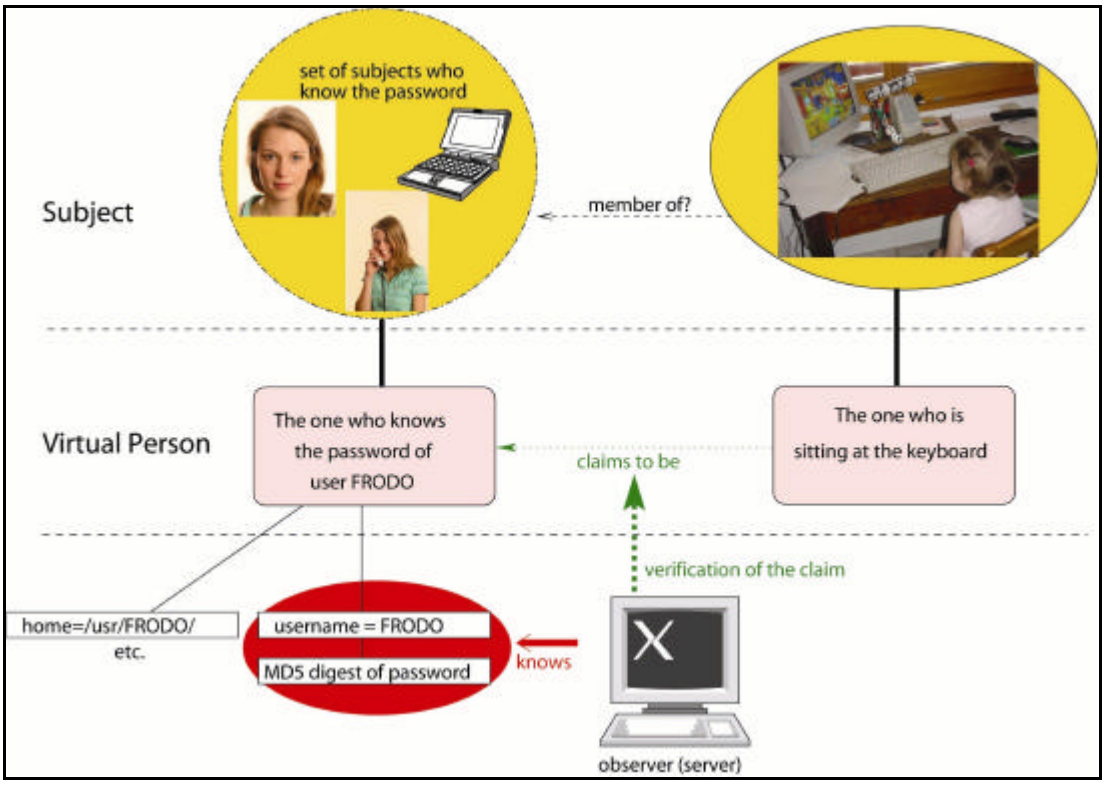


Figure 5: Login on a system

The server has to deal with two initially distinct virtual persons: the first one is the virtual person “The one who knows the password of the user FRODO”, the other one is the virtual person “The one sitting at the keyboard”. Moreover, the observer has access to some information tautologically identifying the first virtual person, e.g. an MD5 digest of FRODO's password. The second virtual person claims to be the first one. Here the server has to check this claim, and usually will do this by asking to provide the password. The level of confidence of the server in the existence of a link between both virtual persons is high enough if and only if the password is correct.

Note that the server can never be sure of the real existence of this link. But to give access to the resources, it is only necessary that the level of confidence in this link be high enough.

Border Control Consider the situation where you stand in front of a guard at a border, cf. Fig. 6. Usually the guard will ask you to show your passport in order to "check your identity". More precisely, here again, several entities interact: the guard at the border acting as the observer, the virtual person "The one described by the passport" and the virtual person "The holder of the passport".

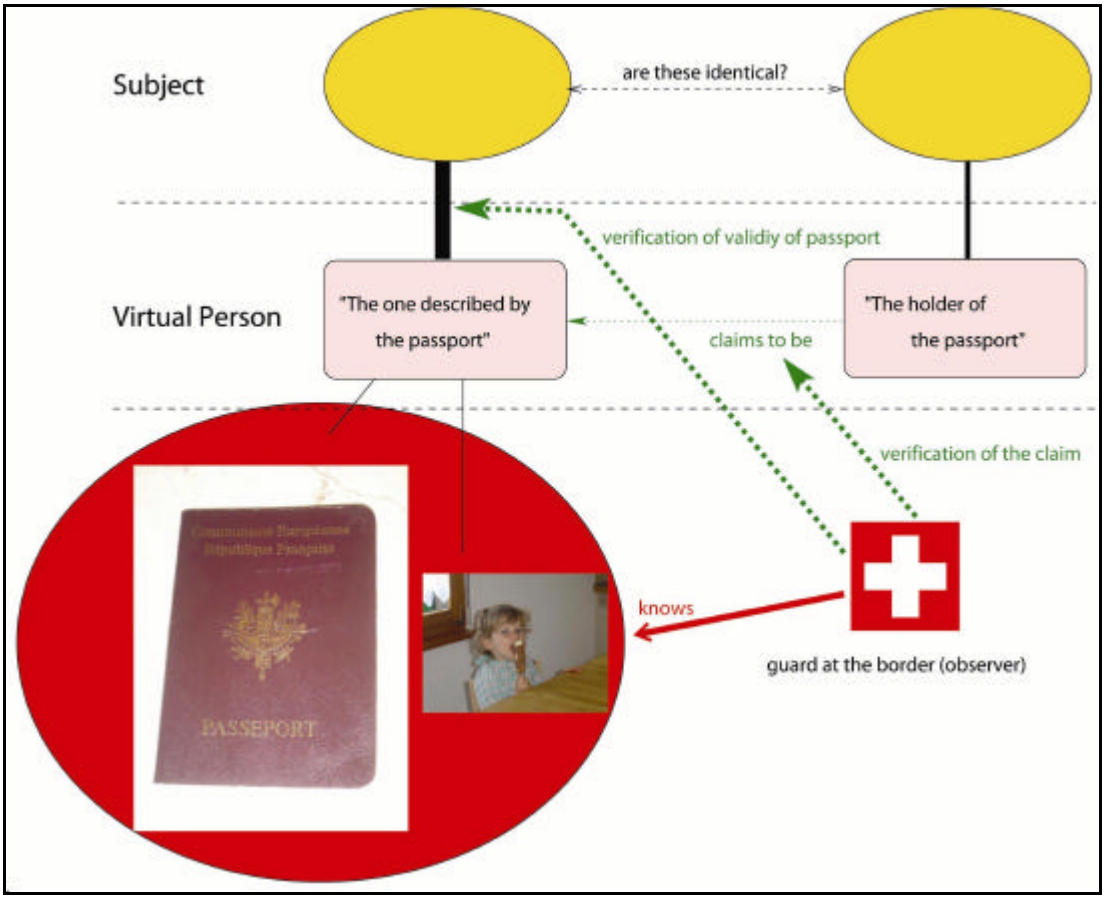


Figure 6: Border Control

Often, the guard will make two different tests:

1. First, he will try to figure out the validity of the passport; in a way he tries to check the validity of the link between this passport and a subject.
2. Then, he will check the existence of a link between both virtual persons, using the information available in the passport: a photo or some biometric data.

3.3.3.2 Search of a Link

The following examples deal with the second kind of identification: search for a possible match between one given virtual person and members of a community of virtual persons. For example, which member of the community matches «best» the given virtual person.

Typical examples: Who is the murderer? To whom do these fingerprints belong? Who is the tallest person in this room?

Chat: Whom do I talk to? You know that your friend Alice spends a lot of time in the evening chatting in a chatroom on the Internet. You know very well which chatroom she's usually in, and therefore on a Saturday evening, you decide to enter the same one. Several virtual persons are already in the chatroom, and you would like to know behind which pseudonym your friend Alice really is, cf. Fig .7.

The pseudonyms used in the chatroom are tautological identities of the corresponding virtual persons.

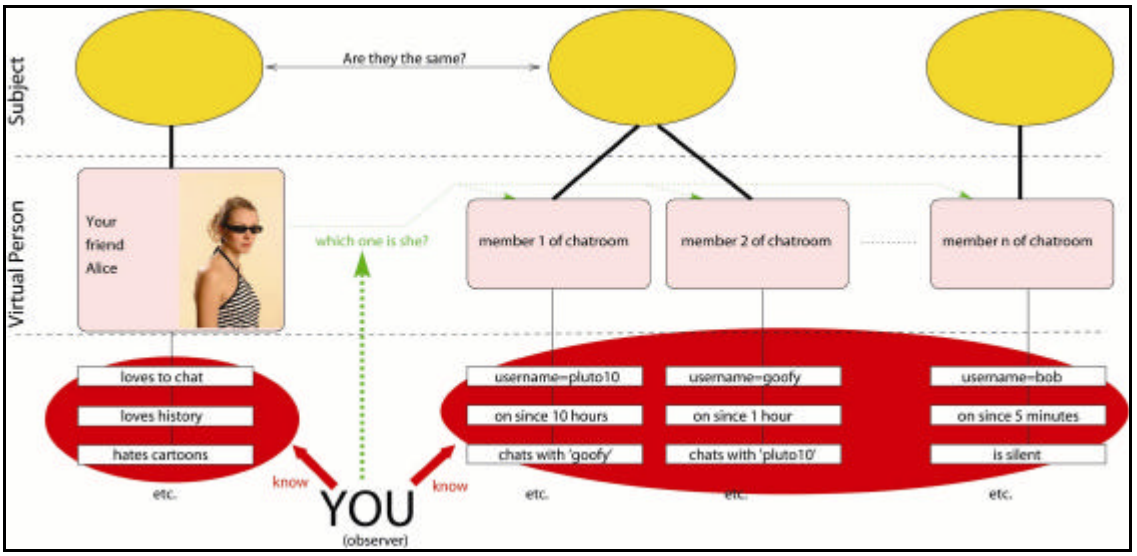


Figure 7: Whom do I talk to in this chat?

In this situation, you are the observer of the situation and the community is the set of virtual persons currently active in this chatroom. You know well the virtual person "My friend Alice" and have some information about her. In the chatroom, there are actually *n* different virtual persons, each one having a name (pseudonym) and some other attributes which are visible to you: for example, how long he/she has been in the chatroom, as well as the partners one specific virtual person is chatting with. You can even eavesdrop on some of the conversations going on and get information thereof. Your goal, as the observer, is now to select the virtual person(s) in the chatroom which you think matches "My friend Alice".

In an optimal situation, you find only one virtual person that matches Alice's profile with high probability from your point of view; but in other cases you might not be so sure. Note that in

Fig. 7, there are two virtual persons, members 1 and 2 of the chatroom, which belong to the same subject. Such a situation is clearly possible.

What's her name? Now consider the following common situation: a woman is standing in front of you and you know very well you have met her a long time ago but you can't remember her name, cf. Fig. 8.

You quickly go through your memory and try to match one of the virtual persons you've met before with the virtual person "Person now standing in front of you". Again, in this situation, you are the observer trying to get a link that you can trust while eliminating all the other ones.

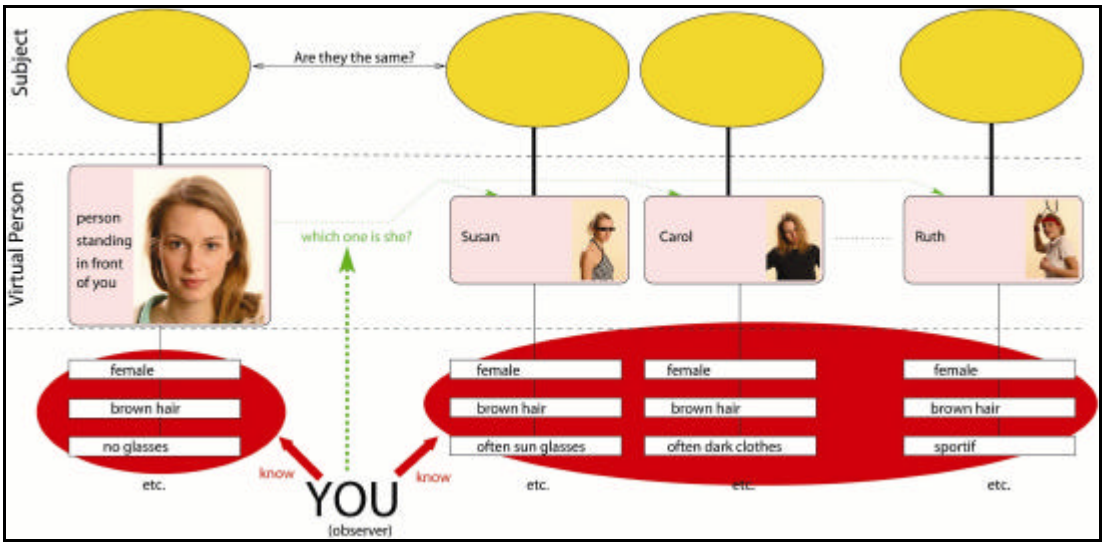


Figure 8: What's her name?*

3.4 Conclusion

The concepts defined in this article, especially both concepts of subjects and of virtual persons, allow a better description and understanding of many identification, authentication and authorization schemes, by creating a generic model. We have seen that we can apply this model in a diversity of examples: username/password, border control, finding someone in a chatroom.

The concept of virtual persons allows a unified handling of (currently) existing and/or non-existing subjects, even if the subjects are of different types. It serves as a basis for the definitions of identity, identification and the like.

Pseudonyms become a special kind of identity. Authentication and authorization schemes become a special case of identification in our unifying model. Indeed, identification is not always linked to a subject anymore.

* Pictures of the woman in this paper are copyrighted. Christoph Edelhoff has granted us the right to use them.

From a practical point of view, most identifications actually occur between virtual persons.

3.5 References

FIDIS D2.1 (2005), "Del. 2.1: Inventory of Topics and Clusters", FIDIS deliverable 2.1, September 2005; available at the FIDIS web site: http://www.fidis.net/

Goodman, David, editor (2004); "Towards understanding Identity", eema, the independents european association for e-business www.eema.org.

Kent, Stephen T., and Lynette I. Millet, editors (2004); "Who goes there? Authentication through the lens of privacy", The National Academic Press, Washington DC.

Pfitzmann, Andrea and Marit Hansen, editors (2005), "Anonymity, unlinkability, unobservability, pseudonymity, and identity management – A consolidated proposal for terminology", http://dud.inf.tu-dresden.de/Literatur_V1.shtml

4 Tracing the Identity of a Money Launderer, LSE

Ana Isabel Canhoto and James Backhouse, London School of Economics.

4.1 Introduction

In the information society, almost every aspect of daily life – from magazine subscriptions to financial transactions - is subject to being captured and incorporated in a database. The electronic traces are then used to develop models of who people are and what they do which, in turn, are used to inform decision-making in a variety of areas. One such area is crime prevention and detection, and this paper describes how profiling is used in the fight against money laundering.

4.2 Money laundering: definition and methods

Money laundering refers to the processing of the financial proceeds resulting from criminal activity. It includes any type of predicate crime ranging from tax evasion and forgery, to drug- and people-trafficking. It is assumed that the criminal will want to disguise the illegal source of the money, while trying to maximize profit[19].

In practice, the money launderer tends to commit various forms of crime – for instance, smuggling and tax evasion will occur simultaneously because the person who brings goods to a country without declaring them to customs is also unlikely to pay taxes on the profits of such activity.

The cast of characters in the world of money laundering is varied, and ranges from individual criminals that launder the money themselves, to the highly sophisticated organised crime group that has its own "financial director". The type of launderer will be determined by a number of factors, such as the volume of money to be processed or the type of predicate crime committed[20].

Regardless of who intervenes in the actual task of laundering the proceeds of crime, the underlying principle is, in the words of the National Crime Intelligence Service (the British Financial Intelligence Unit): "*Most organised crime is not worth anything to a criminal unless they can launder the money. A high percentage of criminal gangs has money laundering as a secondary activity*"[21].

Being an illegal activity, there are no official measures of its size – but, estimates from the International Monetary Fund suggest that the volume of funds being laundered every year is in the range £500 billion to £1 trillion worldwide.

---

[19] Since 2001, this definition has been extended to include the financing of terrorist activity, a practice referred to as "reverse money laundering". Due to the different nature of the activity, however, the topic of terrorism financing is discussed in a separate paper.

[20] A thorough description of the typology of money launderers is available in Bell, R. E. (2002) "An Introductory Who's Who for Money Laundering Investigators", Journal of Money Laundering Control, 5 (4), pp. 287-295.

