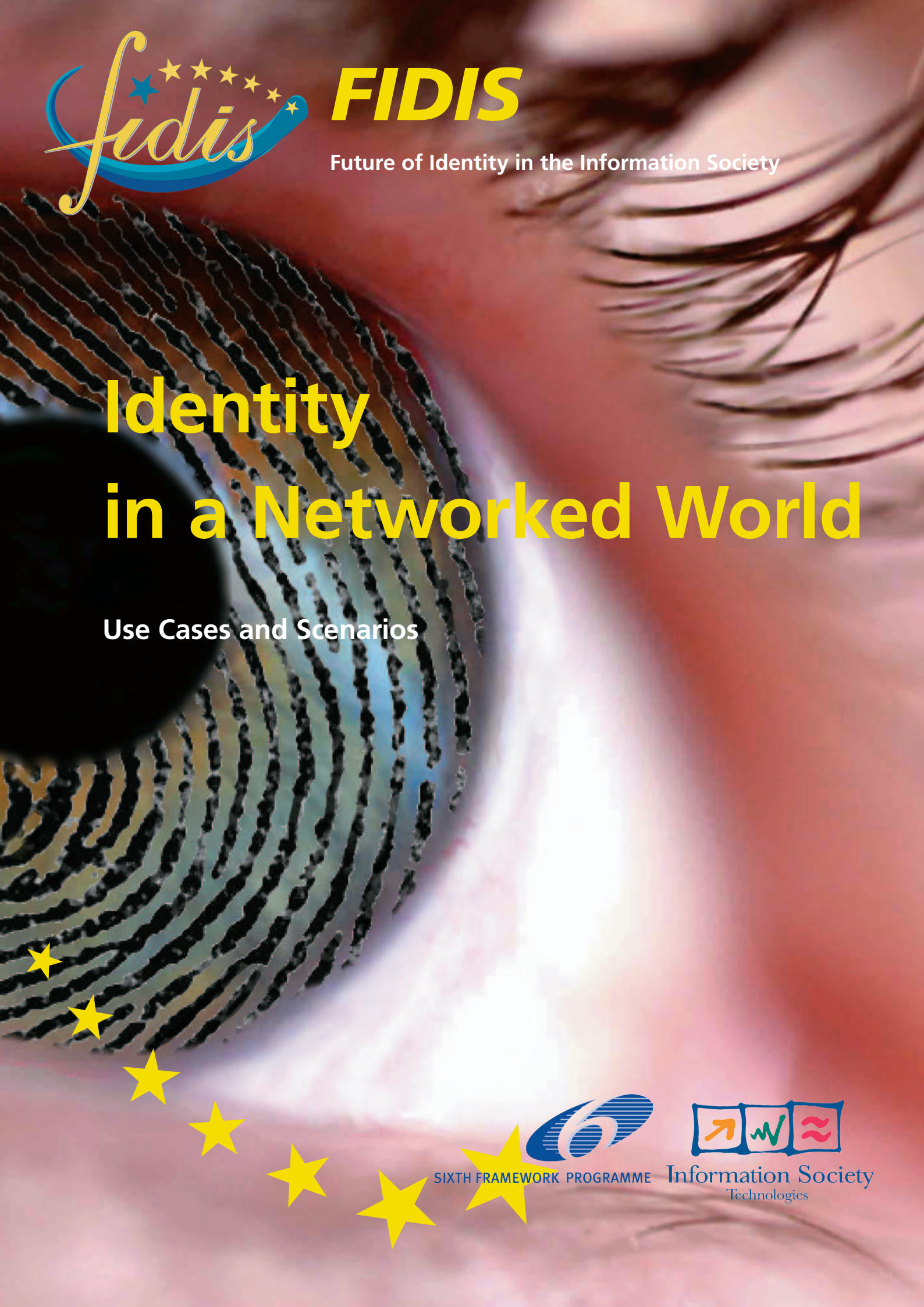

fidis
FIDIS
Future of Identity in the Information Society
Identity
in a Networked World
Use Cases and Scenarios
SIXTH FRAMEWORK PROGRAMME
Information Society
Technologies

EDITORIAL

The digitisation of identity may be regarded as a bottleneck in the engagement of citizens with Information Society services. Identity in such environment plays a central role and more and more tools are required to manage identity and deliver suitable services. Management of identity will constitute one of the first challenges for the future Europe in terms of mobility, accessibility and interoperability in order to facilitate online navigation and social (digital) interactions between European citizens in the Information Society. Personal information will be digitized and the Internet extension to home and mobile networks, the multiplication of modes of connection and types of gateway, will make the individual the central point. The future of identity then is a key element for the emerging Information Society; it represents the main vehicle of the cyber-citizen in this new digital environment.

In addition, we are faced to an ever-evolving variety of technologies that promise to solve problems in the field of identity, identification, authentication and the like. Each product, each technique promises to make life easier for us. Identities can be more secure but at the same time its management brings more privacy issues. The identity management tools will have to respect the user's privacy and security, and they will also have to facilitate the application of laws. In other words, the balance between privacy and security will have to be preserved in the future Information Society. Therefore, there is a clear need to assess the implications in this new digital environment, which tends to blur the traditional boundaries between the private and the public space.

As a multidisciplinary and multinational NoE (Network of Excellence) FIDIS (Future of IDentity in the Information Society), appropriately, comprises different country research experiences with heterogeneous focuses, and integrates European expertise around a common set of activities. Additionally, all

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

relevant stakeholders are addressed to ensure that the requirements are considered from different levels. FIDIS network aims at Integrating European research with regard to Technologies to:

- Support identity and identification
- Interoperability of identity and identification concepts
- ID-theft, privacy and security
- Profiling and forensic implications
- Mobility and Identity

One objective of FIDIS is to contribute to the understanding of the concept of identity in the context of digital social environments, of ICT usage and in the new social dimension of internet, regarded as valuable fields for investigation and research for the future identity. In these evolving environments the concept of identity would have to be re-defined in such a way as, on the one hand, to raise public confidence in the security of the online environment and, on the other, safeguard citizens' privacy rights while ensuring compliance with, and enforcement of, the law.

