Identity REvolution

Multi-Disciplinary Perspectives

fidis

Edited by David-Olivier Jaquet-Chiffelle

Designed by Giampaolo Possagno
Art directed by Claudia Nuara

Photography: © Giampaolo Possagno / www.arteplus.ch
Except page 18: © David Woods / Fotolia
page 27: © olly / Fotolia
page 37: © David-Olivier Jaquet-Chiffelle

Li-lian: Fareeda Anklin
David: Frédéric Mast
Zoe: Loïc Anklin
Thanks to Sandrine Viatte and Paul Vincent for their hospitality.

Print: Stämpfli Publikationen AG, CH-3001 Bern

Copyright © May 2009 by the FIDIS consortium - EC Contract 507512
All rights reserved.

www.fidis.net | booklet@fidis.net

ISBN 978-2-8399-0515-2

Identity ***R***Evolution

Multi-Disciplinary Perspectives

The identity [r]evolution is happening. Who are you, who am I in the information society? In recent years, the convergence of several factors – technological, political, economic – has accelerated a fundamental change in our networked world. On a technological level, information becomes easier to gather, to store, to exchange and to process. The belief that more information brings more security has been a strong political driver to promote information gathering since September 11. Profiling intends to transform information into knowledge in order to anticipate one's behaviour, or needs, or preferences. It can lead to categorizations according to some specific risk criteria, for example, or to direct and personalized marketing. As a consequence, new forms of identities appear. They are not necessarily related to our names anymore. They are based on information, on traces that we leave when we act or interact, when we go somewhere or just stay in one place, or even sometimes when we make a choice. They are related to the SIM cards of our mobile phones, to our credit card numbers, to the pseudonyms that we use on the Internet, to our email addresses, to the IP addresses of our computers, to our profiles… Like traditional identities, these new forms of identities can allow us to distinguish an individual within a group of people, or describe this person as belonging to a community or a category.

How far have we moved through this process? The identity [r]evolution is already becoming part of our daily lives. People are eager to share information with their "friends" in social networks like Facebook, in chat rooms, or in Second Life. Customers take advantage of the numerous bonus cards that are made available. Video surveillance is becoming the rule. In several countries, traditional ID documents are being replaced by biometric passports with RFID technologies. This raises several privacy issues and might actually even result in changing the perception of the concept of privacy itself, in particular by the younger generation. In the information society, our (partial) identities become the illusory masks that we choose – or that we are assigned – to interplay and communicate with each other. Rights, obligations, responsibilities, even reputation are increasingly associated with these masks. On the one hand, these masks become the key to access restricted information and to use services. On the other hand, in case of a fraud or negative reputation, the owner of such a mask can be penalized: doors remain closed, access to services is denied. Hence the current preoccupying growth of impersonation, identity-theft and other identity-related crimes.

Where is the path of the identity [r]evolution leading us? The first part of this booklet presents several possible futuristic scenarios, some of them in the near future, within the next 20 years, others in the long-term, e.g., to explore the areas of human enhancement and robotics. They have been originally described in FIDIS deliverable D12.5: *Use cases and scenarios of emerging technologies*, edited by Mark Gasson from the University of Reading, UK. These scenarios have been written by several members of the FIDIS consortium, of different backgrounds and specialities, in order to cover a wide range of possible issues. Even though these scenarios cannot encompass the entire work carried out within FIDIS, they illustrate in a lively manner how emerging technologies might impact our daily lives and our vision of identity in the future. These ten scenarios are short and each of them focuses on one particular subject: the potential impact of ambient intelligence environments for the first two scenarios, biometrics, social networks, virtual identities, grid computing and forensics for the next six scenarios, and the co-existence of human beings, cyborgs and non-human intelligent actors (robots) in a future world for the last two. These scenarios illustrate several perspectives related to emerging technologies and should stimulate the reflection on their potential use, misuse or abuse, on related security, privacy and ethical issues, as well as on their social and legal implications. The narrative form makes some of the theoretical FIDIS results easier to grasp for a non-specialist. We hope that these scenarios will reach a wide community of people and provide a valuable insight into what has been done within the FIDIS European Network of Excellence. The interested reader is encouraged to deepen his knowledge of the work of FIDIS, either through the FIDIS Summit book or by selecting specific FIDIS deliverables.