[21] http://www.assetsrecovery.gov.uk/downloads/newsletter1.pdf

Money launderers will use both the financial and the non-financial system to launder their money. The method involves three stages:

- *Placement* – When the money is introduced into the system. It will involve, for instance, the breaking up of large amounts of cash into smaller sums that, being less conspicuous, are less likely to draw the attention of the intermediary. Another possibility is the recycling of cash as revenues of a 'front' business;
- *Layering* – A series of transactions to distance the funds from their source or destiny. This may be achieved through the purchase and sale of investment titles, for instance, or simply by transferring funds through a series of accounts or intermediaries across the globe. In some instances, these transfers may be disguised as payments for goods or services to give them a legitimate appearance;
- *Integration* – When the funds re-enter the legitimate economy. For instance, through business ventures and the payment of tax.

Money laundering causes major economic and social disruption, which is why national governments and international organizations alike invest considerable resources in tackling the problem.

4.3 Tools for Anti Money Laundering

One key component of the fight against money laundering is emerging in the development of models of who money launderers are and how they act. The objective is not only to detect those engaging in criminal activity - leading to the imprisonment of those individuals and/or the seizure of their assets - but also to prevent future occurrences of the crime.

The modelling usually encompasses the use of automated monitoring tools - powerful algorithms that sweep through the records stored in transaction databases looking for those patterns of financial behaviour that deviate from the norm. The transactions flagged by the monitoring software are then subject to scrutiny by a human agent (e.g., the employee of a bank or financial intelligence unit) in order to separate those transactions that are merely unusual for a specific customer from those that are, indeed, suspicious. The unusual behaviour only becomes a source for concern when there is no known legitimate source for the income or the observed lifestyle does not fit the one expected from someone with a specific legitimate economic activity: a sudden peak in a butcher's bank account may be due to the sale of a house rather than the reward from some criminal activity, for instance.

It is crucial for financial investigators and other anti-money laundering agents to command a holistic picture of the identity of each person flagged by the automated monitoring systems, as discussed in the next section.

4.4 The various components of identity

There are many aspects that contribute towards the identity of a person. In particular, the following four components of identity can be considered:

- *Socio-demographic characteristics* – Includes characteristics such as gender, age, ethnic group, household size, or employment status. It is based on the premise that demographic groups are relatively homogenous and lends itself easily to quantification, measurement and classification. Additionally, it is difficult to falsify unless a false identity is being used. However, profiling on the basis of socio-demographic characteristics leads to emphasis on the "usual" suspects and may be discriminatory against minority groups in society; indeed profiling has a distinct pejorative notion in North America for this reason.
- *Benefit sought*[22] - The benefits desired from pursuing certain behaviour, including the underlying motivation. It focuses on common values and attitudes across cultural groups. It may be extremely difficult to observe and is not suitable to assess individual, rather than group, behaviour.
- *Lifestyle adopted* - Focusing on options made regarding travel patterns, or the type of goods and services acquired, for instance. This factor potentially offers the most insight regarding how the money is acquired and spent.
- *Behaviour exhibited* – In relation to the financial institution. That is, based on data resulting from actions of the account holders, such as length of relationship with the bank, modes of payment and shopping preferences, product ownership, and contributions to political, religious, and charitable groups. An underlying assumption prevails that past or current behaviour offers the best predictor of future behaviour. It is very useful in anti-money laundering but easy to falsify and often difficult to measure.

The ability to construct a profile based on one or more of these four aspects, however, is subject to the technical limitations of integrating different data bases and the legal frameworks aimed at protecting the privacy rights of individuals. Additionally, it is crucial to see through the "noise" created by money launderers with the purpose of disguising the origin of the funds – for instance, the division of the sum to be processed in small amounts, or the use of intermediaries who intervene in parts of the process and who tend to change frequently.

The next section exercises a case recently discussed in the British press to illustrate how the four components discussed above contributed to the development of the subject's identity as a money launderer.

4.5 Case study: the City PA

In the spring of 2004, Joyti De-Laurey, a personal assistant at Goldman Sachs in London, was convicted of stealing £4.3m from her bosses, through fraud and forgery, and laundering the proceeds of her crime with the help of her mother and her husband (a 50-year-old former chauffeur).

De-Laurey's gross salary with bonuses amounted to £42,000 a year[23]. Yet, during her time at Goldman Sachs, she acquired, among other things, a £750,000 seafront villa in Cyprus, £500,000 worth of furniture, £400,000 in jewellery, several top of the range cars and a

[22] Also referred to as psychographic profiling
[23] http://news.bbc.co.uk/1/hi/england/london/3629087.stm

£150,000 power boat[24]. The gap between her known source of income – a socio-demographic characteristic - and her exhibited lifestyle was enormous and led to alarms being raised by several financial institutions. This picture was compounded when, in court, it was revealed that De-Laurey was planning to start a new life with her family in Cyprus, and she had described herself on a school registration form[25] as a banker – an indication of the benefit sought with the behaviour pursued. The string of cheques with forged signatures being deposited into her account and, later, the transfer to Cyprus was considered suspicious behaviour. Similarly, the pattern of transfers between De-Laurey's bank accounts and those of her husband and mother implicated them in the associated money laundering charges.

The components of identity were used in order to identify De-Laurey and her associates as money launderers. The construction of someone else's identity is, however, not an objective process; rather it is one subject to the prejudices and judgement of those who engage in the identity construction exercise. Several suspicious transaction reports were filed against De-Laurey, yet the case of her being a money launderer took some time to build because, in the words of a financial investigator interviewed by the authors, she *"did not fit the typical money launderer profile: man, white, 40 years old"*.

[24] http://news.bbc.co.uk/1/hi/england/london/3614597.stm
[25] idem

5 Tracing the Identity of a Terrorist Financer, LSE

Ana Isabel Canhoto and James Backhouse, London School of Economics.

5.1 Introduction

The United Nations defines terrorism as the activity carried out "to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act"[26]. The report of the High-Level Panel on Threats, Challenges and Change, published in early December 2004[27] highlights that in today's interconnected world a threat to one state's security is a "threat to all". The report also mentions that terrorism has important economic consequences, as illustrated by the terrorist attacks of September 11th 2001, in the Unites States which, according to World Bank estimates, cost more that $80 billion dollars and pushed 11m people in developing countries into poverty[28].

Financial intelligence – that is, the collection and analysis of financial data - is gaining importance as a key tool in the war on terror. The monitoring of financial transactions carried out by individuals and organizations, together with complex profiling models, facilitate the identification and detection of terrorists, as discussed in this paper.

5.2 Terrorist financing: definition and methods

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity.

A terrorist group, like any other criminal organization, builds and maintains an infrastructure to facilitate the development of sources of funding, to channel those funds to the providers of materials and or services to the organization, and, possibly, to launder the funds used in financing the terrorist activity or resulting from that same activity.

Terrorist organizations derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income. The forms of financing can be grouped in two types:

- *Financial support* – In the form of donations, community solicitation and other fundraising initiatives. Financial support may come from states and large organizations, or from individuals.
- *Revenue generating activities* - Income is often derived from criminal activities such as kidnapping, extortion, smuggling or fraud. Income may also be derived from legitimate economic activities such as diamond trading or real estate investment.

The terrorist financer will want to disguise the illegal end of the funds, while trying to maximize the revenues for the organization sponsored. It may be necessary to disguise the source of the funds, as well, either because such funds have an illegal origin, or because the

[26] Article 2 of the International Convention for the Suppression of the Financing of Terrorism
[27] Available at www.un.org/secureworld
[28] Annan, K. (2004) "Courage to fulfil our responsibilities", The Economist, December 4th 2004

organization wants to preserve the continuity of the legitimate financing. The need to camouflage the source of the funds means that terrorist financing has certain similarities with traditional money laundering, namely the use of three stages[29] to place, layer and integrate the funds in the international financial system.

There is a crucial difference between traditional money laundering and terrorist financing, however. The monitoring of financial transactions in traditional money laundering, from a financial investigator point of view, is done in order to link the funds to a criminal act that has taken place already and to strip the criminal and any accomplices from the economic benefits of engaging in criminal behaviour. In terrorist financing, however, the investigation is done in order to prevent individuals to gain access to funds that could finance future criminal activity and, therefore, it is done in order to prevent a crime from happening. The monitoring of financial transactions with the purpose of identifying terrorist financers, therefore, must take into account the intentions of those engaging in the financial transactions observed.

5.3 The role of social networks and motivations

The war on terror demands a focus on connections between individuals, between organizations, and between the individuals and the organizations. The purpose is to identify those that may be financing or otherwise aiding the activities of known terrorist organizations.

The case of the Bank of Credit and Commerce International (BCCI) is an example of the importance to uncover social networks, as well as the motivations of those belonging to the networks. BCCI was a Luxembourg-based bank, founded by Pakistani banker Agha Hassan Abedi[30]. It operated in more than 73 countries worldwide, and it did business with former Iraqi dictator Saddam Hussein, the Palestinian terrorist Abu Nidal, the Pakistani terrorist group Mujahideen, as well as Osama bin Landen. BCCI's founder was interested in more than enriching its clients, though. His goals included to "fight the evil influence of the West" and "finance Muslim terrorist organizations"[31].

The day to day of the fight against terrorism financing, however, is done by applying financial intelligence to the behaviour – financial and otherwise – of millions of individuals. Such intelligence goes well beyond typologies of transactions, paying special attention to the individuals or organizations involved in such transactions. The detection and prevention of terrorism financing requires high-street banks to step up security, including detailed identity checks on new and existing bank customers. Banks and other reporting institutions are told to pay special attention to those without regular income, those without regular expenditure patterns, and those who send and/or receive wire transfers, in small amounts, to/from particular geographical locations. This simplistic financial profile is not surprising if we remember that the terrorists that hijacked the airplanes used in the September 11th attacks, probably the highest profile terrorist attack in recent years, had posed as students while living in the US, and participated in wire transfers of small amounts to and from Dubai, for instance.

Three socio-demographic groups that fit the profile described above regarding income, expenditure and wire transfer of small amounts are, notoriously, students, unemployed people

[29] Discussed in the paper "Tracing the identity of a money launderer", in this same publication
[30] A thorough report is available in http://fas.org/irp/congress/1992_rpt/bcci/index.html
[31] http://www.washingtonmonthly.com/features/2004/0409.sirota.html

and migrants employed in low paid, temporary roles. It is also believed that some members of terrorist cells, namely those operating in Europe, are illegal immigrants that can neither make a living nor claim benefits in the host country, and are subsequently drawn into the illegal activities of the terrorist cells in exchange for accommodation, forged documentation and income.

The next section refers to a criminal investigation that took place, recently, in the United Kingdom.

5.4 Case study: Ricin found in a London Flat

On January 5th 2003, British police arrested seven men at two addresses in London, and seized ricin, a very potent poison with no known antidote, as well as equipment that could be used to produce the poison[32]. Two of the men arrested were teenage asylum seekers aged 16 or 17. The others arrested were in their 20s and 30s[33].

The men are of North African origin, and participated in a network of North African extremists, believed to be sympathetic to al-Qaeda. The investigation following from the January 5th arrests sparked numerous other investigations in a "domino effect", leading to raids in several other British towns[34]. The network appears to operate in small cells, dispersed in several European locations[35].

The criminal investigation has revealed that the individuals engaged in multiple identity fraud, and held forged passports and identity cards. The individuals had also engaged in the fraudulent opening and use of bank accounts, including the participation in cheque fraud, and the fraudulent use of loans and other credit facilities[36]. Preliminary work seems to suggest a close resemblance between the profile of a terrorist financer and that of an individual likely to pose a high credit risk for a financial institution – that is, someone likely to defraud a bank or to default on loan repayments. This finding is extremely important because financial institutions have had in place, for a long time, very advanced methodologies to assess credit risk that can, now, be put to service in the fight against terrorism financing.

It is also worth noting that the bank account activity of the individuals arrested in the context of this criminal investigation, included wire transfers to regions such as the Balkans, Pakistan, Iran and Iraq, as well as to charities operating in the UK. The cells to which the individuals belonged had raised funds through donations and collections at mosques and other Islamic centres, as well as through the sale of Islamic merchandise and publications[37].

The construction of the identity of a terrorist financer requires from the financial intermediaries a complex balance between computerized risk assessment models and personal judgment of the motivations behind specific observed financial behaviour. It also stresses the interconnectedness of identities, and that one person's identity is composed not only of elements that identify that person, but also of the social networks in which that person

[32] http://www.cnn.com/2003/WORLD/europe/01/31/britain.ricin/
[33] http://news.bbc.co.uk/1/hi/uk/2637515.stm
[34] http://news.bbc.co.uk/1/hi/uk/2659807.stm
[35] http://news.bbc.co.uk/1/hi/uk/2639625.stm
[36] Source: Interviews by the authors
[37] Idem

participates. Finally, the location of terrorist networks like the one discussed in this case raises important questions regarding privacy, as well as the risk of stigmatisation and discrimination of specific segments of the population.

6 Identity and Privacy in case law: On Revocable Anonymity, VUB

Wim Schreurs, Vrije Universiteit Brussel - V.U.B.

6.1 Introduction

People today increasingly access the internet in order to participate in the information society. The information society offers many advantages which can not be found in the off-line world such as free chat and phone communications, immaterial distribution of entertainment goods, new services and technologies with added value, immediate and organised access to a worldwide archive of documents and information.

The people's access to the internet as well as to the emerging wireless environments in public and private spaces, occurs in (roughly said) two ways: Or the user willingly provides parts of his identity and other information that can be linked to his physical person, or the user does not willingly provides information relating to his real identity or to parts of it.

In the first way, people provide others, like service providers, consciously with personal data such as name, address, credit card information etc… This occurs often when people subscribe to services (like newsletters), buy goods (like plane tickets) etc… In these cases, one could say that people are in fact confronted with only one professional party in a professional and corporate environment which they trust when they give their personal information. In these situations, the personal information is not just thrown into the unknown public, but provided as a necessary part of a confidential and trusted relationship. People mostly understand that it is necessary to reveal their identity or parts of it, because the trust-relationship is needed from both sides.

In the second way, people do not willingly or explicitly give away their identity: They act anonymously or under a pseudonym. In this case, one could say they are not confronted with a private 1-2-1 contact, but with a public in which a lot of (non-trusted) parties participate. This applies for newsfora and chatrooms but this also counts for the use of peer-2-peer software and the participation in peer-2-peer networks where any unidentified user can have access to the memory of your computer. Then, of course, people are less willing to just give away data that can relate to their identity. Also, it is not necessary to give away parts of your identity in order to participate to the service. Newsfora and chatrooms need news and chats, regardless of the origin of the words. Peer-2-peer networks just need peers, not identifiable persons. From a legal point of view, both the right to freedom of expression (in public spaces) and the right to privacy (in private spaces) are - to our opinion - almost natural expectations of the people towards the law, the government and companies.

Now, in the second way - subject matter of this contribution - people are often identifiable or transparent *anyway* because they automatically leave traces such as their IP address (internet) or their location and phone number (GSM). This means that often at least one person can have the possibility to revoke the anonymity or pseudonymity that is used by a particular user. This person is most often the service provider who provides the user with access to the network. This also means that a person, having access to the information that leads to the individual person, is another person than the one willing to have the identity of the person. And last but

not least, technologies creating, organising and managing your anonymity in the access to and in the communications through the almost omni-present ambient network around us, emerge with a quite fast speed…

This chapter deals with some cases relating to identity, anonymity, privacy and freedom of expression, which have been brought before a court. Case law, which is there to solve conflicts in particular situations, applies the law and fills in how the law should be explained in particular or new situations which were not really foreseen by the lawmaker. Although the binding character of case law is a complex issue (in most jurisdictions decisions only bind the parties), it is generally a good indication of the direction the law is taking. Important cases that imply important decisions with far-going consequences are called leading or even "landmark" cases.

6.2 Case n° 1: The Ouvaton Case

Do you have the right to encourage people on a website to destroy some street bulletin boards in the metro of Paris? Maybe you have, maybe you haven't, but the question here is whether you have the right to remain covered by anonymity or not. The Tribunal de Grande Instance de Paris (in a summary proceeding) had to answer this question when it was confronted with the following facts[38].

"Ouvaton", a French hosting provider, hosted a website[39]. This website encouraged its readers publicly and explicitly to destroy publicity boards in the metro of Paris as a protest to the content of the publicity. "Metrobus" was the company responsible for the bulletin boards in the Paris subways. Metrobus asked Ouvaton to provide with all information that can help identify the authors of the stopub.ouvaton.org website. Although the website closed after being summoned and although the hosting provider was not liable for the content because it was closed after being summoned, the hosting provider was ordered by the Tribunal to communicate to Metrobus any information that could lead to the identity of the authors.