The deliverable "D2.2 Cases, stories and scenarios" represents the second document created in the context of the work package 2 of the FIDIS Network of Excellence, aiming at better understanding the "Identity and Identification" concepts. From this deliverable, seven topics have been selected to provide an overview of digital social environments from the viewpoint of the subject of identity and to raise citizen's awareness of the diversity and richness of these environments and of the different related identity issues.

Sabine Delaitre

IMPRESSUM

Editors:
David-Olivier Jaquet-Chiffelle, Emmanuel Benoist, Bernhard Anrig
VIP, Berne University of Applied Sciences

Authors:
Bernhard Anrig VIP, James Backhouse LSE, Emmanuel Benoist VIP, Ana Isabel Canhoto LSE, Sabine Delaitre IPTS, Claudia Diaz KUL, Marit Hansen ULD, David-Olivier Jaquet-Chiffelle VIP, Thierry Nabeth INSEAD, Árpád Rab ISTRI

Cover and graphical realization:
Giampaolo Possagno VIP

Address:
VIP - Virtual Identity and Privacy Research Center
Berne University of Applied Sciences,
P.O. Box, CH-2501 Bienne

Contacts:
VIP: fidis@vip.ch http://www.vip.ch
FIDIS: fidiscoord@fidis.net http://www.fidis.net

USER-CONTROLLED IDENTITY MANAGEMENT
THE FUTURE OF PRIVACY

Marit Hansen

Marit Hansen *is a computer scientist and is head of the "Privacy Enhancing Technologies (PET)" Section at the "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein" (the State Privacy Commission), Germany. Since her diploma in 1995 she has been working on security and privacy aspects especially concerning the Internet, anonymity, pseudonymity, identity management, biometrics, multilateral security, and e-privacy from both the technical and the legal perspectives. In several projects she and her team actively participate in technology design in order to support PET and give feedback on legislation.*

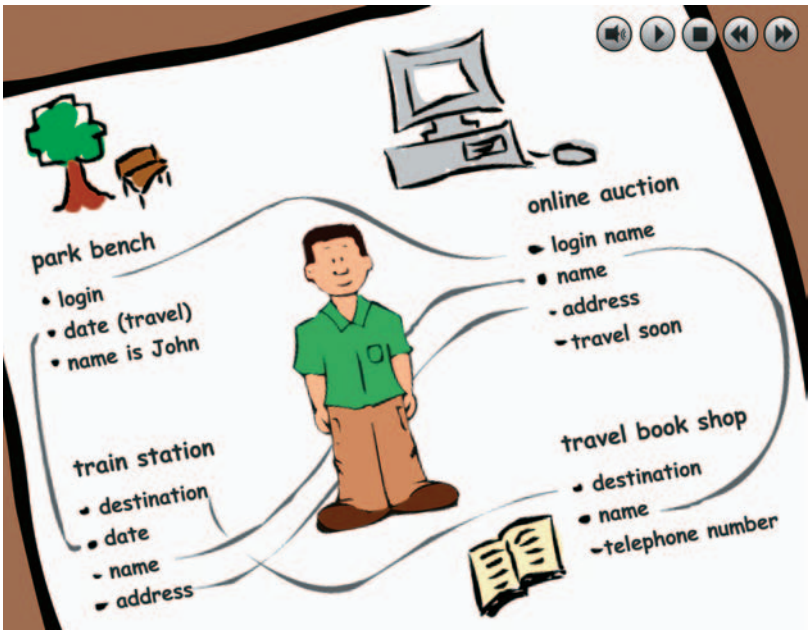
Currently users face the risk of lacking control over their personal data in the online world. User-controlled identity management are promising tools aimed at maintaining the users' right to privacy.

"In the Internet nobody knows you are a dog." – Well, this famous saying from early Internet times does not seem to be true today: Online shops, advertisers, search engine providers and of course the access providers have a lot of data on each Internet user, often keeping them for a long time. Many users are not aware of the *data traces* they leave in each communication and which enable profiling of their behavior. Combined with the information which users disclose for facilitating transactions, e.g., giving their e-mail address, their home address and credit card information, more and more parties in the online world get a picture of the user, including her interests and sometimes even her social network. This increases the risk of identity theft.

Anonymisers are tools which help to minimise data traces – but this alone does not solve the problem: Users need control over all disclosure of their personal data. As in the offline world, a user would decide intuitively what to tell whom according to the specific situation. For example different data are required in professional life than in private life, and in a book store other data are relevant than in the sports club. Nobody gets to know the full identity of a user – instead, only specific partial identities can be perceived.

Data traces comprise e.g., an IP address which identifies the user's computer at the time of use, cookies containing unique IDs, and referrer data which informs about the webpage the user came from. This set of information can be used to profile the user's behaviour, e.g., for sending her personalised ads. Today, even setting prices according to the user's click behaviour are being discussed.

This is the focus of *user-controlled identity management*: The user manages her partial identities according to specific situations and contexts. This means choosing and developing appropriate partial identities with respect to the current application needs. They enable the users to handle the plurality of accounts and passwords. Not always the real name of the user is required. Instead, different pseudonyms could be used to prevent undesired context-spanning linkage and profiling by other parties.