The second part of this booklet is meant as a teaser to discover the FIDIS Summit book "*The Future of Identity in the Information Society – Opportunities and Challenges*", a complete document published by Springer that offers a synthesis of the main achievements of FIDIS. The editors are the FIDIS coordinators Kai Rannenberg, Denis Royer and André Deuker from Goethe University Frankfurt in Germany. Each chapter summarizes an important topic covered by the FIDIS EU-project and has been edited by members of the FIDIS consortium directly involved in the research related to this topic.

What is the future of identity? Where is the path of the identity [r]evolution leading us? Is it the premise of an ambient intelligent space? Does it foreshadow the advent of a Big Brother (or Soft Sister) society? It is not the aim of this booklet to propose a definitive answer. It is rather an opportunity to provide a wide community of citizens, decision-makers, ethics specialists, etc. with a glimpse into some possible challenging futures, in order to bring out questions and stimulate discussions that hopefully will lead the European citizen to form his own opinion and take informed decisions.

Last but not least, I would like to thank the contributors for the quality of their work, as well as all the persons who have made this printed version possible. A special thanks goes to Giampaolo Possagno for the design and the graphical realization.

I wish you all enjoyable and fruitful reading!

David-Olivier Jaquet-Chiffelle
Editor

VIP – Virtual Identity and Privacy Research Centre, Bern University of Applied Sciences and University of Lausanne, Switzerland

Setting the Scene

While developing the scenarios, it has been deliberately intended that the basic characters should remain consistent, i.e. the same characters are used where possible, although the situations vary depending on the scenario. Some ‘character development’ may, however, be needed, and in these cases extra background information will be given at the beginning of the scenario.

Introducing the main two Characters

David Cragg is a 39-year-old humanities teacher and housemaster at a British public school in Royston Vasey, in the north of England. He first met his now wife Li-lian (née Cheung) while holidaying in mainland Greece. Li-lian’s family is originally from Hong Kong, but she is second generation in the UK. Li-lian works as a security director of a big hotel chain and frequently visits companies producing security devices.

Ambient Intelligence – putting the machines in control

Mark Gasson (University of Reading, UK)

Ambient Intelligence (AmI) is a development of Information Communication Technology which seamlessly integrates intelligent devices into the environment. If the current visions of Ambient Intelligence come true, then we will move to an age where we equip our entire environment with the ability to ‘think’ on its own and to make ‘smart’ decisions for us. The aim of the Ambient Intelligence (AmI) environment is to provide a context-aware system, using unobtrusive computing devices, which will improve the quality of people’s lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf.

The concept of AmI obviously refers to something that is more than just science fiction, but it is still unclear to what extent it indicates an already unfolding reality. Although it is impossible to predict if and in particular how this evolution towards AmI will take place, we can see many emerging technologies, supported by standardisation, social acceptance and legal frameworks, which could facilitate AmI. The decrease in cost of these emerging technologies as well as the emergence of customers that are willing to pay for the services that can be provided seems to increase the likelihood that at least some kind of AmI practices will surface. Besides these supporting and enabling technologies, techniques of user modelling and profiling are already widely-spread, providing customers with enhanced, personalised and customised services (e.g. Amazon’s customised suggested purchases or customisation of financial offers such as insurance quotes). Equally, there seems to be a smooth connection between targeted advertising, location-based services and ambient intelligence.

Having planned their wedding some 12 months earlier, the Craggs are on honeymoon for two weeks in Crete. This, due to circumstance, coincides with the imminent delivery of their first child whose announcement came as a 'happy surprise' some months earlier.