We can conclude from this case that it is necessary that the communication of information relating to a possible identity (namely in this case IP numbers, known by the hosting provider only) can only be required by a judicial order in a criminal case. But, as a perverse consequence, it is the civil party that now also has access to the identity of the website creators, so that it (Metrobus in casu) can claim civil damages. Thanks to the court order in a criminal case, whether it has lead to a criminal prosecution or not, the civil party gains access to the identity of a third party that relied in first instance on its anonymity. Thirdly, we can conclude from this story that the non-identified person (the creators of the Ouvaton website) himself in fact had no possibility to defend himself before court against the revelation of his identity. If he would like to be involved in the court case to defend himself, he would become identified so that the involvement in the procedure to protect one's own anonymity would have a contradictory effect…

[38] Tribunal de Grande Instance de Paris, Ordonnance de référé, 1 décembre 2003, Société Métrobus vs. Société Ouvaton, http://www.legalis.net/jurisprudence-decision.php3?id_article=1025
[39] Ouvation web site : http://www.stopub.ouvaton.org/

6.3 *Case n° 2: R.I.A.A. (Recording Industry Association of America) vs. Verizon & others.*

The facts in the Verizon case are simple: the R.I.A.A., an organisation representing the music recording industry of America, tries to find and locate people that illegally upload copyrighted music files by using peer-to-peer networks. They access the per-to-peer networks and look for IP numbers from which copyrighted works are uploaded in the form of mp3 files. They do this in fact to obtain civil damages and compensation.

So, the R.I.A.A. can only do this by identifying the IP-numbers of the computers from which the music is illegally uploaded. The R.I.A.A. then contacts the ISP's and requests for the names and addresses of the physical persons that are behind those IP-numbers (the customers of the ISP's). This gives rise to discussion about privacy, data protection and anonymity on the internet, especially in the case of peer-2-peer networks.

A landmark case in this "war against copy" was R.I.A.A. vs. Verizon. In a first judgment in January 2003, the judge decided that Verizon was obliged to give to the R.I.A.A. the names of some subscribers who were accused of having infringed copyright law by uploading music through peer-2-peer networks. This created a storm of protest. This decision was however overruled by the Court of Appeal of Washington in December 2003, deciding that providers could only be obliged to give the identity of the alleged subscribers to the R.I.A.A. in the case of hosting, not in the case of mere conduit (peer-2-peer)[40].

There are many cases like the above mentioned: Judges sometimes decided that the names of customers must be handed over, while in other cases they ruled that the identities of their subscribers should not be given. Since December 2003, R.I.A.A. filed more than 7000 lawsuits against anonymous persons for infringement of copyright law through online file sharing[41]. An important consequence of these differences is that it leads to legal uncertainty.

These cases, however, raise some other interesting questions, such as: does the R.I.A.A. have the right to search on my PC for illegal content and illegal activities (whereas the Ouvaton case was about (illegal) information on a public website ; are software programs and websites which reveal IP-numbers legal, even if they don't reveal the physical persons which are behind those IP's (whereas the Ouvaton case was based on know Ip-numbers, you need some special software to find the IP-numbers behind peer-2-peer databases; and, do the ISP providers have the right to provide my identity (this is the same question as in the Ouvaton case)?

We can have an intermediate conclusion after these two cases: Firstly, ISP's can provide personal data like IP numbers of their customers only upon a court order in a criminal matter. Secondly, there is legal uncertainty whether yes or no your personal data can be provided to a third party because the judgements can differ from each other.

Now one could tackle the problems of providing (parts of) identities to third parties (by ISP's) without the consent of the person-to-identify by putting in the general terms and conditions of the ISP's that the names and addresses of the customers can be handed over to third parties if there is to the opinion of the ISP a reasonable indication of illegal activity. According to the

[40] An archive of this case can be found at http://www.eff.org/legal/cases/RIAA_v_Verizon/

[41] Grant Gross (2005); "Court Rejects RIAA Request to Identify Song Swappers"; IDG News Service, January 05, 2005. url: http://www.pcworld.com/news/article/0,aid,119172,00.asp

law: Yes. But should this be reasonable? Should there be no data protection law or consumer protection law that prohibits these terms and conditions?

6.4 Case n° 3: Pessers vs. Lycos in the Netherlands

This case very much sounds like the Ouvaton case. However, there is a difference: This is a purely civil case. There is no criminal prosecution at all: A private party is seeking for damages and compensation because harm was done to him on a public website. The facts were - in short - the following: Someone created an anonymous website on which he or she anonymously accused another person (who was an on-line post stamp seller) of illegal practices on Ebay. The person, accused of illegal practices, sent an email to the anonymous website asking for the wrongful accusations to stop. He never received an answer. He then asked the ISP to provide the name and address of the person who holds the anonymous website.

The ISP refused to do this because it is confronted with a dilemma: If it provides the identity of its customer and had not the right to do this, it is infringing the law; however if they don't provide the identity while they should have done so, they infringe the rights of the person that requested the information. In the end, providers don't want to play private police and don't want to have the responsibility to investigate every demand for de-anonymising a client, both because this is not their business and because will cost them a lot of money.

The accused person sued the ISP to obtain the name and address of the accusing person and won the case two times: in first instance and in appeal (Court of Amsterdam, 24 June 2004). The case is actually pending before the Supreme Court of the Netherlands[42].

This case is in fact about what is called conditional or recoverable anonymity and the right to speak anonymously. Two things are interesting in this case: Firstly, the identity had to be provided to the third party in a civil case where there was no speaking of a criminal investigation. In this sense, it importantly differs from e.g. the Verizon and the Ouvaton case (in which however, the personal data are used anyway for civil purposes…). Secondly, the court developed a so-called "four-steps' test to decide whether a client's identity should be revealed or not. It is this "four steps test" that may turn this case into a landmark case, provided the SC accepts these steps as a valid set of criteria. For the ISP, the four steps leading to obligation to disclose it's customer's identity are:

1. the possibility that the information, as such, is illegal and harmful towards a third person, is sufficiently plausible;
2. the third person has a real interest in the acquisition of the data;
3. it is plausible that, in the concrete case, no less infringing possibility exists to retrieve the data;
4. when weighing the interests of the third person (the one seeking for the identity of the person that accused him) should prevail over the interests of the service provider and the website holder (the anonymous person).

[42] All documents including actual and future proceedings and the future verdict related to this case can be found in Dutch on http://www.lycos.nl/rechtzaak.

While the law on anonymity is not clearly crystallised, judges can decide and in fact *define* in which cases and under what circumstances anonymity (and privacy) should be limited. Cases like this (can you remain anonymous? what can you do anonymously? when will your identity or aspects of it like your location, etc… be revealed?) are of major importance when one takes into account the Draft Framework Decision of 28th April 2004 of the Council of the European Union, which creates a rule that providers of a public communications network or publicly available electronic communications services must retain all traffic data, location data, user data, subscriber data, sources - routing - destination – time & data – duration - place and device of communication for a minimum period of one year and a maximum period of three years.

However, in these types of procedures, another interesting problem remained: The anonymous person had no right to defend himself before court when the revoking his anonymity was discussed. As far as we know, this issue is not solved yet because in many legal systems, people can not anonymously intervene as a party before court.

6.5 Anonymously defending your anonymity

The problem of the anonymous person, wanting to defend and retain his anonymity when it's revocation is being questioned before court, could be solved by analogy of California draft legislation (Assembly Bill 1143, see info.sen.ca.gov). This draft legislation creates an official procedure for de-anonymising and goes as follows:

1. a plaintiff suits (asks) an ISP to de-anonymise a client and provides the ISP with the reasons.
2. the SP notifies the anonymous personand sends him a copy of the suit,
3. the anonymous is granted a reasonable period to defend himself against the petition and sends his defence to the SP who sends it to the judge.
4. the judge rules on the defence.
5. if the party that files the suit abuses this procedure, he has to pay damages.

* * *

6.6 References

Sources Legislation

U.S. California Assembly Bill 1143 : "An act to amend Section 1985.3 of the Code of Civil Procedure, relating to Internet communications" : http://info.sen.ca.gov/

Draft Framework Decision of the Council of the European Union on data retention as of April 28 2004 : http://www.statewatch.org/news/2004/apr/8958-04-dataret.pdf

Opinion 9/2004 of the Data Protection Working Party on the draft Framework Decision: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm

Sources Case Law

R.I.A.A. vs. Verizon (Archive) :
http://www.eff.org/legal/cases/RIAA_v_Verizon/

Pessers vs. Lycos (Decision - Dutch):
http://www.solv.nl/nieuws_docs/1057Hof%20Adam%20240604%20(Lycos-Pessers).pdf
http://www.lycos.nl/rechtzaak
http://www.ivir.nl/publicaties/ekker/noot_pesserslycos.html (Dutch)

7 Identity and Privacy, KU-Leuven

Claudia Diaz, KU-Leuven

7.1 Introduction

We consider here two scenarios that highlight the privacy and anonymity issues we anticipate in the future development of the Information Society.

First, we describe a scenario to which no privacy enhancing techniques have been added, and analyse the potential impact of the lack of privacy protection on individuals. We present a second scenario with infrastructural anonymity and privacy enhancing mechanisms. We balance anonymity control requirements with accountability and law enforcement. We conclude with an analysis of the tradeoffs of privacy protection and accountability.

7.2 No Privacy Scenario

We make several assumptions, as realistic as possible, on the development of the Internet.

- The majority of the citizens are connected to the Internet and use a variety of electronic services (e-government, e-banking, e-commerce, e-voting, …)
- Remarkable development of storage devices, database technology, profiling algorithms, data gathering and data mining techniques exist.
- User's communication is traceable (i.e., no anonymous communication infrastructure is implemented).
- Unique identifiers, such as national ID numbers, are used to authenticate users (note that this is the case in some of the most recent electronic ID developments, such as the Belgian electronic ID card [1]).

In these conditions, and taking into account that companies increasingly consider customer profiling and databases as a "gold mine", it is reasonable to predict that more and more transactional, behavioural and personal data will be stored and used for different purposes. While e-government and e-voting create data procession with public authorities, e-banking and e-commerce create data procession by private authorities. It is even possible that public authorities provide data to private authorities and vice versa.

Given that no communication anonymity mechanisms are implemented, and due to the use of unique identifiers, users do not have means to prevent the linking of information their electronic activities generate. The gathering of data may even be invisible to the user.

The linkability of all information generated by an Internet user (e.g., through the IP address, national ID number or social security number), allows for sophisticated profiling of each user. Let us list some of the information that could be gathered and stored directly or indirectly, just by monitoring the user's communication: email address, age, gender, location, religious

preferences, sexual orientation, civil status, number of children, school of the children, bank, job, organisation, list of products bough on the Internet, daily supermarket and groceries lists, type of car, name of the garage, period of holidays, political orientation, race, lifestyle, interests, social network…

Information can also be gathered indirectly by linking data together, e.g. by storing which mobile phones of different persons are often together in the same area, one could infer social relationships.

Who would want to access these heterogeneous set of data? Here we give some examples of how the data could be profitable for different organisations.

- Private sector: Marketing companies can develop highly sophisticated campaigns if they get these data. For example, they could provide a service that shows on the TV (GSM, spam, or other new forms of publicity that may appear) of each person the ads that are more likely to stimulate him to buy a product (or a service). The economic gain of those in possession of the data could be enormous. Already today, ads are more and more personalised so that they have much more value: When entering a website like hotmail.com, the ads are automatically provided in the language of and towards the interested public of the location that is linked with the IP number.
- Public sector: Political (including extremist), religious (including abusive and dangerous sects) and even criminal or terrorist organizations could target the people they are interested in. For example, they may use it to recruit new members among those who are more likely to be "converted"; they could also use this information to select when and where to commit a crime (personalized crime could emerge, where the criminal selects and studies the victim in order to better plan and commit the crime).
- Private sector: Human resources departments could use these data in order to control their employees and to select their personnel. Discrimination based on personal details would be difficult to control. For example, people who have had medical problems would be more likely to be fired or not employed. Even if legislation would forbid medical examination before offering someone a job (as is the case in The Netherlands), it would be difficult to prove that information regarding medical problems was the reason for firing or not employing a person, especially if one has no access to the information that is available to the other party.
- Public and Private sector: As to both sectors, data can be abused by individual persons who abuse the database for personal purposes. The risk here is especially high because in this case people may really have an interest in accessing data, and the harm that is done could be very big
- Public sector: Regarding the public sector, that is governments, intelligence agencies, police departments, etc., it is difficult to imagine that they will resist the temptation of collecting and storing these data. As the draft framework decision of the Council of the European Union indicates, the priority for law enforcement and security may make them monitor citizens and push the legal and practical limits on the use of the data gathered. This is a more serious threat to individual freedom in weak democracies and undemocratic systems, where people who oppose the political regime may be retaliated. The point is that we do not know when democracies weaken and who will be in charge if they do. As an example of an explicitly undemocratic regime, China

demonstrates the extent to which a government may want to move to remain in control.

As we can see, personal information is valuable for organizations, whether it is for economic profit, or for controlling employees or citizens and their personal lives beyond today's imaginable limits. It is important to note that a crucial point will be the extent to which access to information is asymmetric. Especially in the case of asymmetric access (either because data protection legislation is absent or because it is not effective) personal information will give power and control to those in possession of the information, leaving profiled individuals in a vulnerable situation, as they do not have means to control who has access to which personal information, and for which purposes this information is used. In extreme scenarios, in which the amount of information available on individuals is very large, the degree of control on the profiled individuals could be enormous.

Finally, we would like to remark that once the information is no longer under the control of the user, it cannot be guaranteed that it will be completely removed. Therefore, in some sense, once privacy is "lost", it cannot be recovered. This is why personal data must be protected not only through legal means, but also through technical means that prevent the collection of the information.

From the Identity perspective, we could say that a very large portion of the identity (in the broad sense) of individuals would be exposed to external entities, which are not under the control of the data owner. This would give organisations in possession of the data the power to exploit and influence people's identities and behaviour for their own purposes.

7.3 Privacy-Enhanced Scenario

In order to highlight the impact of privacy enhancing technologies in the Information Society, we present here a slightly modified scenario, to which privacy-enhancing infrastructures have been added. The assumptions made for this case are:

- An anonymous communication infrastructure is in place, making all electronic communication untraceable. This untraceability exists not only to the content (encrypted) but also to source and destination of the communication (e.g. mixes [3,4,5,6,9])
- Revocable anonymous credentials [7,8] are used for different services: these credentials allow for pseudonymous identity management, in such a way that different user transactions are unlinkable. For applications that require so (e.g., e-commerce), clients may be required to present encrypted identity information that can be revealed by a judge in case of fraud or crime.
- Other kinds of privacy enhancing technologies, such as pseudonymous signatures [11], anonymous email [2,10], etc. are implemented and widely used.

Companies know their customers by pseudonyms. Different pseudonyms of a user are not linkable to each other. The pseudonyms are generated from a master secret of the user, which may be kept in a smart card or other secure storage device. Users have the tools to manage their identities when electronically interacting with different organisations (the supermarket,

the library, the doctor, etc.) is such a way that they can prove the required attributes (e.g., proof of subscription), but they do not leak any other identity information.

In this scenario, the degree of profiling that organisations can do on customers is very much limited in comparison with the previous case. Users may choose to disclose some preferences in their interactions, in order to get personalized services, but this decision is now on the user's side, and not with the company. With these technologies, users can decide which are the identity aspects that they want to make available to a certain organisation. Companies are not able to collect all kinds of data about customers in huge databases, and instead, they are provided with specific data (e.g., preferences for a certain services).

The collusion of two or more different organisations does not threaten customers' privacy, as these organisations are not able to merge their databases, because there are no unique identifiers for the individuals whose personal data appear in two or more databases. Effectively, organisations may collect the data they need on pseudonymous individuals (with some limitations though), but different organisations cannot find out whether they have in their databases information on the same individuals or not.

Regarding accountability, it is clear that anonymity systems cannot succeed on a large scale if individuals cannot be held accountable of their acts. For example, the applications that involve economic transactions (e.g., electronic payments) are particularly sensitive to abuse.

Anonymous credentials may optionally include encrypted identity information that can be revealed by a trusted party (e.g. a judge). Users may be required to prove the correctness of this information in order to carry on a transaction. The other party of the transaction may keep these data in order to be able to go to a trusted party who can identify the communication partner in case of dispute.

7.4 Tradeoffs

Privacy has a cost. The inclusion of privacy enhancing and anonymity techniques puts an overhead on the system, in terms of communication, computing power, performance and complexity. Therefore, the first technical tradeoffs that need to be found are between security, robustness, anonymity degree [12,13], availability, and functionality, performance, overhead and usability.

Regarding the management and storage overhead, it is not so clear which of the two options is more efficient. In the first option, the management of the data is centralized, and the amount of data gathered in databases is larger. In the second, the storage is more distributed (as users would take care of storing their own data), and the management of the information is mostly done on the user side. The particular design choices made to implement these systems would determine the management and storage costs of each scenario.