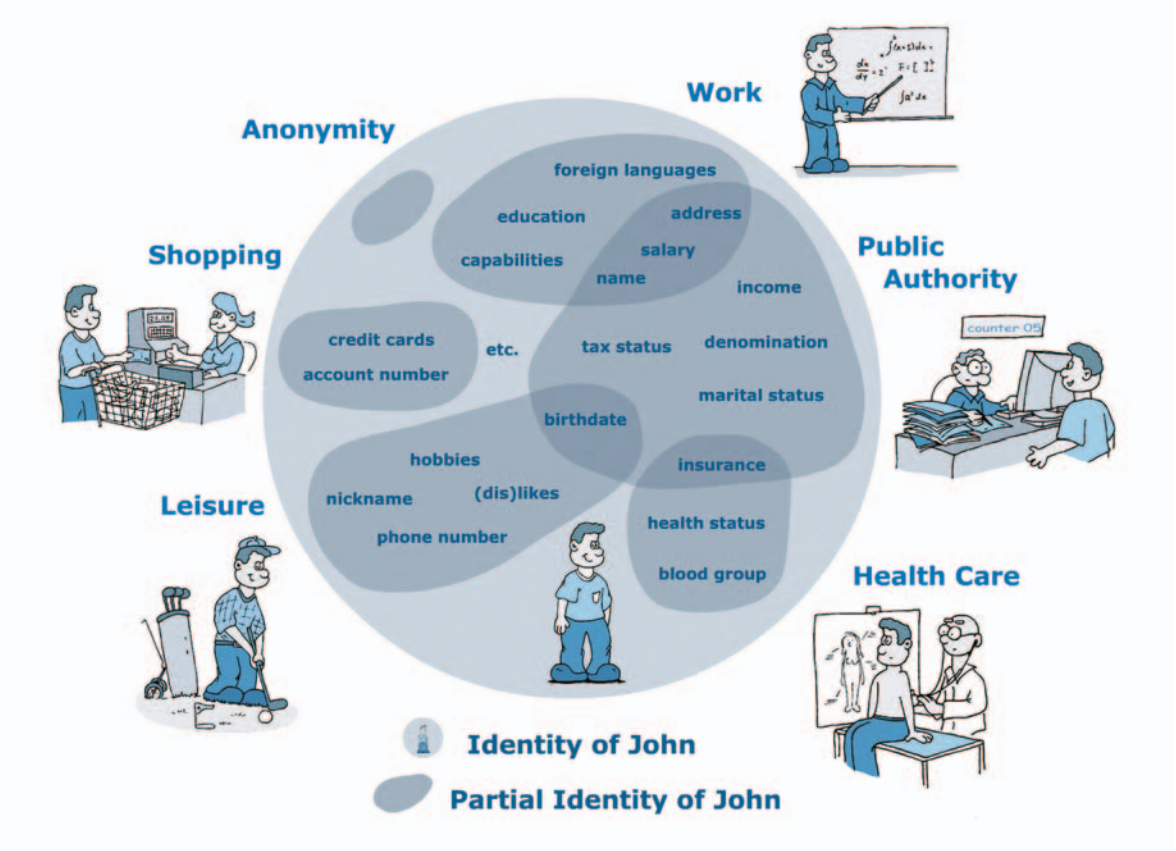


User-controlled identity management

User-controlled identity management systems do not only offer pseudonyms, but also keep track of which personal data have been disclosed to whom. Thus, the user can see which personal information the various communication partners have received in former transactions. To know who knows what about oneself is necessary for one's informational privacy.

At present, only very few people have a look at the privacy policies of online shops eventhough they contain important information, namely how the provider promises to treat the personal users' data, e.g., for which purpose data are stored or when they will be deleted. The identity management system could analyse them and show the user what is essential for her privacy rights. The user could decide on the basis of this information whether to give consent for data processing, which data to disclose or whether to refrain from interacting with the site at all. Even more sophisticated requirements may be negotiated, e.g., how long the data may be stored, which third parties may get access to personal data for specific purposes, or that the data may only be used if the provider pays for that. The privacy policies would be stored together with the information on disclosed data, like keeping a copy of the general terms and conditions.

In several cases the application requirements will not offer many degrees of freedom, so that the users' choices are limited, e.g., in e-government applica-



tions. Then the identity management system is still useful to visualise the requirements and to keep track of the data disclosure to enable maximum transparency to the user.

The current landscape

There are quite a lot identity management systems which support the users' convenience, e.g., for password management and form filling. The FIDIS project is elaborating a database of different types of identity management systems which will be online end of 2006 (cf. http://www.fidis.net/). Beware of those systems which "manage your identity on your behalf" on centralised servers: Those providers can monitor all your activities and may have their own interests regarding your data.

Meanwhile more and more concepts for federated identity management are being implemented, e.g., by the Liberty Alliance, by Microsoft's CardSpace or by the open source project Higgins. All these approaches cover only a part of the functionality described above. In the EC-funded project "PRIME – Privacy and Identity Management for Europe" the full flavours of identity management are being researched and developed. As a specialty their approach uses "private credentials" which enable proving one's authorisation without revealing information that may lead to an identification of the individual – as long as there is no misuse. In addition they are looking into ways for users to really exercise their privacy rights, e.g., to get access to check their personal data stored at other parties in the Internet or to withdraw their consent if they are not satisfied anymore with the site processing their data.

Without user-controlled identity management Scott McNealy's provocation "You have zero privacy anyway. Get over it." from 1999 may become true. But by empowering the user and increasing transparency, which are the key issues of user-controlled identity management, we will be able not only to keep the important right to privacy alive, but to develop it further according to the needs of sovereign individuals in the Information Society.

Credits:

The figures were taken from the tutorial of "PRIME – Privacy and Identity Management for Europe" which explains privacy and identity management aspects in an easily understandable way. The tutorial includes a movie and interactive components which deepen the understanding of important concepts. It is available via http://www.prime-project.eu/

VIRTUAL PERSONS APPLIED TO AUTHORIZATION, INDIVIDUAL AUTHENTICATION AND IDENTIFICATION

Bernhard Anrig, Emmanuel Benoist and David-Olivier Jaquet-Chiffelle

The concept of *virtual persons* that we have developed within the second work package of FIDIS *Identity of Identity* creates an abstract layer allowing a more faithful description of many scenarios appearing in our modern society, in particular in authorisation, individual authentication and identification schemes.

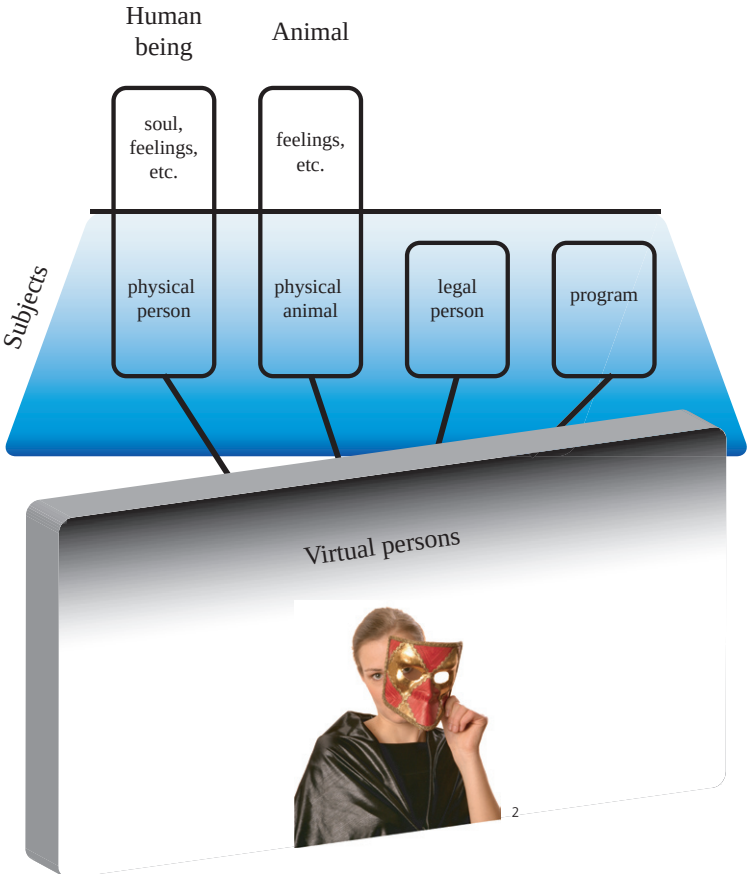
David-Olivier Jaquet-Chiffelle *is full professor of Mathematics and Cryptology at the University of Applied Sciences of Berne in Bienne, Switzerland, since 1997. He is lecturer at ESC (School of Criminal Sciences) at the University of Lausanne, Switzerland, and gives regular postgraduate courses in cryptology. David-Olivier Jaquet-Chiffelle is also Head and Founder of V.I.P, Virtual Identity and Privacy research center since 2001.*

Etymologically speaking, person comes from personae which means mask. A physical person can be seen as the mask of a human being. A legal person is any personality (mask) which is recognised by the law of a country; it has rights and duties. It is often recorded in registers and has a legal status.

In authorisation, individual authentication and identification schemes, physical persons and legal persons are subjects acting or playing roles in these scenarios. More generally, a *subject* will be any physical or legal entity having – in a given context – some analogy with a physical person. Here, subject is not opposed to object. Indeed, physical objects, like a computer, may be a subject too. Our subjects *are*…, they *have*…, they *do*…, they *behave* or they *know* something just like physical persons do.[1] Typical subjects are persons or groups of persons, but can also be animals or computer programs.

Virtual persons

A *virtual person* is a mask of a subject. The same subject may have several masks; the same mask may hide several subjects. However, virtual persons acquire their own existence which becomes independent of the real existence of the corresponding subject(s): the subject(s) behind a mask may be alive or not, may exist or not; in some cases, no subject at all hides behind the mask.



2

In general, virtual persons can be defined by what they like, what they feel, what they think, what they do, etc. In the very specific context of individual authentication or identification, we want virtual persons to fit closely with the four classes of authentication technologies themselves: something you know, something you have, something you are, something you do. Therefore, in this context, *a virtual person* is usually defined by what it *knows*, and/or what it *has*, and/or what it *is*, and/or what it *does*.

It can also be defined by its *attribute(s)*, and/or its *role(s)*, and/or its *ability(-ies)*, and/or its *acquisition(s)* (see figure 2). However, even in the context of identification, these categories are not exhaustive; sometimes, a virtual person can also be defined by its *preference(s)*, and/or its *habit(s)*, for example as a result of data mining techniques.

The *President of the United States* is a virtual person defined through its role. The subject linked to it might change after each Presidential election. After the election, the subject inherits several attributes, rights and duties associated with the virtual person.

The *owner of a credit card* and the *user of this credit card* are two different virtual persons that may be linked or not to the same subject.
The *owner of a given fingerprint* is a virtual person whose corresponding subject may be alive or not. Biometrics try to create a strong, non revocable link between a physical person and the corresponding virtual person: the owner of a given biometric feature.

Emmanuel Benoist *is full professor of Computer Science the University of Applied Sciences of Berne in Bienne, Switzerland, since 1999 and member of V.I.P, Virtual Identity and Privacy research center since 2001.*