Accountability mechanisms may prevent fraud and abuse of the system. However, we note that the task of law enforcement agencies may get harder when it comes to trace communications that do not violate the system's rules. For example, the online monitoring and tracing of (off-line) criminal suspects (i.e., those who commit crimes outside the Internet) may become harder with privacy enhancing mechanisms in place. A tradeoff must be found in the legal and technical issues in order to provide law enforcement with tools to fight crime.

From a conceptual point of view, the central concepts involved are trust, privacy, individual freedom, security and control. The relationship between these different concepts is complex. For example, privacy and security are not necessary contradictory, as a lack of privacy constitutes a security hole in a broad sense. However, the issues of freedom and control are directly contradictory, as the balance between these two will define where to draw the line. For example, a difficult, borderline case would be that of someone expressing an opinion which is unacceptable for the public powers (e.g., what would happen to someone who posts pictures of torture applied by an army? Would that person be identified? On the one hand, public institutions do have the ability to identify annoying citizens, which is dangerous; on the other hand, these tools are needed in order to prevent crime).

The key concept is that of trust. Users must trust that the entities with the ability of identifying them will only do it respecting the legal guarantees. The trust in single entities can be enhanced by distributing the trust, so that several entities need to collaborate in order to identify a subject (e.g., the agreement of three judges is required). Verifiability of the identification processes also enhances trust. It is worth noting that trust is a very subjective concept, which depends not only on technical or legal objective factors, but also on cultural, psychological and social factors.

7.5 References

[1] http://eid.belgium.be/

[2] Untraceable electronic mail, return addresses, and digital pseudonyms. David Chaum. Communications of the ACM 4(2), February 1981.

[3] ISDN-mixes: Untraceable communication with very small bandwidth overhead. Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner. Proceedings of the GI/ITG Conference on Communication in Distributed Systems, February 1991, pages 451-463

[4] Web MIXes: A system for anonymous and unobservable Internet access. Oliver Berthold, Hannes Federrath, and Stefan Köpsell. Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, July 2000, pages 115-129.

[5] A Pseudonymous Communications Infrastructure for the Internet. Ian Goldberg. Ph.D. thesis, UC Berkeley, December 2000.

[6] Tarzan: A Peer-to-Peer Anonymizing Network Layer. Michael J. Freedman and Robert Morris. Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington, DC, November 2002.

[7] Design and implementation of the idemix anonymous credential system. J. Camenisch and E. Van Herreweghen. Proceedings of the 9th ACM conference on Computer and Communications Security, pages 21–30. ACM Press, Nov 2002.

[8] An efficient system for non-transferable anonymous credentials with optional anonymity revocation. Jan Camenisch and Anna Lysyanskaya. EUROCRYPT, volume 2045 of Lecture Notes in Computer Science, pages 93+, 2001.

[9] Generalising Mixes. Claudia Díaz and Andrei Serjantov. Proceedings of Privacy Enhancing Technologies workshop (PET 2003), March 2003.

[10] Mixminion: Design of a Type III Anonymous Remailer Protocol. George Danezis, Roger Dingledine, and Nick Mathewson. Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 2003.

[11] Signature Schemes and Anonymous Credentials from Bilinear Maps. Jan Camenisch, Anna Lysyanskaya. Proceedings of CRYPTO 2004, pages 56-72.

[12] Towards measuring anonymity. Claudia Díaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), April 2002.

[13] Towards an Information Theoretic Metric for Anonymity. Andrei Serjantov and George Danezis. Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), April 2002.

8 Ubiquitous Computing Scenario, Univ. of Reading

Mark Gasson, and Kevin Warwick, University of Reading, UK

8.1 Executive Summary

Issues relating to identity are set to change as technology continues to evolve. Here we consider how potentially invasive technology has already found applications in our everyday lives and may continue to do so, despite the continuing concerns over identity and privacy issues.

8.2 Introduction

The emergence of the internet, and with it the possibilities of distributed computing (i.e. using several computing devices, that are not necessarily located in the same geographic location, for a specific task) has had a profound effect on our way of life. Ubiquitous Computing is the next wave of technology, a paradigm shift from our current relationship with technology, whereby many thousands of wireless computing devices are distributed in the environment in everyday objects around us. This technology is one of the tools which aims to achieve the idealised Ambient Intelligence (AmI) Environment (see section 2.2). However, here the concept is restricted to how the emergence of this potentially invasive technology may become commonplace in the very near future.

Firstly, an example existing scenario will be considered to demonstrate how such invasive technology has already become accepted in our everyday lives.

8.3 Current Technology: Loyalty Cards

It is perhaps not always appreciated how much information about ourselves and our personal identity that we willingly allow third party companies and individuals access to because of a perceived benefit to ourselves. For example, one of the more surreptitious technologies that has appeared over the last few years is that of the supermarket loyalty card. Whilst offering money saving vouchers and discounts to the customer, the system allows direct association between items bought and an individual, specific details of whom are disclosed by the individual themselves during the initial sign-up procedure.

Supermarket chains argue that such information allows for more tailored discounts to be offered to the customer and research has shown that loyalty cards help keep customers tied to a specific store chain, thus maintaining their existing customer base[43]. More importantly for the retailers, shopping habits, such as the type of cereal bought, can be monitored, and bonuses such as additional loyalty points offered to the customer if they try a similar, but more expensive brand, in essence a form of targeted advertising.

[43] http://news.bbc.co.uk/hi/english/business/your_money/newsid_336000/336590.stm

However, beyond this simple application, improvements in database technologies and data-mining techniques mean that new information can potentially be *inferred* from other seemingly innocuous data, thus producing complex (although not necessarily accurate) profiles of customers. For example, a sustained increase in the amount of basic foods such as bread and milk may imply a new member in the household, whilst the start of regular purchasing of nappies suggests a new baby. This information is invaluable to third-parties wishing to target a specific group of people or to product manufacturers, and notably in the US, disclosure of loyalty card information has enabled its use in personal injury and family law cases. However, more worryingly are reports that law enforcement agencies have reviewed loyalty card records of people convicted of specific terrorism acts to build a hypothetical profile of ethnic tastes and supermarket shopping patterns associated with terrorism.

The UK government has expressed its concern over the potential (mis)use of information gathered through supermarket loyalty cards[44]. However, it has already highlighted the possibilities by noting that such information could be used to identify customers who bought excessive amounts of foods high in fat, sugar and salt, and that this information could be used to promote healthier alternatives to these customers[45].

Figure 8-1: Market research by *TNS*[46] shows that by mid 2003, around 85% of UK households had at least one loyalty card

Whilst it is assumed that due to existing data protection laws in the UK such information would not be used to the extent of criminal profiling, concerns exist over the 'function creep' phenomenon, i.e. an information system design for one application can end up being used for another.

[44] http://news.bbc.co.uk/1/hi/uk_politics/4018939.stm
[45] http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/12/05/ntesco05.xml
[46] Taylor Nelson Sofres plc

With this in mind, it is pertinent to extrapolate existing technology to examine the identity concerns that may arise in the future information society scenario.

8.4 Emerging Technology: Radio Frequency IDentification (RFID)

The first clear step towards the ubiquitous computing scenario is the use of Radio Frequency IDentification (RFID) tags in supermarket product packaging. Although similar to the security tags that wirelessly detect if a product is being removed without payment from the store, RFID tags are *unique* identifiers which allow an individual item (not just type of product) to be wirelessly detected. In this way they are more useful to the supermarket than product barcodes, since the tags can not only reveal the product (and thus the price at the till), but which batch it actually came from and other data regarding its history that may have been logged. This could allow a centralised system to keep account of any items due to expire on the shop shelves which should be moved to a more prominent position for quicker purchase, or items that are running out of stock and need reordering.

Ultimately the aim is to tag every item sold, including food, clothes, electronic goods and medicine, with an internet database that holds a record of every item. Current trial applications have seen the tagging of razor blades[47] such that a security camera can be activated when the product is removed from the shelf, in an attempt to reduce theft of these high value items. In the US, the Food and Drug Administration (FDA) has already announced plans for medicines to be tagged[48], in an attempt to combat counterfeiting of drugs such as Viagra. Although useful in the supply-side context, the exploitation of these unique identifiers after sales is a privacy concern.

Beyond the retail application, tagging of banknotes has been proposed as an anti counterfeiting and money laundering method and tags in plane tickets have been trialled to help locate passengers within the airport. School children have been issued RFID cards in parts of Japan to keep track of their movements[49], whilst others have had small tags sewn into their clothing. Similar systems have been trialled in hospitals[50] to increase medical efficiency such as medicine distribution, and amusement parks have utilised RFID bracelets to help track children who have gone astray.

In more invasive procedures, human implantation of RFID devices has also been proposed for a variety of applications. In 1998, Professor Kevin Warwick of the Department of Cybernetics at the University of Reading, UK became one of the first people to have such a device implanted. By being able to track and uniquely identify him, the departmental building was able to build a profile of his behaviour, and customise it to his preferences, including adjusting light levels, starting his computer, and even brewing the coffee on his arrival.

[47] http://news.bbc.co.uk/1/hi/england/berkshire/3110650.stm
[48] http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html#radiofrequency
[49] http://www.guardian.co.uk/japan/story/0,7369,1259845,00.html
[50] http://news.bbc.co.uk/2/hi/uk_news/england/west_midlands/3957743.stm

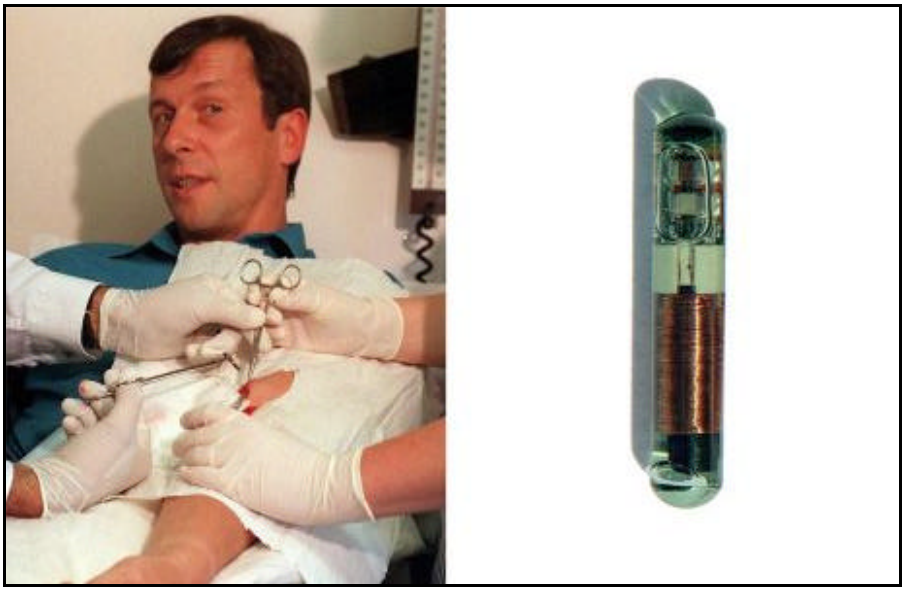


Figure 8-2: Prof. Kevin Warwick has a 2cm long identifying implant (shown enlarged, right) surgically inserted into his arm

In other applications, some four years later, implanted identifying tags have been commercialised to essentially replace 'medic alert' bracelets and to relay medical details when linked with an online medical database[51]. Other implanted devices have been used to allow the individual access to secure areas, and even to identify clubbers such that payment for drinks can be automatically debited from their account[52].

8.5 Potential Scenario

A man is waiting in a dark alley hidden from view; his aim is to attack a passer-by for their money and valuables. His wireless RFID scanner is located on the side of the path, detecting people as they walk past and sending their unique embedded RFID tag information to his wearable personal display screen. These unique tag codes are cross-correlated in real-time with an online database to reveal the actual identity of the item.

The first person walks past, and the following information is revealed:

25€ in banknotes – Titanium hip replacement – 1 box of bran flakes – Leather shoes – Wax jacket – Bottle of Viagra – Reading glasses – Bingo Club membership card

The man decides to wait.

The next person walks past, and the following information is revealed:

205€ in banknotes – Unbranded Denim jeans – 'Puma' trainers – Designer glasses – Library card – 1 litre orange juice – 1 loaf of bread – Book on family planning – 'Rolex' watch – High dosage asthma inhaler

The assailant is able to make an informed choice based on the information 'leaked' by the RFID tags, and decides to attack.

[51] http://news.bbc.co.uk/2/hi/health/1981026.stm

[52] http://news.bbc.co.uk/2/hi/technology/3697940.stm

8.6 Discussion

The use of RFID technology for even simple innocuous applications may suffer from the 'function creep' issue, thus the subsequent misuse to which it may be put is of real privacy concern and needs to be addressed.

However, given that RFID technology will most probably become widely accepted and ubiquitous, it is feasible that the profiling technologies being developed for applications such as supermarket loyalty cards can be utilised to reveal extensive descriptions of behaviour, belongings, personal preferences and daily habits, to name a few.

Worryingly, research has shown that public perception of such developments is negative, yet apathetic. Ultimately, people seem to have concerns about the technology, but have resigned themselves to its inevitability.

9 Identity in the Ambient Intelligence Environment, IPTS

Sabine Delaitre, IPTS

9.1 Executive Summary

This sections aims at defining the concept of Identity in the Ambient Intelligence (AmI) environment and describing its different facets.

After a short description of the AmI environment, the concept of the identity will be introduced. Next, a scenario will be used as a starting point to establishing two cases studies. From the analysis of them, the different facets of the Identity in AmI environment will be highlighted. This analysis is, in fact, an ontological analysis; it is interesting since this allows a first formalisation of the different facets of the Identity.

9.2 Ambient Intelligence Environment

The Ambient Intelligence motivator is to enrich the quality of the everyday life. Indeed, AmI is a vision aiming at placing human beings at the centre of the future development of the knowledge-based society and information and communication technologies.

AmI vision mainly encompasses three key technologies:

- Ubiquitous Computing: the integration of microprocessors into everyday objects like furniture, clothes or toys.
- Ubiquitous communication: enabling communications between object-object and object-user. (An object is for example an electronic device such as a PDA, Personal Digital Assistant).
- Intelligent User Interface: enabling the user of the AmI space to control and interact with this environment in a natural and personalised way.

The purpose is to deliver seamless applications and services to citizens in order to support their everyday activity. Hence, AmI vision is based on a user-driven approach with the goal to foster the integration of the technology into our environment. This approach involves the understanding as to how people interact with the technology and the handling of an indispensable component, the user context. In order to fulfil theses objectives, the characteristics to be achieved are ubiquity, awareness, transparency, intelligent, sensitive, adaptive and responsive.

9.3 Identity in the Ambient Intelligence Environment

9.3.1 Identity Information

We can split the identity information into three types:

- Offline Identity Information
- Digital Identity Information
- Identity Information to bridge offline and digital Identities

The offline Identity information can be 1) related to the appearance such as hair, eyes colour, glasses, etc. 2) used as social information, e.g. name, postal address, phone number and 3) represented by identity tokens (passport, visa, credit card, security social number, Bank Account Number or BAN).

The digital identity can be described in the same way. So the information related to the appearance can be incorporated into, for instance a biometric template (fingerprint template, iris template). The corresponding social information can be a nickname, an e-mail address or an IP address. And the digital signature or more generally any digital certificates can be considered as identity tokens for the digital identity.

For describing Identity information to bridge offline and digital Identities, we can distinguish the information related to the knowledge-based Identification (password, PIN) and the information gathered from the user context (profile, user preferences).

9.3.2 Identity Information concerns

In the framework of AmI space, four concerns related to the identity information can be underlined:

- Interoperability
- Privacy
- Data Protection
- Storage

Thus, the Identity information should be understandable by any device (interoperability) and should be used only by authorized devices (privacy). More importantly, the user should be able to control and/or specify which information to disclose and to whom.

The AmI environment should provide efficient and reliable mechanisms to ensure data protection (transfer, storage) in order to increase trust and confidence in the information society. The storage concern is related to the choice to use centralized database or not. This choice involves different measures to be taken concerning not only the protection of data and

but also the security in general (e.g., access rights, etc.) and identity management (e.g., identity synchronisation, identity revocation, etc.).

9.4 Scenario: Enjoy a bar in 2012

What does a bar in the future look like? This scene (see Figure 9.4-1, image source: [Beslay et. al, 2005]) helps to describe the features of such bar.