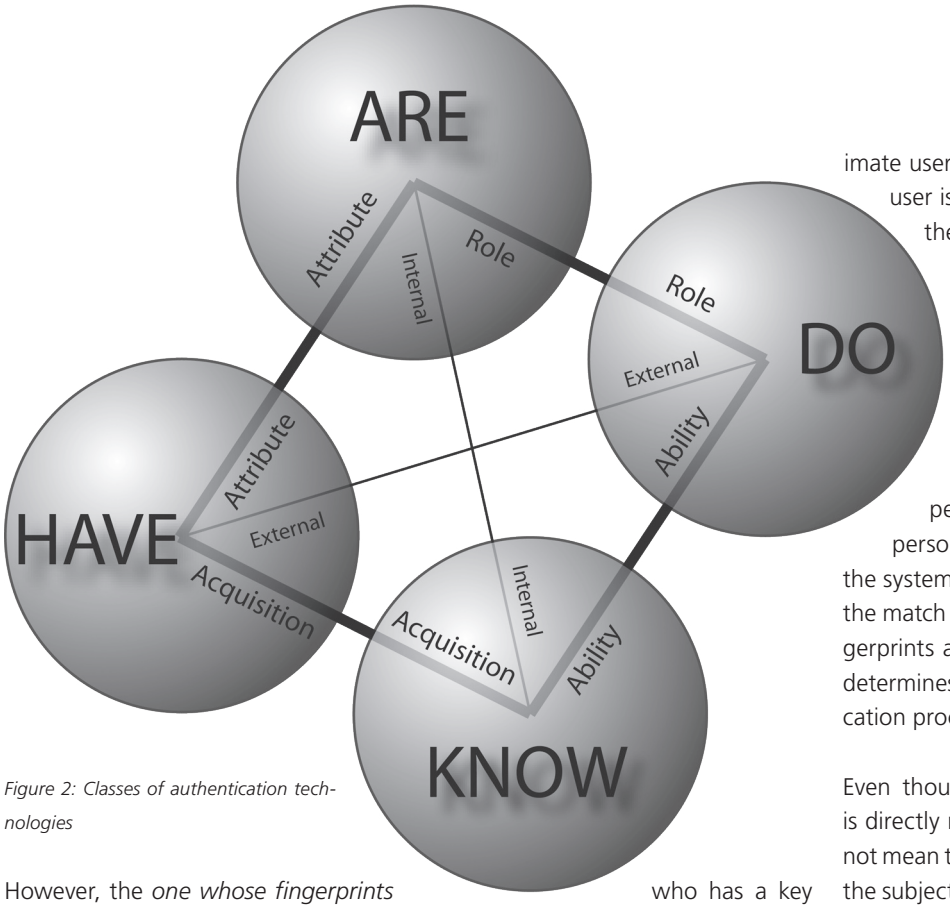


Figure 2: Classes of authentication technologies

However, the *one whose fingerprints give a match with some fingerprint template* is a virtual person to which more than one subject is sometimes linked. Our model emphasises the fact that even when biometrics are hard to forge, the link between a biometric template and a physical person remains an indirect link.

Authorisation, individual authentication and identification

Authorisation is the process of deciding what an individual ought to be allowed to do.[3] We need to consider two virtual persons. The first one is an abstract one with an associated list of what it is allowed to do. It does not have, *a priori*, a specific subject directly related to it. The second one is "the one acting in the scheme in order to get some authorisation". The subject related to this second virtual person is usually time dependant. The authorisation process consists in authenticating the link between both virtual persons. This authentication can be done, for example, by verifying that the second virtual person possesses a key which opens a certain door. The first virtual person would be "the one who has a key to open this door" and an associated right would be to enter the building.

Individual authentication and identification are processes establishing an understood level of confidence that a certain identifier refers to a specific individual.[3] The identifier might be a biometric template, a username, a public-key, etc. We consider again two virtual persons. The first one is "the one who is compatible with the given identifier". The second one is "the one to be authenticated or identified".

Let us take the example of an individual authentication without identification: consider a computer requiring user's authentication through fingerprint recognition at startup.

The first virtual person is defined during the registration phase where the legitimate individual presents its fingerprints (an identifier). A template of the fingerprints is then stored in the computer. The first virtual person becomes "the one whose fingerprints are compatible with those of the legitimate user". Hopefully, the legitimate user is the only subject related to the first virtual person, but this is not always true, especially when weak, easy to forge fingerprint systems are used. The individual authentication process consists of authenticating the link between both virtual persons. The second virtual person submits its fingerprints to the system. The level of confidence of the match between the presented fingerprints and the legitimate template determines the result of the authentication process.

Even though the first virtual person is directly related to a subject, it does not mean that an observer can identify the subject; indeed, the identity of the subject might be unknown. The legitimate user may choose a pseudonym in conjunction with his fingerprints to define an account; he does not need to give his name, his address, etc.

The second virtual person – the one trying to access the computer – is always the same mask; however, the subject linked to it changes when different persons try to access the computer. This illustrates the difference between subjects and virtual persons.

[1] *Our subjects look like the grammatical «subject» in a sentence as it has been pointed out by Sarah Thatcher, London School of Economics, during the FIDIS WP2 workshop in Fontainebleau (December 2004).*

[2] *The picture of the woman in this paper is copyrighted. Christoph Edelhoff has granted us the right to use it.*

[3] *"WHO GOES THERE ? Authentication Through the Lens of Privacy", National Research Council of the National Academies, 2003, Stephan T. Kent and Lynette I. Millett, editors.*

Bernhard Anrig *is full professor of Computer Science at the University of Applied Sciences of Berne in Bienne, Switzerland and member of V.I.P, Virtual Identity and Privacy research center since 2003. Prior to joining V.I.P, he worked as senior researcher at the University of Fribourg, Switzerland on reasoning under uncertainty, especially probabilistic argumentation systems.*

The current domain of research and activities of the three authors covers security and privacy, identities and virtual identities, PETs, pseudonyms and biometric pseudonyms, anonymization, applications of mathematics and cryptology to protect privacy.

VIRTUAL ONLINE SOCIAL ENVIRONMENTS, REAL DIGITAL IDENTITIES ISSUES

Thierry Nabeth

Thierry Nabeth *is a Research Fellow at INSEAD Centre for Advanced Learning Technology, France. Thierry's researches are focussed on the design of the next generation of collaborative virtual environments that will be cognitively informed and that will be providing more pro-active support to the users' activities.*
Practically these next generations virtual environments will conformed to the Web 2.0 principle, and in particular will be open, community-based and will harness collective intelligence. They will rely on the construction of a deep (cognitive) understanding of the users that will be obtained by the observation of their online behaviours. Cognitively artificial agents, informed of the users' profile, will intervene proactively support people activities.

The new Internet of Blogs, Wikis, online social networking and reputation systems, represent new virtual social environments in which rich identities are created. Although these environments are only virtual, they raise real identity issues.

The Internet has very much become a social space. People develop real and long-term friendships or relationships (online dating) in online communities (Friendster) and online games (MMORPG – Massively Multi-users Online Role Playing Games) with people they have never met in the "physical word" and that they will probably never meet. They use online networking systems such as LinkedIn to better manage their relationships, for instance to find a job. Online vendors develop reputations in commercial spaces such as eBay. Knowledge worker create blogs as knowledge exchange channels to interact with other professionals, or to present themselves to potential employers. People participate collaboratively in the construction of online encyclopaedias such as Wikipedia. Children use MSN, or eSpace to interact with other children that they know in the physical world, or that they have only met in these virtual spaces. By doing this, people are dedicating an increasing amount of their leisure and work time, money, and emotional involvement in these spaces, which are becoming an integrated part of their life.

Identity in virtual environments

The reader of these lines may say "Ok, I have understood why these online worlds are important; but can you tell me more about the online identities that people develop in these worlds and what makes them special?" Identity is particularly important in virtual environments. Since virtual environments are usually not supervised (people decide to enter into an interaction on a totally voluntary basis), the quality of the interaction that people develop in these spaces is strongly correlated to the image that people project of themselves. For instance, an effective interaction is very dependant on the level of trust between the participants involved in an interaction.

Identities in virtual environments are complex, and include both the explicit personal identities (real or faked) that are managed via digital identity management systems or declared by people when they fill in a profile. More interestingly, they also include all the implicit social identities (such as reputation, social networks) that people develop via their online behaviours (when they post, discuss, act). This later "social identity", sometimes summarised as "you are who your network is", possesses a particular significance in the digital worlds, since contrary to the off-line world, it is made persistent, and can be explicitly represented (people's relationships are for instance captured in social network services software, behavioural traces are present in log files, etc.). This behavioural information can later 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 can even be mined and be the subject of profiling operations for automated utilizations.

Cases of real Identity issues in virtual environments

To conclude, we would like to list a number of examples that illustrate some Identity issues that have occur in virtual worlds.

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.).

The blurring of public / private identity: 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)[1] reports several cases of problems that have occurred for people who posted on a personal blog. 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. They wrongly assumed that their personal blog only belonged to their private sphere.

Approaches for isolating life spheres: 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 [2].

This example illustrates how an experienced "netizen" organises his "online social network life" to isolates different life spheres (dating, discussion, business, …).

Beware of online reputation: 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?

Warner Melanie (2003) in an article[3] 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 had adopted a new on-line identity.

[1] *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*

[2] *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/*

[3] *Warner Melanie (2003); "eBay's Worst Nightmare"; FORTUNE, Monday, May 12, 2003*

REAL LIFE IN VIRTUAL WORLDS
ANTHROPOLOGICAL ANALYSIS OF MMO GAMES

Árpád Rab

***Árpád Rab**, Hungarian anthropologist, ethnographer and web programmer. His main research field is digital culture in the information society. In Massively Multiplayer Online Role-Playing Game (MMORPG games) a lot of important elements meet: virtual worlds, committed players, online and offline identities etc. In this research he wants to understand the background of the games' success – this kind of "entertainment" is one of the most typical digital cultural phenomenons.*

Switching, undertaking, using and dropping roles and identities is as old as human civilisation. The phenomenon lives on in the age of the information society with the appearance of a new factor, *network identity*. Network identity, although it is to a great extent determined by technological circumstances, is a human set of identities.

MMO (Massively Multiplayer Online) games are becoming more and more popular and fashionable nowadays. In the virtual world of Everquest there was a time when 12,000 players played simultaneously! World of Warcraft had 3 million subscribers within half a year; the MMO games attract an even bigger user base in Asia – a game named Yulgang could boast 9 million subscribers within a month. Although the game style has existed for quite a long time – for almost ten years – it is only these days that an **explosive growth** on the market can be observed. With this growth several sub-types are generated of course, every developer tries to come up with something new, and also professionalism can be observed on a higher level.

MMO games are not only characterized by the fact that they can be played exclusively online, but also that the aim of the game is not to go through a prewritten story line, but **life in a virtual world**. Tens of millions of people play such games all over the world. Among them there are some who only identify themselves with the same character temporarily, but some do so for years. The identity of the MMO players is made special by the responsibility associated with the character, which can derive from loving the character or simply from the fact that the game is paid for. It is also important that these characters not only have online but offline identities during the game, and there is a triple twist to it, namely the identity they take up in the virtual world. **These identities overlap**, and mutually strengthen one another.

Research has proved eloquently that, during the game, characters are not only having fun (although this is their primary purpose) they also get involved in economic activities, building relationships, careers, etc. The analysis of MMORPG communities constitutes a chance to **analyse** identity in **different and unique ways**: voluntary but strong identity; assumed identity; several oscillating identities; responsibility towards the identity; power to build and shape community; intercultural environment, financial risk; levels of anonymity and the role of technology in the preservation of identity, the issue of trust.

The real and the virtual worlds are connected in many ways, and the medium of these connections is of course the player himself. In an MMO game **the participants play with several identities simultaneously**: their real life identity (RL), their role play identity (the character they personalise), as well as a virtual identity, which are connected to playing on a computer, such as anonymity, account etc. These identities mutually affect one another. A connection however does not only exist in the minds, but also on a physical level too.

World of Warcraft™, copyright by Blizzard Entertainment.

World of Warcraft and Blizzard Entertainment are trademarks or registered trademarks of Blizzard Entertainment, Inc. in the U.S. and/or other countries.

PRIVACY RISKS SCENARIO

Claudia Diaz

The development of electronic services and the widespread use of the Internet to conduct all kinds of activities (such as e-government, e-banking, e-commerce or e-voting) open a whole new world of convenience and opportunities. Unfortunately, these very technologies also introduce new risks.

Together with many other new functionalities, in the last years we have seen a remarkable development of storage devices, database technology, profiling algorithms, data gathering and data mining techniques. The implementation of the EU directive on Data Retention will require Internet Service Providers to store traffic data for several years. It is often the case that traffic data gives significant information on the content being accessed. Moreover, unique identifiers, such as national ID numbers, are used to authenticate users across many different domains.