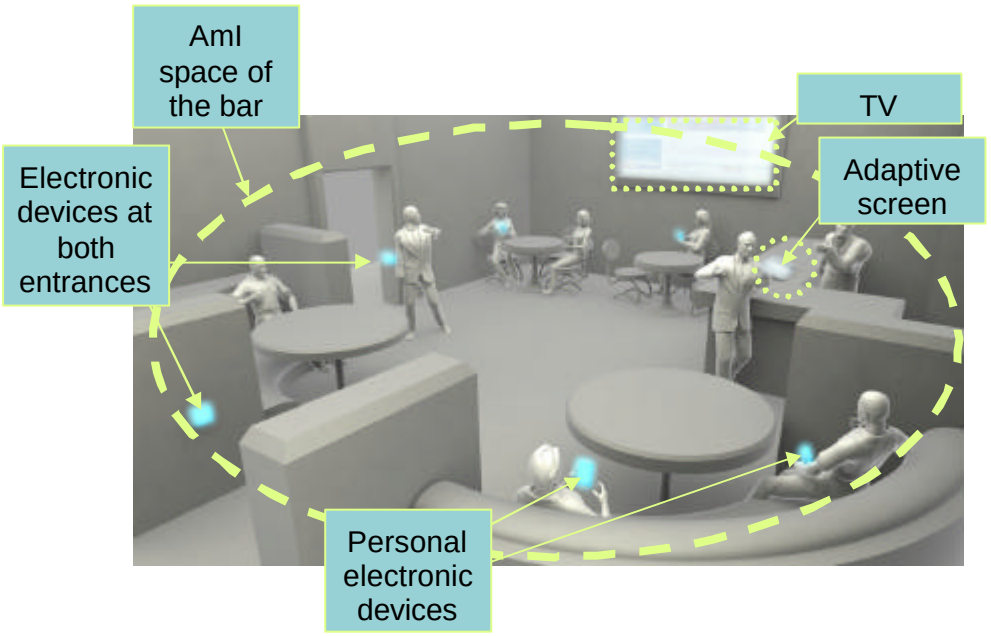


Figure 9.4-1: A scene in a bar in 2012

First of all at both entrances, we can observe electronic devices (e.g. for the detection of new customers or the transmission of information); on the wall a special TV; at the bar an adaptive screen and personal electronic devices (e.g. a PDA) for some customers. The Ambient Intelligence environment of the bar is symbolized by the dashed oval - this determines the space in which communications are enabled and all devices can interact.

The scenario is composed of four moments as depicted in the schematic view below (see Figure 9.4-2). The customer (i.e., the user of the AmI environment) enters into the bar, enjoys a moment at the bar, he is fortunate enough to have a chance encounter and finally, he pays for the drinks.

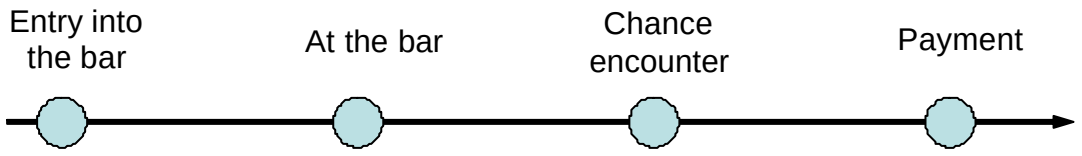


Figure 9.4-2: Schematic view of scenario

9.4.1 Case Study 1: in his city

Entry into the bar: *The customer declares his preferences (using his PDA) and activates his availability to meet a friend (Thus, the following data are transmitted - to the adaptive screen for example - : his favourite drink, language etc., his user specificities, e.g. prescribed medication and list of friends.)*

At the bar: *Barman: do you want a cappuccino? (the transmitted favourite drink). The adaptive screen shows also him the soft drinks option (it knows he cannot have alcohol because of his medication).*

Thanks to his electronic device he "watches TV in the language of his choice (preference)". (more precisely, he listens to the sound in the language of his choice through his PDA and the corresponding image is displayed on the TV screen).

Chance encounter: *An alarm notifies him a friend has arrived.*

After a nice conversation with his friend, he decides to leave.

Payment: *He chooses whether to pay with fingerprint mode or with RFID (Radio Frequency IDentification) card from local account.*

9.4.2 Case Study 2: foreign country

Entry into the bar: *He declares his preferences. A temporary account is opened.*

At the bar: *The adaptive screen automatically provides him the menu in his own language (preferences).*

After he has a drink and makes a local hotel reservation through the WI-FI connection, he becomes relaxed and activates his availability to meet a person, putting his profile at disposal.

Chance encounter: *An alarm notifies him two answers (of course, from two people in the bar). He accepts one.*

Payment: *His temporary account indicates the amount to be paid in both currencies with the conversion rate. And he pays by credit card.*

9.5 Different Facets of Identity

First of all, from these two case studies (cs1 and cs2) it is possible to illustrate the three types of Identity information:

- Offline identity
  - Related to the appearance: *fingerprint (cs1)*
  - Identity tokens: *RFID card (cs1), credit card (cs2), BAN (cs1, the Bank Account Number is known by the bar through a contract between the bar and the customer for the use of fingerprint mode payment)*
- Digital identity
  - Related to the appearance: *fingerprint template (cs1)*

- Social information: *Identifier of the personal electronic device (cs1&cs2)*

- Identity Information to bridge offline and digital Identities
  - Knowledge-based Identification: *password or PIN of the personal electronic device (cs1&cs2, not explicitly described in the scenario but essential to switch on some devices)*
  - Related to the user context: *profile, user preferences (cs1&cs2)*

The following sub-sections detail the analysis of the case studies, and more precisely form an ontological analysis. By scanning the text of each case study and detecting the terms related to Identity, directly or otherwise. Then, each of these terms is described by its corresponding ontological representation from the ontology of the identity.

9.5.1 Case Study 1 analysis

Entry into the bar: *He declares his preferences and activates his availability to meet a friend*

At the bar: *Barman: do you want a cappuccino? The adaptive screen shows him the soft drinks.*

Thanks to his electronic device he "watches TV in the language of his choice".

Chance encounter: *An alarm notifies him a friend has arrived.*

After a nice conversation with his friend, he decides to leave.

Payment: *He chooses whether to pay with fingerprint mode or with RFID card from local account.*

Each underlined term is related to the identity concept. From the identity ontology (described in the D2.1), these terms are described as follows:

Term	Ontological representation	Observation
Preference(s)	Profile representation → individual profile → preferences	Other possibility: Identifier / bridge offline and digital identities / related to the user context
Friend	Profile representation → individual profile →sociological profile → personal network (→	

Term	Ontological representation	Observation
	friend)	
Electronic device	Identifier → electronic device (→ id PDA)	Other possibility: Identifier/digital identity / social information / ID electronic device
Fingerprint	Identifier → biometrics → fingerprint	Other possibility: Identifier / digital identity / related to the appearance / biometric template
RFID card	Identifier → electronic device → id card / RFID	Other possibility: Identifier / offline identity / token
Implicit Term	**Ontological representation**	**Observation**
BAN (of the customer for the fingerprint mode payment)	Profile representation → individual profile →financial information → banking information	Other possibility: Identifier / offline identity / token
Password, PIN (of used electronic devices)	Identifier → digital identifier → password	Other possibility: Identifier / bridge offline and digital identities / knowledge-based identification /PIN, password
(dash style) term	**Possible ontological representation**	**Observation**
Interaction: declares, activates, or notifies him	Identity / device communication / access	The declaration (*declares*) may be active (the user acts, e.g. pushes a button, sends information) or passive (the bar device detects the customer)
Fingerprint mode	1) Identity / data protection 2) Identity / storage / biometrics template	Indeed, the fingerprint mode payment raises two important concepts related to the identity the data protection and the storage of the fingerprint template.

9.5.2 Case Study 2 analysis

The following analysis of the case study 2 only focuses on the additional information related to Identity.

Entry into the bar: *He declares his preferences. A temporary account is opened.*

At the bar: *The adaptive screen automatically provides him the menu in his own language.*

After he has a drink and makes a local hotel reservation through the WI-FI connection, he becomes relaxed and activates his availability to meet a person, putting his profile at disposal.

Chance encounter: *An alarm notifies him two answers (of course, from two people in the bar). He accepts one.*

Payment: *His temporary account indicates the amount to be paid in both currencies with the conversion rate. And he pays by credit card.*

(dash style) term	Possible ontological representation	Observation
Profile	Profile representation → individual profile → sociological profile /anonymous	The user decided to disclose in the AmI space of the bar only some information in an anonymous way. Other possibility: Identifier / bridge offline and digital identities / related to the user context / anonymous
Interaction: declares, activates, or notifies him	1) Identity / device communication / access 2) Identity / device communication / interoperability / standards	This story takes place at a foreign country. So, the interoperability concern arises.

Here, the scenario approach and especially the cases studies play the role of a validation tool; indeed, thanks to the stories we can verify the usefulness of ontological representations (case of the underlined term in solid style) and detect some gaps (case of the underlined term in dash style) or new requirements, so we can extend or modify the ontology in an effective way.

9.6 Conclusion

As previously shown, the identity information in the Ambient Intelligence environment encompasses three types of information: offline Identity Information, digital Identity Information and Identity Information to bridge offline and digital Identities. The case studies based on the scenario "enjoy a bar in 2012" have helped to illustrate these types of information in concrete situations and the ontological analysis of these cases studies has allowed highlighting (and formalizing) the different facets of the identity.

9.7 References

Laurent Beslay and Hannu Hakala (2005), "Digital territories: bubbles", to be published *in the Vision Book* (2005)

10 The Role of Reputation and Privacy for Identities in Digital Communities, TUD

Sandra Steinbrecher, Technische Universität Dresden, Germany

10.1 Reputation in Digital Communities

With the growth of the Internet more and more people spend a lot of their spare time in so-called Internet Communities – a manifestation of digital social environments on the Internet - instead with friends or relatives at their domicile. Most of these virtual friends they have neither met in the past nor will meet them in the future. Certainly as for every rule there exist exceptions: More and more non-virtual friend- and relationships have been started in such Internet Communities.

The spectrum of Internet Communities from various providers reaches from mailing lists, newsgroups and discussion forums to role-playing and electronic marketplaces.

Members of the communities naturally have the typical security requirements (confidentiality, integrity and availability) on the technical systems implementing these communities. But even more than in the systems they have certain requirements on the other (initially unknown) members they are interacting with. And even more than in interactions with well-known opponents they have the same requirements on the unknown opponents. Beneath the system guaranteeing secrecy and integrity of information also the other users should do so if specified by the user:

- Someone seeking advice might get technical integrity of other user's answers, but if they give him false advice, technical integrity is meaningless for his problem.
- Someone who wants his requests within the community to be kept secret from others than legitimated readers of the question might get this guaranteed by the system, but what about if other users distribute this information manually?

In the real world formal agreements between unknown people are ensured by handwritten signatures. This guarantees the legal enforceability of statements. The same might be reached for digital information and actions by adding digital signatures (and if necessary time stamps) that guarantee integrity and authenticity of the information resp. actions. This needs appropriate public-key infrastructures. But as in the real-world the members only get evidences for others' misbehaviour. Every dispute between them has to be solved outside the Internet community in a legal process. The legal enforceability of digital information and actions depends on how legally binding the corresponding security measures are considered to be in national and international law.

When becoming a member of an Internet community an individuum develops a new partial digital (or virtual) partial identity within this community. Often for becoming a member of a community a user has to register at the provider by choosing the pseudonym he wants to use and eventually declaring some additional personal information (e.g. his age, postal and e-mail address) that may be verified by the provider but more often is not. So the individuum starts with a new pseudonym and has to gain a reputation for this pseudonym within the

community. His reputation will depend on his (mis)behaviour and other member's valuation of this.

Reputation systems can collect the experiences members made with interactors in past interactions in a technically efficient way. These experiences may help other members to estimate the future behaviour of unknown interactors. This assumes that past behaviour indicates future behaviour.

But it does not prevent any member from making bad experiences with new interactors because reputation usually is context-depending and beneath that members may lie about others' behaviour (Dellacoras, 2000) or suddenly change their behaviour. Technical security measures cannot prevent the latter 'social' attacks but a usually large number of reputations and an honest majority of members will hopefully reach that dissatisfied members are the exception. For the case that two members are dissatisfied with an interaction, technical measures should still give them the possibility to reach legal enforceability of each other. So reputation systems do not make other technical security measures obsolete, but hopefully reduce the expensive legal process of enforcing them.

10.2 The Example of Marketplace Communities [53]

Very popular Internet communities are the so-called marketplace communities, whose members are allowed to sell and buy arbitrary items within the community. One of the greatest providers with nearly 95 million registered members worldwide at the end of 2003 (eBay Annual Report 2003) is eBay[54].

After an item within the community has been sold the respecting seller and buyer somehow have to exchange the item purchased and the reward pursuant to its price. This exchange must be fair, i.e. seller and buyer both have to receive what they have agreed upon. If the item is a digital good (e.g. information) and for the reward electronic money is available, the exchange can be realized by electronic fair exchange (Asokan et al, 1998). In the EU project SEMPER (Waidner, 1996) a framework for an optimal electronic marketplace which allows trade with digital goods, was developed. But most items are physical goods that can be exchanged either directly between seller and buyer or via a trusted third party that guarantees the correct transfer. Many providers offer or mediate an appropriate transfer service against a charge.

But because the price of many items sold within marketplace communities is quite low (e.g. books, CDs, computer games) many buyers and sellers decide to exchange money and item directly. The provider provides them with the other member's personal data necessary to do this. Usually the buyer transfers money from his account to the seller's account and after the money has been credited his account the seller sends the item by mail to the buyer.

This exchange needs trust in each other that own expectations and the other's behaviour are equivalent. Many of these exchanges are successful, but unfortunately some are not. In the eBay community continuously frauds are discovered where a member pretended to sell items, collected money from buyers, but did not deliver the items offered. In 2002 more than 51,000 complaints about Internet auction frauds in the U.S. were reported to the Federal Trade

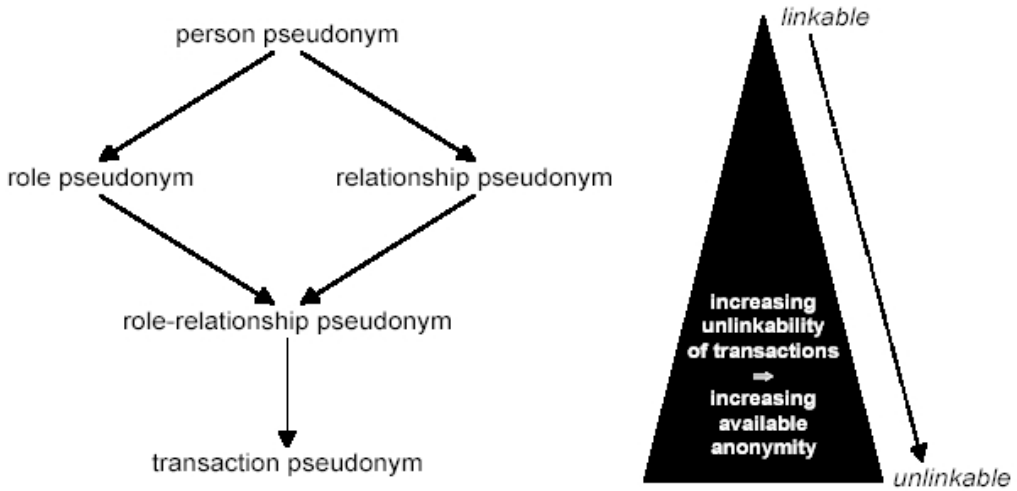
[53] This section is a summary of work performed within the FIDIS project and published as: (Steinbrecher, 2004).
[54] eBay http://www.ebay.com/

Commission (Federal Trade Commission, 2003). Although the actual percentage of fraud in such exchange is small (for instance a eBay representative indicates (Wearden, 2004) that "Fewer than 0.01 percent of all listings on eBay result in a confirmed case of fraud"), the nuisance perceived by the customer is high, and can hamper the further development of electronic marketplace communities.

Reputation systems were introduced to most providers' service to handle problems that might occur during the interactions between sellers and buyers. This is cheaper for providers than adding expensive public-key measures and infrastructures to give the members authenticity and legal enforceability of digital information within a trade. After the direct exchange of money and item is completed (satisfying or not) both may give comments or/and marks to each other. These are added to the member's feedback profile (usually together with the annotator and the exchange considered as context information). Before buying from or selling to a person every member of the community can inform himself about the other's reputation profile.

10.3 Identity Management and Reputation

Reputation systems as data bases for community members' experiences with other members should be protected by means of technical data protection to ensure users' right of informational self-determination. Because beneath the legitimate interest of the community members who inform themselves about future interactors numerous data collectors will be desirous to get access to such large data bases which contain information who interacted at



which time with whom and in which context.

Figure 3

Unfortunately the reputation systems currently in use in the above example of electronic marketplace communities (Kollock, 1999) allow to generate interest and behaviour profiles of pseudonyms (e.g. time and frequency of participation, valuation of and interest in specific items). One distinguishes between different pseudonym types depending on their usage as it is

also illustrated in Figure 3 (Köhntopp and Pfitzmann, 2004) If the pseudonym becomes related to a real name, as it typically does for trading partners, the profile becomes related to this real name as well. But surveys (Pew Internet & American Live Project, 2000, and Harris Interactive, 2002) indicate that a lack of privacy seems to reduce the success of electronic commerce. Every member wants to determine himself how much and when he wants to reveal data about his person, behaviour and interests.

User-controlled privacy-enhancing identity management (Clauß et al, 2002) gives the possibility to reach pseudonymous interaction on the Internet that tries to satisfy all parties' security requirements. Typically the user-server scenario is considered, A user can protect against unauthorized access to information while by the use of credentials the server can be sure pseudonymous users are reliable and can be made accountable for misbehaviour. E.g., the use of an identity management system is applicable to the scenario of classical e-Commerce on the Internet (Clauß and Köhntopp, 2001). The difference to Internet communities is the change of roles (between servers and users) that happen within them.

In the EU project PRIME (http://www.prime-project.eu.org/) a prototype for a privacy-enhanhing identity management system is built that gives the user the control over his personal data and its use for different applications e.g., e-commerce. The prototype will make an appropriate design of the user side and possible server sides. This will need application providers to install this software on the server side and provide access to their services using identity management software.

Reputation systems are an important part to be integrated in identity management systems to lower the costs of interactions between members in Internet communities.

To increase privacy in Internet communities instead of person pseudonyms a pseudonym type that is restricted to fewer uses should be used.

Unlinkability between different contexts (or context types) a member of the community is involved in can be reached by using role pseudonyms regarding to the roles he has in these contexts. E.g., by this measure the contexts 'offering goods within the community' or 'giving advice regarding a specific topic' or 'chatting about a hobby' could be separated by using different unlinkable pseudonyms. Using this pseudonym type has the positive side effect that reputations for these roles are collected separately. This should even increase the trust in the reputation system because members might be different trustworthy depending on the context. The definition of a context and the distinction between contexts has to be made in the reputation system to make the reputations collected under a pseudonym sensible.

All members with access to the reputation system have the opportunity to link all context information regarding the used pseudonym. Beneath using role pseudonyms for different contexts users should change the pseudonyms they use within these contexts from time to time. To give members the possibility to use their reputation with different sequenced pseudonyms a similar mechanism than for convertible credentials (Chaum, 1985) could to be used.

The anonymity set in Internet communities usually is quite large. If the number of possible reputations is limited, e.g. by a numerical sum of ratings many members will have the same reputation and thus the anonymity set of one single member contains all members with the same reputation. If the reputation system allows the members to give additional comments regarding their rating, the possibility for the formulation of comments has to be limited as well to guarantee an appropriate anonymity set. This gives members the possibility to

determine the linkability of their actions within the community. After an appropriate time the members of a certain anonymity set should change their pseudonyms to new ones to reach unlinkability to their past interactions but they will still be able to use the same reputation.

Because the change of a pseudonym and the corresponding reputation usually is costly and needs many members to participate, there has to be made a trade-off between the costs of a pseudonym change and the linkability of information regarding a pseudonym.

Beneath these privacy measures every member's accountability for his interactions has to be guaranteed. Also in privacy-enhancing identity management systems every pseudonym has to be linkable to a real name for at least identity providers where the member has registered himself as a member and under a pseudonym.

Future research on this topic and the design of a prototype within a privacy-enhancing identity management system will be executed at TU Dresden.

10.4 References

Asokan N., Shoup Victor, and Waidner Michael (1998); "Asynchronous protocols for optimistic fair exchange", IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos, 86-99, 1998.

Chaum David (1984); "Showing credentials without identification. Signatures transferred between unconditionally unlinkable pseudonyms". EUROCRYPT 85, LNCS 219, Springer-Verlag, Heidelberg 1986, pp. 241-244.

Clauß Sebastian, Köhntopp Marit (2001): "Identity Managements and Its Support of Multilateral Security"; in: Computer Networks 37 (2001), Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219.

Clauß Sebastian, Pfitzmann Andreas, Hansen Marit, Van Herreweghen, Els (2002); "Privacy-Enhancing Identity Management"; The IPTS Report 67 (September 2002) 8-16.

Dellarocas, Chrysanthos (2000); "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior"; Proceedings of the 2nd ACM Conference on Electronic Commerce, October 2000.

eBay. Annual report 2003. available from http://investor.ebay.com/annual.cfm, 2003.

Federal Trade Commission (2003). "Internet auction fraud targeted by law enforcers". available from http://www.ftc.gov/opa/2003/04/bidderbeware.htm, 2003.

Graeme Wearden (2004); "Judge raps eBay over fraud", December 7, 2004. http://news.com.com/2102-1038_3-5481601.html

Harris Interactive (2002). "First major post-9/11 privacy survey finds consumers demanding companies do more to protect privacy". Rochester Feb. 2002, http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429.

Köhntopp Marit and Pfitzmann Andreas (2004); "Anonymity, unobservability, and pseudonymity - a proposal for terminology". Draft v0.20., September 2004, available from http://dud.inf.tu-dresden.de/Literatur_V1.shtml (v0.5 and all succeeding versions).

Kollock Peter (1999); "The production of trust in online markets". Advances in Group Processes (Vol. 16), Greenwich, CT: JAI Press., 1999.

Pew Internet & American Life Project (2000); "Trust amd privacy online: why americans want to rewrite the rules". http://pewinternet.org/reports/loc.asp?Report=19, 2000-08-20.

Steinbrecher Sandra (2004); "Balancing Privay and Trust in Electronic Marketplaces", DEXA Conference on Trust and Privacy in Digital Business, LNCS 3184, Springer Verlag Berlin, pp. 70-79.

Waidner Michael (1996); "Development of a secure electronic marketplace for Europe". ESORICS 96, LNCS 1146, Springer-Verlag Heidelberg, pp. 1-14.

11 Understanding the Identity Concept in the Context of Digital Social Environments, INSEAD

Thierry Nabeth, INSEAD

11.1 Executive Summary

This document, which aims at contributing to the understanding of the concept of identity in the context of digital social environments, starts by pointing out the rising importance of the social aspect in the use of the Internet, and digital social environments as a valuable field for investigation and research for the identity concept. It analyses in general the different identity issues that can occur in an online social context and in particular it indicates the importance of social identity (an abstract and informal identity) in this context. It then provides an overview of the different categories of digital social environments (which include the email, forums, blogs, wikis, MMORPG, electronic marketplaces supporting reputation, etc), and for each of them illustrates the identity issue by a short example, case or a scenario.

This paper then concludes by indicating some research directions on identity in online environments, and in particular how to articulate the more traditional formal approach of identity with the more informal one (abstracted identity).

11.2 Introduction

The Internet is increasingly becoming more alive and more social, moving away from the idea of Internet as only a gigantic encyclopaedia or a massive shop, and in which the interactions only happen with machines. People today not only use the Internet more and more to interact others people, but they use it to socialize, to generate some lasting relationships, and even to develop a "real" social virtual life (in online forums, chats, massively multi-player online games, etc.).

In this context, the online identity that people develop represents a critical element of the activities taking place in these virtual spaces. This digital identity - that represents how they are perceived in the online environment -, has a direct impact in enabling or preventing the social interaction, and on the nature of the interaction (for instance you do not interact the same way with someone that you know and you trust than with someone for whom you have no information at all). This online identity can be explicit, and managed by some forms of identity management systems, or can be more abstract and diffuse. In the latter case, it includes the *social identity* that people develop on line, and that exists in the form of the reputation that they acquire (in forum, blogs, etc.), or the network of relationships that they build (in "friends" specified in their blogs, in the Instant messaging buddy list, etc.).

Importantly, and contrary to the off-line world, the trace of this "implicit identity" can be recorded in the digital space, be accessible to human agents, or mined and exploited by automatic mechanisms. This does not happen without posing a series of issues (trust, privacy, identity thief, etc.), in particular when you know that part of this digital life is becoming more prominent in people's lives, or that the frontier between digital life and real life is becoming blurred.

The objective of this document is to present an overview of digital social environments from the viewpoint of the subject of identity. Its aim is to raise awareness on the diversity and richness of these environments, and on the different identity issues that may occur in these environments.

The first part of this document consists in a general presentation and analysis according to an "identity" perspective of the concept of identity in the context of digital social environments. This document then presents the main categories of digital social environments, and illustrates each of them with a case or story presenting a particular issue. It then concludes by providing some directions of future thinking about online digital identity, and in particular the blurring of online and off-line words, the phenomenon of convergence (identity considered more holistically in the future), and the articulation between formal and informal identity.

11.3 Identity issues of Digital Social Environments

11.3.1 Introducing the identity issues of Digital Social Environments

The increase of the social dimension on the Internet

As the Internet is becoming more mature and is being adopted by a larger (and in particularly less technophile) portion of the population, its usage is becoming less centred on information, and more oriented towards the mediation of the social process. More concretely, people are increasingly using the Internet to engage in activities that include a strong social dimension such as: the participation in communities of interest (intervening in online forums and other virtual community spaces), the expression of their opinions, visions, and description of their lives etc. via personal journals that are made available to others (the "blogging phenomenon" (Kumar et al. 2004)), the exchange of opinions and the building of reputation (examples include reputation systems' mechanisms found in eBay), the participation in online games or virtual worlds in which the players intervene as avatars, or the use of matching systems (dating systems, social networks) which are used to help the establishment of relationships with other people and to exploit them. If the social dimension of the Internet is not new (emails and newsgroups have supported the social process for years), it is however changing in nature since it is now becoming accessible to the "non-geek" population, is more deeply supported (they are no longer seen only as "side products", and for instance social network systems aim at explicitly supporting them), and is experiencing a major revival after the new evolution of the World Wide Web as a less information-centric and a more service-oriented system (see for instance (Fox et al., 2005) for some predictions about the evolution of the Internet).

The importance of Identity in Digital Social Environments (DSEs)

In the context of these "socially enhanced" spaces, the online identities that people construct and develop represent critical elements: The quality of these identities (representing the images of themselves that they project in these environments and therefore how they are perceived) has direct implications on the value obtained from these spaces and the quality of the interaction. Obviously, people do not interact the same way with people that they know and trust (even if they have never met them in real life) than with perfect strangers. These identities are complex, since they include both the explicit personal identities (real or faked) that are managed via digital identity management systems or declared by people by filing a

user profile, as well as the implicit social identities that people develop through their behaviours (postings, conversations, actions) and that are often recorded and made persistent in digital systems. This later "social identity", sometimes summarized as "you are who your network is", possesses a particular significance in the digital worlds, since contrary to the off-line world, it is explicitly represented (people's relationships are for instance captured in social network services software, behavioural traces are present in log files, etc.), and can therefore be exploited for instance in reputation systems to help in the forming (via social translucence mechanisms) of online reputations (one major component of social identity), and in some cases be mined and subject to profiling operations for automated utilizations.

Identity issues in DSEs

Online identities in these social enhanced spaces are raising many identity issues (reliability of the information, pseudonymity, privacy, identity thief, etc.), and therefore represent a very useful playground/laboratory for the analysis of identity issues in general, and abstracted identity (informal identities that can be extracted from data) issues in particular.

For instance, in many cases in these spaces it is difficult to check the validity of the information declared by a user, and therefore to trust the validity of the "displayed" identity (for instance people do not hesitate to change gender in online forums or online games). This is particularly true in the case of virtual worlds (gaming, virtual communities, virtual dating, etc) that people use for the purpose of changing for and experimenting temporarily with a more desirable life than the one they have in the real world (in other words, the value that people get from these worlds is exactly in the possibility to "pretend" to be someone else). For instance, a fantasy world will give an insignificant employee in the real world the opportunity to become a renowned knight (Steinkuehler, 2004), a blog will provide a professor the possibility to become a rock and cultural critic (Nardi et al., 2004), and a dating system will permit an introvert to overcome his/her shyness in an online world and to engage in some relationships with individuals of the opposite gender.

On the other hand, and at the same time, people may not be fooled by other people's "declared identity", when they can observe the behaviours of these people in these environments: there is a limit to what individuals can pretend to be and they can be betrayed by their behaviour. For instance (Berman and Bruckman, 2001) have conducted some research on the different way in which men and woman behave online, or if people's communication patterns can help to determine information about age, race, or national origin. In the famous musical comedy "My Fair Lady", based on the play "Pygmalion" by George Bernard Shaw, Prof. Henry Higgins, a renowned linguist, demonstrates his ability to determine the social and geographical origin of people just by analysing the way they talk. If this story is imaginary, the idea of the stickiness of social attributes (the way in which people talk in this case) is not, both in sociology (with for instance the work of Pierre Bourdieu in social capital, (Bourdieu, 1980)), and in people's beliefs.

Another element, pseudonymity, is extensively used in virtual digital environments, even for conducting the more serious or critical activities. For instance online gamers (but also people participating in online forums) typically choose names that help them better to live a fantasy. eBay vendors and buyers (eBay is an electronic marketplace providing reputation mechanisms) conduct their businesses using pseudonyms, and activists hide their real identity to protect themselves from retaliation when creating and posting in a blog (personal online journal used to express opinions).

In addition, the complexity and persistence of digital traces make it difficult for users to control sufficiently the disclosure of this information to third parties (for instance some people have been fired for posting information on their blog that they wrongly assumed to be a private space), and raise concerns related to privacy. Finally, spoofed/forged emails have been used in several cases to damage people's reputation (using spoof email of hatred messages).

Are DSEs identity issues really important?

It is of course legitimate to question the importance of these identities that develop in digital social environments and in particular the abstracted one (the social identity): after all, these virtual worlds are not real, and the consequences can only be minor, and in no way similar in identity to the issues that occur in the real world (identity thief, money laundering, and credit card forgery)! This would be forgetting that these digital social environments are gaining an increasing importance in people's lives. For instance (Stafford and Gonier, 2004) in a study of AOL users' population report that socialisation is now recognised as a significant factor for using the Internet, and a Pew Internet & American Life Project report ((Rainie, 2005) indicates that end 2004, 7% of the 120 million U.S. adults who use the Internet say they have created a blog, and 27% of Internet users say they read blogs. We can also add that the ruining of an online reputation can be disastrous in real life (when it happens for an eBay vendor or for a politician) and that the frontier between these worlds and the real world is progressively burring (for instance a project such as I-Neighbour helps to strengthen local bonds and social interaction by vitalizing real local communities, blended learning combining the online and off-line learning is increasingly attracting attention about the future of learning, etc.). Besides, the support of more informal mechanisms in identity management systems, such as the one found in reputation systems like eBay, is making people's activity more visible and accountable, and can in some cases provide more flexibility in managing certain identity and identification aspects than more formal ones which often rely only on one time authentication that can give a false feeling of security.

Better understanding the DSEs, their variety, and their identity issues

The objective of this paper is to contribute to the clarification of identity issues in digital social environments. Practically it consists in presenting and analysing, according to an "identity" perspective, the main categories of digital social environments, and in illustrating with cases or stories the identity issues that can be found in these environments. This paper does not pretend, however, to make an exhaustive inventory of all the possible issues, but rather to raise the awareness of the reader about the richness and the diversity of the identity concept in these environments.

11.3.2 Defining DSEs

Internet as a mediator of social activity

People, when using the Internet (in working, shopping, playing), are increasingly dealing with other humans rather than only information or machines.

Indeed, as the Internet matures and is adopted by a larger portion of the population (of people who are not necessarily technophile and who are definitely more interested in the "human and social life"), its role as a tool for mediating human interaction is becoming more prominent.

People are participating in the digital forums of communities of interests, are "chatting" with friends using Instant-messaging tools, or are having a new life playing in the massively multi-player online games. Interestingly, even the more traditional information perspective (Internet as a big information repository) is becoming extended with social aspects helping to better manage this information: For instance opinion and social translucence mechanisms (Erickson et al., 2002) are used in electronic marketplaces such as eBay to facilitate the evaluation of the quality and the relevance of product information, and coordination mechanisms are used for instance in Wikipedia to facilitate the collaborative construction of an online encyclopaedia.

This usage of the Internet for supporting people's communication is not new, and was actually relatively important before the advent of the Web, with systems such as email, chat systems (IRC), newsgroups and other forums. However, with the maturing of the Internet (with reliable high speed infrastructures - more than 50 percent of the total U.S. Internet population access the Internet via broadband (Hu, 2004) -), its democratisation (making it very affordable to all the classes of the population), and its ease of use (new tools like blogging do not require you to be a technical expert), we can observe a radical transformation of the demographics of the user population, and consequently of the usage: a significant portion of the population (in the most advanced country) is now integrating the Internet directly as part of their life (to get informed, to communicate with others, to shop, to learn), and in some cases (for instance with the case of massively multi-user online games) creating totally new life territories in which they can develop a life having a strong social dimension.