The amount of collected behavioural, transactional and personal data grows relentlessly and invisibly with respect 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.

But who would want to use it and for what purpose? Besides offering convenient and personalised services, companies can use these data for unfair commercial practices (such as price discrimination), unsolicited targeted advertising, and employee control. Governments, besides offering better public services to citizens, can also use the data beyond legality (for example, to develop massive surveillance capabilities).

But the problems do not stop there. The data is often transmitted and stored insecurely; meaning that malicious company insiders, eavesdroppers listening to the communication lines, or crackers, can get access to the data and use it to personalise crime.

Criminals could use the data to select their victims and better plan and commit their crimes. Vulnerable people (such as lone elders or handicapped people) would be easily found. Knowing information about the victims can also help impersonate employees of companies trusted by the victims and gain access to their homes. Political and religious fanatics find it easier to get new recruits if they know who to target.

In summary, personal information is valuable for organisations, whether it is for economic profit, for controlling employees or citizens and their personal lives beyond today's imaginable limits, or for criminal purposes. 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.

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 and linking of the information.

Claudia Diaz *is a postdoctoral researcher at the COSIC group at the Faculty of Engineering of the K.U.Leuven. Her research is focussed on Privacy Enhancing Technologies. In particular anonymity systems, anonymity metrics, e-government, e-health and electronic identity systems.*

ENJOY A BAR IN 2012

Sabine Delaitre

The digitisation of life and mainly of identity may be regarded as a bottleneck in the engagement of citizens with Information Society services and particularly with Ambient Intelligence environments. The concept of identity in such environments presents two main aspects: multifacet and ubiquitous. This article deals with the concept of identity in this specific environment and describes the different facets of identity in the future.

Sabine Delaitre *is a Computer Scientist with a Doctorate in the areas of Artificial Intelligence, Knowledge Management and Risk Management from ENSMP and in collaboration with INRIA at Sophia Antipolis. During the period 2001-2004, she worked on a number of EU-funded projects in areas of computer network security, Knowledge Management for eGovernment, eBusiness and eLearning domains. In July 2004, she joined the ICT unit, IPTS, European Commission's DG JRC. She is currently working on projects related to Cybersecurity Activities and on FIDIS.*

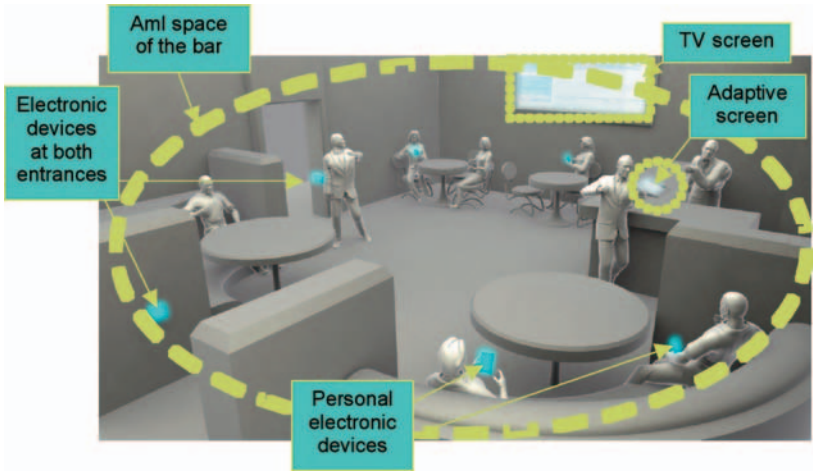
In the ambient intelligence (AmI) space, a future environment combining off-line and on-line life, communications and exchanges of personal data (identity information) proliferate. The purpose of the AmI environment is to deliver seamless applications and services to citizens in order to support their activities. Profiling activity is an essential and continuous background task and consists of extracting the useful information from the current context related to the user, identifying the users' needs, selecting and providing suitable services in order to allow that the AmI environment behaves according to the users' preferences, actions and expectations. Hence, the AmI vision is based on a user-driven approach with a goal to foster the integration of the technology into our environment. Profiling activity thus involves the proliferation of communications, exchanges of personal user data, and identity information, and their storage by means of numerous types of technologies, sensors and devices. Therefore, a growing quantity of identity information will spread over many different systems and increase digitisation of authentication/identification processes. This implies the omnipresence of identity information, but what kind of identity-related information is ubiquitously disseminated in AmI Space?

In AmI environments, we can split identity information into three types. The off-line identity information can be related to appearance such as hair, eye colour, etc.; used as social information, e.g. name, postal address, phone number; and represented by identity tokens (passport, credit card, security social number, bank account number). The digital identity or on-line identity information can be described in the same way. For example, the information related to the appearance can be incorporated into a biometric template. And finally identity information bridging offline and digital Identities that is represented by the 'knowledge-based' identification (e.g. password, PIN) and information gathered from the user context (e.g. a user profile).

In what way does AmI shape the environment of a bar in the future? This scene (see figure) helps describe the hypothetical features of such a bar, a specific public AmI environment.

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 AmI space of the bar is symbolised by the dashed oval: this determines the space in which communications are enabled and all devices can interact.

The story is composed of four moments: the customer (i.e, the user of the AmI environment) enters into the bar (place), enjoys a moment at the bar, is fortunate enough to have a chance encounter and finally, he pays for the drinks.



A scene in a bar in 2012 – background image source (Beslay et. al, 2005)

Story: Enjoy a bar in 2012

Entry into the bar: The customer *declares* his *preferences* (using his *PDA* protected by a *PIN* code) 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 him the soft drink options (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 his local *account*.

Each italic term is related to the identity concept. The table presents some of these terms, which are ontologically described in order to examine the different facets of identity.