What are digital social environments (DSE)

In this paper, we define Digital Social Environments (DSE) as the category of Online Environments that provide some form of support to the social process. This definition therefore covers all the digital environments that we have mentioned in the previous chapter. This definition is rather broad, and includes a variety of systems ranging from very explicit and centralized community systems directly supporting people's interactions (such as virtual community platforms or forums), to some more decentralized communication systems that are supporting a more peer-to-peer mode of interaction and that are directly controlled by their users (for instance email, Instant messaging systems, blogs). DSE also include environments that do not directly support people's interactions themselves, but provide some services of intermediation. In a similar way these services can be centralized (for instance a system like eBay which provides some matching services between vendors and buyers, and implement a series of reputation mechanisms), or decentralized (such as in the case of online social networking systems like LinkedIn in which people manage individually their social network, or peer-to-peer networks that are used to directly exchange digital items).

	Interaction/communication	Intermediation
Centralized (Collectively controlled)	Virtual community systems, Forums, Wiki, MMOG, CMS, etc.	Marketplaces (reputation and recommender systems), …
Decentralized (Individually controlled)	Blogs, Instant messaging, email, etc.	Online social networking, peer-to-peer networks, etc.

Table 1: DSEs centralization / interaction

"Table 1: DSEs centralization / interaction" summarizes this categorization of DSEs according to their centralized or decentralized nature, and on their main role (support for the interaction or intermediation), although in reality the frontier is not always very strict, and that we see some movement of convergence and merging of these systems into more holistic ones (for instance Bill Gates in (Kanellos, 2005) suggests for the future the integration of everything – social networking, blogging, instance messaging, etc.- into a single system).

11.4 Illustrating the Identity Issues in Digital Social Environments

In this section, we are going to provide a more concrete overview of the different categories of the digital social environments, and for each of them, we will give an example, case or scenario illustrating a particular issue.

11.4.1 Electronic mail

Description and identity issues.

Email communication represents one of the most important tools used on the Internet (Stafford and Gonier, 2004), and one of the oldest. Electronic mail represents the principle means for people on the Internet to communicate directly and asynchronously with one another, which consists in the transmission of a message to a given electronic destination of the receiver.

The Identity in email systems is essentially managed via the email addresses (identifier@domain) that people utilize to communicate with one another. Practically, people's authentication is done by the "sender" attribute in the email. Privacy is protected by the non-disclosure of this email to third parties (which may be difficult because this information may be transmitted from a party that was originally trusted). Some information can be inferred from the domain of the email address (this domain sometimes represents the name of the organization to which the user is affiliated, such as a company or a university). Electronic mail is sufficiently well known to have to further describe it in this document.

The management of this email is therefore extremely primitive, and includes many flaws, resulting in many identity issues and problems. First, an email address associated with an organization does not usually provide any indication related to the level of the affiliation (we can however mention the exception of the email addresses issued for alumni of big universities, which indicate the affiliation of the person). Second, the email address can very easily be forged (and appear to originate from an entity or a location different from the actual source) with the objective of misleading the reader about the origin of its initiator. This forging, also called spoofing, has been used in some cases to harm the reputation of individuals or organizations by making them "say" things considered as inappropriate. Spoofing is also frequently used by spammers to force some of the protection of basic email filtering. This spoofing is also used in phishing activities (pretending to be a trustful organization) aiming at "extorting" credit card information. Third, email can be borrowed and used without the knowledge of its owner. In the latter case, this could mean of course the theft of the user's account, but much more often originates from some virus activities (such as the Melissa Virus that was spread by sending itself via email on behalf of the user's email account, but without his knowledge). Fourth, we can mention the problem of the "calamity"

spamming, which outrageously uses people's email addresses totally against their will. Finally, we can indicate some serious privacy issues that have appeared with the major Internet player Yahoo, which in exchange for a free massive mailbox, ask the right to mine the content of the emails in order to display automatic advertisements based on the text of e-mail messages (McCullagh, 2004).

To conclude, email represents very insecure systems related to the management of identity. On the positive side, people happen to know about it and are able to live with it, even if some advanced cases of phishing continue to lure the more naïve users, and if the exploitation of email systems by viruses or spamming companies continue to represent a major problem.

A short case of email identity forging, and the consequences for a person's reputation.

In October 1994, someone broke into the computer account of Grady Blount, a professor of environmental science at Texas A&M University, and sent out racist email to more than 20,000 people on the Internet. The message brought death threats and other harsh responses from nearly 500 users and seriously harmed the reputation of this professor, and threatened his career (Blount, said that even his research grants were put in jeopardy as a result of the incident.).

This case underlines the risks of identity forging in the "e-mail virtual space", resulting in very real consequences in the off-line world.

11.4.2 Virtual Community Environments

Description and identity issues.

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) share 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 (typically social pressure).

The management of Identity in virtual community systems covers a variety of aspects. First, the participants in these environments are usually registered as members (they login to these systems to be authenticated), and are visible in these environments via a pseudonym that they have chosen. They can also if they decide display other characteristics described in a user profile, such as age, interest, and other information that can be relevant to the purpose of this community (for instance a community of technophiles will typically display the technological hardware configuration of its users). More interestingly, these systems may also display other characteristics such as the "social status" (e.g. wizard), the position (e.g. moderator) the level of experience (newbie, experienced) or the level of activity of the members, helping the others to make an assessment of their seriousness. It is not uncommon that this latter information to be used to enforce social control (a newbie will for instance be reminded his/her little experience, and be denied some actions). However, one of the most important identity dimension that people use is the social identity (reputation, etc.) that they develop in these environment, and that reflect their behaviour and attitudes and that can be observed in their

postings in the public spaces, as well as in the social relationships they have established with others.

The identity issues that can be found in such environments are mainly the social issues that can be found in the real world, and that are sometimes magnified in these digital spaces, because of some feeling of impunity perceived by some of the new members (older members usually are much more careful to behave well in order to maintain a reputation that is so important to maximize the value that they get from these spaces such as help, recognition or fun) and the perceived easiness of communication. Practically, one of the nuisances in these environments called trolling consists in trying to destroy the good disposition in these communities by surreptitiously creating disorder and frustration (trolling attempts to provoke outraged responses from other forum users) among people who have a feeling of impunity for their action because of some level of anonymity (they use weak pseudonyms with little reputation attached). Another problem is related to identity phishing such as in the case of switching of gender (women for instance receive more attention and are usually better supported in forums, but people may also switch in order to experiment with a new identity (Berman and Bruckman, 2001)). Virtual community environments also raise a question of privacy: the traces that people leave in the shared spaces are accessible for automatic monitoring and analysis. For instance, some research experiments funded by intelligent agencies have been conducted to spy on the activities of chatrooms (McCullagh, 2004b). We can easily imagine that the mining of forum can also easily be achieved, for instance to identify deviant behaviours! Finally, on a different level, we can mention the use of social psychological theories taking advantage of identity information, to manipulate the people "inhabiting" these communities (for instance (Beenen et al., 2004) investigate strategies to be activated to motivate the contributions to online communities, but we can easily imagine other manipulations aiming at far less acceptable objectives).

A practical illustration: The Strange Case of the Electronic Lover

This case (Van Gelder, 1991) tells the story of Joan Sue Green, "…a New York neuropsychologist in her late twenties, who had been severely disfigured in a car accident that was caused by a drunk driver." The accident killed Joan's boyfriend and left her mute and confined to a wheelchair. But, through the use of her computer and the participation in a BBS (Bulletin Board System), Joan was able to befriend many users and let her bubbly personality shine.

The reality proved to be different: Joan was not a disabled person, … and Joan was not a "She"!

This case illustrates the particular issues and the seriousness of "social phishing": the person of this real story was for instance able to extract very intimate information from discussion in the online system. We can very well imagine even more serious problems in the case of sexual maniacs accessing spaces frequented by children, and putting them at risk.

11.4.3 Blogs

Description and identity issues.

Blogging represents the last avatar or "phenomenon" of the "Internet revolution", and is developing at a tremendous rate (Kumar et Al, 2004). Blogs are online journals that are commonly used to chronicle the lives and opinions of their authors. Blogging provides the possibility for people to develop a personal identity that they are able to project in a social space (the bloggosphere) and to enter into interaction with their audience (visitors are invited to comment the blog postings of the owner of the blog). Blogs are also often interdependent: people frequently quote postings from other blogs and some mechanisms are provided to support this cross-referencing between blogs (for instance the trackback is used to notify automatically to another blog that it is being referenced). Besides, blogs often reference explicitly other blogs (acquaintances), creating some networks of blogs.

The management of Identity in blogs should appear to be quite simple, since these blogs are totally controlled by their owners, and are associated to the private sphere (at least for the personal blogs). The reality, however, is more complex. First, in a blog a user can reveal a great deal about himself/herself without fully perceiving the extent of this provision of information (blogging systems are very easy to use technically and posting is often impulsive, and besides the perception of the audience is not very elaborated). One of the main problems with blogging is the lack of clear separation between the private sphere and the public sphere and the risks of information leaking that can happen (for instance (Suitt, 2003) discusses a Harvard Business Review case related to personal blogging in a work context and its implications). Another issue is related to the trust that can be attached to the bloggers and which is connected to the image (identity) that the bloggers project in the online world. Indeed, as the bloggers are posting some significant information that is impacting the "information sphere" (many bloggers improvise as apprentice journalists and publish information that is propagated), it is important for the reader to assess the reliability of the "editor", and therefore know better his/her identity (the risk being that the reader is misled by unverified information, or is manipulated by fanatical groups).

If the control and regulation of blogging appears to be individual and social (social pressure), we can mention some tentative orientation towards more central control originating with the phenomenon of convergence of identity management in the different electronic media. For instance, Microsoft is working on a global identity management approach (with the same account encompassing email, instant messaging, blogging and online gaming), and its latest blogging system MSN space, is now controlled and subject to automated censorship (MSN is considered to be liable for the content posted on the spaces no longer seen as totally private).

A Case: being fired after posting on a blog.

"If you've got a blog and a job, beware. The two sometimes don't go together, as many ex-workers are finding out". (Metz, 2004) reports several cases of problems that have occurred for people who posted on a personal blog, and who had some problem with their work. Concretely, a flight attendant in Texas, a temporary employee in Washington and a web designer in Utah were all fired for posting content on their blogs that their companies disapproved of. A similar story also happened recently in the UK, where an employee was fired because of what he posted on his blog (Barkham, 2005).

This case exemplifies the increasing difficulty of separating the private sphere from the working sphere in the Information Society (privacy issues), and with very concrete and real offline consequences.

11.4.4 Wiki

Description and identity issues.

A Wiki or WikiWikiWeb is a website (or other hypertext document collection) that allows users to collectively write documents using a web browser and a simple mark-up language for formatting these documents. One of the defining characteristics of wiki technology is the extreme easiness with which pages can be created, hyperlinked with one another and updated (wiki comes from the Hawaiian term for "quick" or "super-fast"). Generally, there is no prior review before modifications are accepted, and most wikis are open to the general public - or at least anyone who has access to the wiki server. The most significant example of a wiki is Wikipedia (http://www.wikipedia.org/), a free web-based encyclopedia authored by hundreds of individuals. Wikis implement perfectly one of the original ideas of the Internet culture related to its altruistic nature.

The management of identity in wiki systems is currently rather unsophisticated (people usually only need to register under a pseudonym, but they can sometimes remain anonymous, and then can immediately contribute), although we can mention different categories of problems such as: the reliability of the information posted, problems of plagiarism and of vandalism. Social control (including the emergence of roles such as librarians), as well as some mechanisms of content versioning, and IP blocking are used ways to address these problems. We can however imagine, as wikis are adopted by populations driven by less altruistic goals, that more formal identity and identification mechanisms need to be employed.

A case of Vandalism in a Wiki

Wikipedia is experiencing some vandalism in its site (and as an answer is blocking the vandals). For instance a self-styled god named Sollog who is unhappy with the Wikipedia article on his object of worship, is repeatedly posting articles that include God, Jesus, the Devil, Jim Wales, George W. Bush, Britney Spears, Nostradamus, Adolf Hitler, Einstein, Sollog, Wikipedia, in articles linked on the main page.

This category of behaviour raises again the issue of control, of censorship and of liability, in this category of online systems in which the management of identity is usually relatively weak.

11.4.5 Instance Messaging (IM)

Description and identity issues

Instant messaging (IM) are real time communication systems that allow an individual to communicate immediately in real time with another user (other usages include the creation of temporary private chatrooms supporting the instant communication of groups of individuals). Examples of Instant messaging systems include Yahoo! messenger, Windows messenger, AOL instant messenger or Exodus (used in the open source community). IM systems represent an important communication tool that is used by millions of Internet users ((Shiu and Lenhart, 2004) indicate that 53 million adults trade instant messages and 24% of them swap IMs more frequently than email).

The management of identity in IM systems is rather sophisticated. The management of identity in IM systems comprises an in-depth user profile describing the characteristics of this

user (age, location, picture, interest, etc.) and well as a list of contacts (buddy list referencing the instant messaging acquaintances of this user). Users are also able in an interaction to use some visual tags (emoticons) to indicate mood or emotion (which can help the establishment of confidence). An interesting concept supported by IM systems is the management of presence. Practically users are able to indicate to others (and reversely receive indication from others) about their online status: if they are online or offline, busy or available for interaction, or invisible (the users are in control of the indication of their online presence).

One of the main identity issues with IM is the invasion of privacy (Saunders, 2002)). In a study (Patil and Kobsa, 2004) have identified three privacy concerns: Privacy from Non-contacts (i.e. people who are not part of the contact list), privacy regarding availability (busy/available, at home/at work, etc.) and privacy regarding content (which has to do with the sensitivity of the content of the IM conversations). The privacy regarding the content also relates to the saving of conversations and their divulgation to a third party without the consent and knowledge of one of the parties (therefore a user may have to be liable for private talks happening in an informal chitchat).

Finally it is useful to remind ourselves of the importance of the role that the IM identity should play in the future in the idea of convergence of different online systems (IM, blog, forum, etc.) into a single system for which the big players of the Internet (Yahoo, Microsoft, Google, AOL, etc.) are showing a strong interest.

Digging in IM logs for evidence in a case of law.

In September 2003, in the context of an investigation of security fraud, state and federal prosecutors for the first time searched IM records of licensed brokers and dealers (Smith, 2003). It seems that the investigators were able find evidence in the IM traces of a former Bank of America broker which were related to the execution of after-hours mutual fund trades.

This case illustrates concretely the possibility of observability of online chatting activities and the risks of privacy invasion (for the good cause in this case, since it was used for helping to fight crime).

11.4.6 Online Social Networking Services

Online social networking services (OSN) represented the latest avatar of the "Internet revolution" (Braunschweig, 2003) … before the blogging phenomenon took over this "title". Socialware are services that are helping individuals to manage and develop their social relationships. Social capital represents indeed a critical element of individual performance in the knowledge economy characterized by less institutional stability and fewer reliable corporate resources (Nardi, 2000) and in which the individual has to behave more autonomously. OSN intervene in a number of domains (Li, 2004; Leonard, 2004): friendship (with friendster.com), business relationships (with LinkedIn, Ryze), jobs (Borzo, 2004), community of interest (Orkut, Tribe), etc. To some extent, we can consider that online dating services belong also to the category of OSN.

Practically, OSN are matching and intermediation services based on two elements: (1) the definition of a user profile in which people can specify their interests and affiliations (people can have this affiliation "confirmed" or endorsed by other members of the network); (2) the

explicit specification of a social network of acquaintance that is built via a series of invitations to join the social network by other members of the network. It is important to note that a member is not obliged to accept this relationship, and therefore that a relationship is always the result of an acceptance by both parties (the one that has initiated the relationship, and the one that has accepted the relationship to be established). Different services, exploiting this information and in particular the network, are then possible such as: searching for people (the results are displayed according to social proximity); intermediation (invitations can be relayed via this network from one member to another). In addition, the members have also some control on the visibility of their network for others. For instance some members can decide to make visible their social networks only to their direct acquaintances.

If the online social network represents a fascinating field of practical application of some important social theories, and in particular the theory of the Small World or the Six degrees of separation by which on average the distance in social networks between complete strangers is less than six (Watts, 1999) or the theory related to the power of weak ties (Granovetter, 1973), it is not totally exempt of critics. For instance some people have raised the question of the quality of the networks that are being constructed using OSN. Indeed we can imagine that no serious person (and in particular businessmen, salespersons or top executives) will enter in an electronic system some information that he/she really considers as critical. Besides, some interesting behaviours have been observed such as contest for creating the biggest networks in such systems (Leonard, 2004). Other voices have indicated the nuisances that have appeared in these systems from people who are trying to construct their social identity and who do not hesitate to contact perfect strangers (Kahney, 2004; Leonard, 2004).

Still, the concrete representation of this social identity (social networking) which in the real world was always implicit provides a very interesting possibility opened by online environments that is worth a further investigation from the identity specialists. People are human and are “social animals”, and therefore representing and managing digitally the human and social dimensions is important, and can possibly open many opportunities that make use of these categories of identity to offer services that have the maximum impact and benefit for the end user.

Multiple OSN for multiple identities

“I soon found myself behaving in different ways on different networks. On Friendster, I looked for people to date. On Tribe.net, I joined tribes and participated in discussions. On LinkedIn, a business-oriented service, I didn't do much of anything at all. On Orkut, I went friend-crazy. Orkut was where "my" people were hanging out, the geeks and techies and online journalists”. *Leonard Andrew*.

This example (Leonard, 2004) just illustrates the usage of OSN for an experienced “netizen”, and underscores the strategy adopted for organizing his “online social network life” that isolates different life spheres (dating, discussion, business, friendship).

11.4.7 Reputation systems

Electronic commerce is no longer only seen as a very “efficient” procurement system optimising the matching between the demand and the offer as well as the supply chain, but also as a space where the different actors (both vendors and buyers) can interact with one another. For instance, before engaging into a business transaction, customers will use the

Internet to collect opinions from other customers that will help them to decide what product to buy and which vendor to choose. Electronic commerce also comprises the establishment of closer relationships between the vendors and the customers, and in particular more direct interaction: for instance the creation of a blog for commerce will allow a vendor to communicate information to its prospective clients, but also to engage in an interaction with them. Finally, electronic commerce also includes the reputation systems, popularised by eBay, and which represent electronic marketplaces enhanced with mechanisms supporting the establishment of reputation.

Practically, reputation systems are based on the gathering of comments from buyers and sellers about each other after each transaction, and about making this information visible to the whole community (Resnick et al., 2000). In a reputation system, a new prospective buyer for a product can get access to the whole history of the transaction of the vendor of the product, as well as all the comments that this vendor got from the previous buyers. Obviously bad opinions on previous transactions or the absence of opinions (in the case of a new vendor) will raise suspicion about the seriousness of the vendor, and will seriously reduce the willingness of clients to engage in a transaction. In a similar way, a vendor has the possibility to check the reliability of a client interested by his items, and to decide to refuse to proceed with the transaction. In the latter case, indicators of unreliability of the client include the online age of this customer, the number of transactions that this customer has engaged in in the past, and the opinion that this client gave to other vendors or received from them.

It is very clear that one of the main functions offered by reputation systems is the support for the establishment of an explicit online reputation of the different actors (vendors and clients) involved in an electronic marketplace. This reputation can be considered as an attribute attached to the identity of this actor, and more particularly to its social identity.

The management of this "social identity" is working very well if we observe the success of the company that first implemented the concept (eBay), and its introduction in numerous marketplaces. It requires indeed a minimum of effort and control from the operator of the marketplace infrastructure since it relies on the concept of transparency, and on the contribution of the different actors for establishing the opinions. Interestingly, vendors are strongly encouraged to invite their customer to provide feedback, since it represents for them a main manner to raise their reputation in the marketplace and therefore to increase their profit. Indeed, a good reputation is important not only to attract more customers, but also to justify higher prices (for instance in an experiment on selling postcards (Resnick et al., 2002) has determined that the difference in buyers' willingness-to-pay between reputable vendors was 8.1% of the selling price).

Still, reputation systems (that can also be applied outside the field of the electronic commerce) are not without raising a number of issues and are at the origin of several problems. The first problem is related to the subjective nature of rating and the cultural biases: people are different (some people are harsher than others) and have different cultural values. The risk exists therefore that the constructed social identity does not reflect accurately the reality. Besides, inconsiderate social transparency can in some cases have a negative effect of reinforcing conformance in (virtual) society, "punishing" deviance, and encouraging segregation. The second problem is related to reputation manipulation. For instance (Dellarocas, 2000) indicates that the rating of sellers can be unfair (intentionally false) in order to artificially raise the reputation of a vendor (as would be the case when a vendor creates false transactions just to increase his/her reputation), or decrease it (as conspiring

buyers or competitors would do). In his paper, however, (Dellarocas, 2000) indicates some mechanisms to use to fight again this identity falsification. Finally, we can also raise some ethical issues: how far can social identity be managed and processed by automatic mechanisms that can impose important pressure on individuals (for instance, in the case of the eLance marketplace, in which the goods that are traded are small consulting missions).

Note: Reputation systems such as eBay are sometime associated with auctioning. Mechanisms of bidding are therefore used to establish the price of the goods in this market. It is interesting to mention here the Shilling fraud, an illegal practice in which sellers bid on their own items or persuade friends or associates to do so in order to drive up the price (Brunker, 2000), and that is made easier on the Internet because of the current weaker level of electronic identities.

Fraud at eBay

Should knowing about the seriousness of a vendor from the aggregated feedback of many participants in a marketplace provide a strong sense of security, or not?

This article (Warner, 2003) suggests that people should think twice before trusting too much an identity reflected by a reputation system. Jay Nelson was able to extract $200,000 on eBay, before being caught and his real identity revealed. Jay Nelson had an excellent reputation on eBay however. It just happened that Nelson managed to use several strategies to boost his eBay reputation, such as: multiple user IDs (that he used to generously give himself rave reviews), but also initially selling computers legitimately to create the illusion of authenticity. By the time negative feedback started rolling in from his subsequent fake auctions, Nelson was on to a new identity.

The fact that eBay was able to put in place some mechanisms reducing the possibilities of "scammers" and that Jay Nelson was finally arrested, should not prevent us being careful about the limit of these online identities, even if they appear to be the result of the feedback of a multitude of honest people.

11.4.8 Other DSEs (MMORPG, peer-to-peer network, etc. ….)

Several other DSEs can be mentioned in this paper and can raise very interesting Identity issues. For instance, the domain of entertainment MMORPG (Massively Multiplayer Online Role Playing Games) has opened a whole new space of digital Universes in which participants are able to live lives (and create identities) that were only present in their wildest dreams in the past, or in fairy tale books. Peer-to-peer networks (Kazza, Napsters and the likes), that are used to mediate the exchange of digital media, represent another category of DSEs. Peer-to-peer networks strongly rely for their functioning on the indicators of the level of contribution of the participant (amount of digital media that they make available to the community) and therefore on some form of identity (even if the pseudonyms employed are very much protecting the anonymity). More concretely, the more digital media a given user will contribute, the more this user will be granted bandwidth resource. This same indicator is also employed by music companies to determine the level of piracy of this user and can be used as evidence in a prosecution.

As already indicated previously, it would be wrong to underestimate the importance of these digital spaces in which people dedicate an increasing amount of their time. To detractors that

refute the value of these activities and their importance, we will answer that they are really becoming a "real" part of people's lives (Fattah and Paul, 2002), and in the particular case of gaming, we will provide this quote: "isn't the distinction between game and life not arbitrary?" (Steinkuehler, 2004).

Griefing in Online games

"As online-game companies court new and wider audiences, many are running into an old problem: "griefers," a small but seemingly irradicable set of players who want nothing more than to murder, loot and otherwise frustrate the heck out of everyone else. An increasing number of game companies are fighting griefer damage using a combination of technology, sociology and psychology".

David Becker (2004)

This example raises the question of the consequences of weak identities in the Online Gaming environment, and indicates some direction for addressing the associated problems.

Cheating in Online games

"A small but fractious minority in online gaming circles, cheaters can suck the fun out of a game by introducing homemade characters with unauthorized powers, making it impossible for opponents to win or even survive. They can also quickly pollute the social atmosphere critical to many games".

David Becker (2002b)

This example indicates some technical "hacking" in Online Gaming that allows some individuals to acquire unfair capabilities.

Selling an "Identity" of online games

"Like most RPGs, players can swap items within the game using the game's virtual currency. But many players prefer to get real money, selling items and characters on auction sites such as eBay or specialty barter sites, including CamelotExchange. A search of eBay showed more than 150 DAOC items available Thursday, including online accounts with several highly developed characters selling for $300 or more".

David Becker (2002)

This example illustrates the transferability and the trading of identity in an online world.

11.5 Conclusion

The conceptualization of identity in DSEs (Digital Social Environments) that we have presented in this paper relies to a large extent on a more informal and abstracted perspective of identity than the concept of identity manipulated by the information system or security specialists. Whereas in the last case the identity is managed principally with people representations (as a set of attributes and characteristics that can be stored for instance in an identity card) and their authentication (usually happening once at the beginning of a session), the management of identity in social environments is more diffused, and in particular its control is not granted to a central authority but based on the idea of providing transparency

about the behaviours and the actions of people, and is socially regulated (for instance with social pressure).

Still, a closer look indicates that the two worlds (formal and informal perspective) are not totally alien but are on the contrary complementary, and are subject to cohabit more and more in the future, in particular as the identity issues in the Information Society are addressed more holistically. Indeed, as the frontier between the physical and the digital worlds is becoming blurred (this is best illustrated by the advent of ambient intelligent environments) and is converging, as this new world is becoming very complex and difficult to manage by traditional methods (via explicit identity and identifier, and one time authentication), and as the Information Society is becoming interested in supporting more widely human aspects (privacy, social dimension, etc.), new methods (in particular more flexible and more robust) will need to be activated to manage the identity in our societies.

Social mechanisms (reputation, social control, etc.) represent an effective means of regulation for complex systems, and should be considered (at least for a partial use) in every identity management solution. In particular, social engineering approaches to systems that include an important human component (including management of risk associated with inevitable human errors and biases), a category to which identity management systems belong to, are often more effective and more robust approaches than the technical engineering approach alone. This paper has also indicated that the use of social mechanisms also has its limits, and that the management of identity in DSEs could benefit from the work of the more formal management of identity.

In conclusion, we can consider as suggested in (Jordan, Hauser, and Foster, 2003), that the two approaches are complementary and should be combined in order to implement systems that are more flexible, more robust (in particular concerning human error) and more reliable, for designing the next generation of Internet systems that will be more socially aware, and more humanly friendly than they are today.

11.6 References

Barkham Patrick (2005); “Blogger sacked for sounding off”; The Guardian, Wednesday January 12, 2005

Becker David (2002); “Game exchange dispute goes to court”; Cnet news.com, February 7, 2002

Becker David (2002 b); “Online gaming's cheating heart”; Cnet news.com, June 7, 2002

Becker David (2004); “Inflicting pain on 'griefers'”; CNET News.com, December 13, 2004

Beenen, Gerard, Ling, Kimberly, Wang, Xiaoqing, Chang, Klarissa, Frankowski, Dan, Resnick, Paul, and Robert E Kraut (2004). "Using Social Psychology to Motivate Contributions to Online Communities". To appear in *Proceedings of ACM CSCW 2004 Conference on Computer Supported Cooperative Work*, Chicago, IL. 2004

Berman, Joshua and Amy Bruckman (2001); “The Turing Game: Exploring Identity in an Online Environment”; *Convergence*, 7(3), 83-102, 2001.

Borzo Jeanette (2004); “Online Social Networks Are Havens for Job Hunters”; CareerJournal.com, September 23rd, 2004
http://www.careerjournal.com/jobhunting/networking/20040923-borzo.html

Bourdieu, Pierre. (1980), “Le capital social: notes provisoires”. In *Actes de la recherche en sciences sociales*, volume 31, pp. 2-3.

Braunschweig Carolina (2003); “The new Internet Gamble”; Venture Capital Journal, December 2003

Brunker Mike (2000); “EBay reins in anti-shilling ‘posse’”; MSNBC, Oct. 26, 2000
http://www.msnbc.com/news/481550.asp

Castronova Edward (2004); “The Price of Bodies: A Hedonic Pricing Model of Avatar Attributes in a Synthetic World”; *Kyklos*, Vol. 57, No. 2, pp. 173-196, May 2004
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=546921

Castronova, Edward (2003), "The Price of 'Man' and 'Woman': A Hedonic Pricing Model of Avatar Attributes in a Synthethic World" (June 2003). CESifo Working Paper Series No. 957. http://ssrn.com/abstract=415043

Dellarocas, Chrysanthos (2000); “Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior”; Proceedings of the 2nd ACM Conference on Electronic Commerce, October 2000.

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

Fattah Hassan, Paul Pamela (2002); “Gaming Gets Serious - market, survey data on online gaming - Statistical Data Included”; American Demographics, May 1, 2002

Fox Susannah, Janna Quitney Anderson and Lee Rainie (2005); “The Future of the Internet”; Pew Internet & American Life Project report; 9 January 2005

Friedman, E. and P. Resnick (2001). "The Social Cost of Cheap Pseudonyms." *Journal of Economics and Management Strategy* 10(2): 173-199.

Granovetter Mark (1973); “The Strength of Weak Ties"; The American Journal of Sociology, 78 (May): 1360-1380, 1973

Hu Jim (2004), “Study: Broadband leaps past dial-up”, CNET News.com, August 18, 2004.

Jean Camp L. (2004), “Digital Identity”; IEEE Technology & Society, Vol 23, No 3 pp. 34- 41 (2004).

Jordan Ken, Jan Hauser, and Steven Foster (2003); “The Augmented Social Network: Building identity and trust into the next-generation Internet”; First Monday, Volume 8, Number 8 — August 4th 2003 http://www.firstmonday.org/issues/issue8_8/jordan/

Kahney Leander (2004), “Social Nets Not Making Friends”, Wired magazine, Jan. 28, 2004

Kanellos Michael (2005); “Gates taking a seat in your den”; Cnet news.com, January 5, 2005 http://news.com.com/Gates+taking+a+seat+in+your+den/2008-1041_3-5514121.html

Kumar R., Novak J., Raghavan P., Tomkins A. (2004); "Structure and evolution of blogspace"; *Communications of the ACM* 47(12): 35-39, 2004.

Leonard Andrew (2004); “You are who you know”; Salon.com, June 15, 2004 http://www.salon.com/tech/feature/2004/06/15/social_software_one/

Li Charlene (2004); “Profiles: The Real Value of Social Networks”; Forrester Research, July 15, 2004

McCullagh Declan (2004); “Gmail and its discontents”, by, CNET News.com, April 26, 2004

McCullagh Declan (2004b); “Security officials to spy on chat rooms”, by, CNET News.com, November 24, 2004

Metz Rachel (2004); Blogs May Be a Wealth Hazard; Wired magazine, December 6, 2004 http://www.wired.com/news/culture/0,1284,65912,00.html

Nardi, B., Whittaker, S, Schwarz, H. (2000); "It's Not What You Know, It's Who You Know: Work in the Information Age"; First Monday, May, 2000

Nardi B., Schiano D., Gumbrecht M., Swartz L. (2004); "Why we blog"; Communications of the ACM 47(12): 41-46, 2004.

Patil, S. and A. Kobsa (2004): Instant Messaging and Privacy. Proceedings of HCI 2004, Leeds, England.

Rainie Lee (2005); “The state of blogging”; Pew Internet & American Life Project report, DATA MEMO, January 2005

Resnick, P., R. Zeckhauser, J. Swanson, and K. Lockwood (2002); "The Value of Reputation on eBay: A Controlled Experiment," U. of Michigan Working paper, originally presented at the ESA conference, June 2002

Resnick, Paul, Richard Zeckhauser, Eric Friedman and Ko Kuwabara (2000); “Reputation Systems: Facilitating Trust in Internet Interactions”; *Communications of the ACM*, 43(12), December 2000.

Saunders Christopher (2002); “Enterprise IM Spurs Privacy Concerns”; Instant Messaging Planet.com, November 18, 2002 http://www.instantmessagingplanet.com/enterprise/article.php/1502941

Shiu Eulynn and Amanda Lenhart (2004); “How Americans Use Instant Messaging”; Pew Internet & American Life Project report, September 2004.

Smith Elliot Blair (2003); "Wall St. Bloodhounds Track IMs for Clues"; USA Today, 23 September 2003. http://www.usatoday.com/money/companies/management/2003-09-18-ims_x.htm

Stafford Thomas F. and Dennis Gonier (2004); “What Americans like about being online”; *Communications of the ACM* archive, Volume 47 , Issue 11 (November 2004)

Steinkuehler, C. A. (2004). “Learning in massively multiplayer online games”; In Y. B. Kafai, W. A. Sandoval, N. Enyedy, A. S. Nixon, & F. Herrera (Eds.), Proceedings of the Sixth International Conference of the Learning Sciences (pp.521–528).Mahwah, NJ: Erlbaum.

Suitt Halley (2003); “A Blogger in Their Midst”; *Harvard Business Review*, vol. 81, no. 9, September 2003.

Van Gelder, Lindsy (1991); "The Strange Case of the Electronic Lover"; In *Computerization and Controversy: Value Conflicts and Social Choices*, edited by Charles Dunlop and Rob Kling, Pages 364-375.

Warner Melanie (2003); “eBay's Worst Nightmare”; FORTUNE, Monday, May 12, 2003

Watts Duncan (1999); “Small Worlds: The Dynamics of Networks between Order and Randomness”; *Princeton University Press*, Princeton, 1999).