Term	Identity facet representation
Preference(s)	Identifier → bridge offline and digital identities → related to the user context → profile representation → individual profile → preferences
Interaction: declares, activates, or notifies him	Interaction → devices communication → access request → ID network (declaration) or ID electronic device (notification) → authorisation → Identifier(s) (communication of information) Remark: The declaration (*declares*) may be active (the user acts, e.g. pushes a button, sends information) or passive (the bar device detects the customer). activates refers to an active declaration.
Friend	Identifier → bridge offline and digital identities → related to the user context → profile representation → individual profile → sociological profile à personal network (→ friend)
PDA, an electronic device	Identifier → digital identity → social information → ID electronic device → ID PDA
Fingerprint mode	1) Identity → data protection 2) Identity → storage → biometrics template Remark: Indeed, the fingerprint mode payment raises two important concepts related to the identity the data protection and the storage of the fingerprint template

Implicit term	Identity facet representation
Fingerprint template (used by the fingerprint mode)	Identifier → digital identity → related to the appearance → biometric template

In this article, the concept of identity in the ambient intelligence environment has been examined. By the omnispresence of the identity related information involved in the AmI space, different facets of identity have been described and the ubiquitous aspect of the identity in the AmI space has been illustrated.

Reference

Beslay, L. & Hakala, H. (2005). Digital territories: bubbles, to be published in the Vision Book, 2005.

TRACING THE IDENTITY OF A MONEY LAUNDERER

Ana Isabel Canhoto and James Backhouse

Ana Isabel Canhoto *is a lecturer in the Interdisciplinary Institute of Management at the London School of Economics, and a researcher in the Information Systems Integrity Group. Her research focuses on behaviour profiling and the development of automated money laundering detection systems. She is an experienced manager and, prior to joining LSE, she worked for a variety of organizations in the telecommunications, and in the media and entertainment industries, in Portugal and the UK.*

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.

Money laundering: definition and methods

Money laundering refers to the processing of the financial proceeds resulting from criminal activity ranging from tax evasion and forgery, to drug- and people-trafficking[1,2].The underlying principle is, in the words of the National Crime Intelligence Service: *"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"*[3].

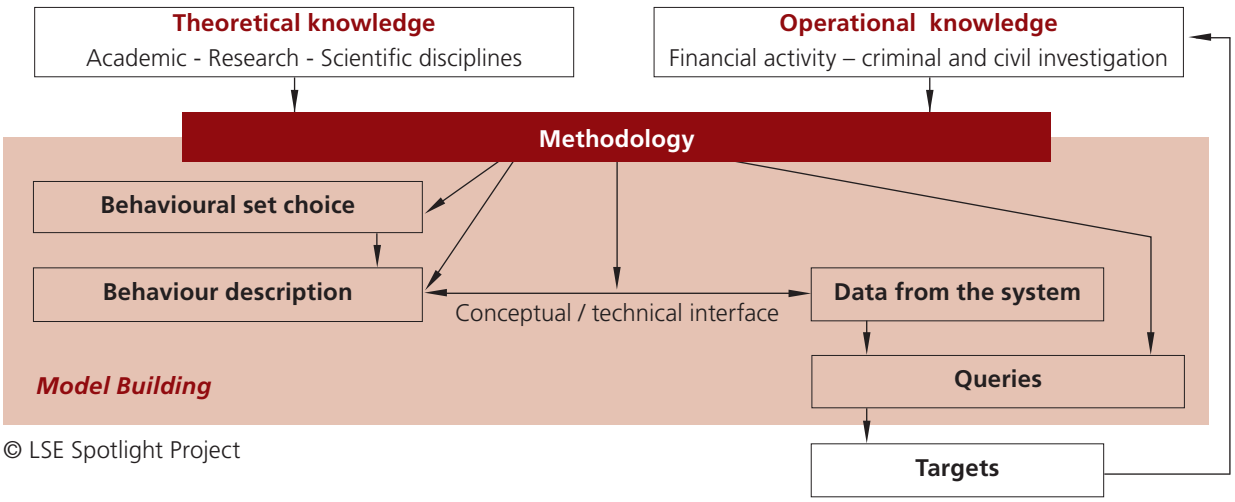
Money launderers will use both the financial and the non-financial system to launder their money. The method involves three stages:

- *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.
- *Layering* – A series of transactions to distance the funds from their source or destiny. 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.

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 modelling usually encompasses the use of automated monitoring tools – powerful algorithms that sweep the records in transaction databases for patterns of financial behaviour that deviate from the norm. 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.

Development of behaviour-based models to target money laundering suspicious activity:



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.
- *Benefit sought*[4] – The benefits desired from pursuing certain behaviour, including the underlying motivation. It focuses on common values and attitudes across cultural groups.
- *Lifestyle adopted* – Focusing on options made regarding travel patterns, or the type of goods and services acquired, for instance.
- *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.

The next section illustrates a case widely covered 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 and the problems it highlighted.

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[5]. 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 £150,000 power boat[6]. 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[7] 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*".

James Backhouse *is Director of London School of Economics IS integrity Group and leads the information systems security programme in the IS Department. At the LSE he pioneered the study of IS security from a social science perspective with his doctoral supervises now in great demand. Recently he led the FIDUCIA collaborative project into modelling risk in public key infrastructure, as part of the ESRC/DTI Management of Information Link Programme. Other current projects involve financial regulation and profiling in anti-money laundering. He is a member of the Senate of the University of London. He was a member of the Committee which extended BS7799 for web-based operations. He has published in numerous academic journals in the fields of security, online education, risk and financial crime.*

---

[1] *Since 2001, this definition has been extended to include the financing of terrorist activity, a practice referred to as "reverse money laundering".*

[2] *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.*

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

[4] *Also referred to as psychographic profiling*

[5] *http://news.bbc.co.uk/1/hi/england/london/3629087.stm*

[6] *http://news.bbc.co.uk/1/hi/england/london/3614597.stm*

[7] *idem*

FIDIS

Future of Identity in the Information Society

Members of the FIDIS consortium

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

Contact: http://www.fidis.net

Printing sponsored by the Computer Science Division, Berne University of Applied Sciences, Switzerland