It's all Greek to me

Their late arrival at 'Hotel Warwikakis' in the city periphery the night before had, on the whole, been uneventful. David had previously opted not to allow his intelligent home to send a public version of his family preferences agent to their hotel in advance, and instead accepted that, because of this, they 'may not be able to provide for all specific needs on the first night'. However he hadn't figured on the Greeks being a little slow on the uptake of new technology, and so despite trying to use his MyComm personal communication device to upload the data at the reception desk, he found he was unable to because their system did not use the latest international standard.

Despite this, after converting the profile agent to an older format and answering a few questions related to the types of personal data the hotel was allowed to read from their agent and for how long they wished their preferences to be stored by the hotel, they enjoyed a room lit and heated to their approximate preferred comfort levels, classical music piped through the suite's music system, and the television channels ordered to reflect their tastes.

After a good night's sleep, the day had started abruptly at 06:45 by a wake-up alarm call. Unfortunately neither David nor Li-lian wished to get up at that time, but during the conversion to the older format, the MyComm had been switched out of holiday mode, and as such had assumed today was like any other typical working day. This was rapidly rectified.

Some time later, after getting out of bed, Li-lian decides that she is too exhausted to venture outside that morning, so she opts to stay at the hotel while David does some sightseeing. As part of Li-lian's travel-insurance policy, she is wearing a MediCheck health-monitoring system which monitors her continually for anomalous physiological changes. David ensures that his

MyComm device is listed to receive alerts, and authorises the device to contact the hotel reception in the event of an emergency. As is default with such devices, in line with Greek law, the local emergency service is authorised automatically to be contacted.

Meeting the local location services

David was never one for shopping, but when away always has a look around the local shops. Like many cities, the centre is littered with international clothing stores, most of which use RFID tag scanners in the doorway so as to scan for tags in clothing and accessories to work out what the customer wears and thus to create a rough profile of them. Additionally, most shops welcome the ad hoc automatic upload of shopping agents from personal communicators so as to create a list of offers and discounts to help tempt the customer. By default, David has such options disabled on his MyComm device, and having felt a sense of personal invasion when, for example, the shop is able to alert him to discounts on his type of underpants based on the RFID tag data, he opted to subscribe to an online tag-swap site which periodically sends him credit-card sized plastic tokens stuffed full of random RFID tags designed to confuse the shop's profiling agents. His favourite one apparently registers him as wearing a sombrero and carrying eight kilos of jam.

After a bit on an amble around the local area, David wants to find some food. Having heard of the local dolmathes, he is interested in trying them, but he also has some dietary requirements that he needs to be wary of. David's MyComm device is a 5th-generation mobile device with many useful functions and access to location-based services. One of his favourites is the locator service which enables the device to pin-point his location and seeks out places of interest to him – in this case restaurants. David's device is also equipped with MInD, a mobile device identity manager which allows him to specify a range of partial identities which he can use when accessing such online services. David enables the service and selects restaurant finder. Then he selects his 'personal food finder' profile which stores details of his dietary requirements and then selects 'local food' and 'time sync', which tells the service to look for items relevant for the current time. After a few moments, the MyComm indicates that the service is requesting further details – in this case his location. David authorises the transfer and a list of appropriate places appears on the screen. David is also notified by his device that he can update his iConcert database via the same service provider using the information he has already sent. iConcert is a plug-in for his MyComm that monitors his music library and generates a personalised list of upcoming concerts in his local area. The filtering of relevant events happens on his local device, so that no further information is needed by the service provider. He chooses not to bother, so he remains unaware that his favourite sitar player, Ravi Shankar, is performing with the Cretan lute-player Ciborgakis in the city just that night.

While en route, David's MyComm informs him that he is carrying insufficient cash funds to get him through the day after a typical breakfast at the restaurant. David is aware of the link between uses on his eComm card and subsequent targeted mailings from his card company's 'trusted group of associates' (a downside of the agreement that assures him a marginally decreased interest rate), and his profiling agent knows that he usually opts to use cash for smaller one-off purchases. As such, a detour to a cash-machine is offered and accepted, after David has authorised his MyComm to give his name and nationality to the local ATM finder service. Cash-machines still use PIN security, but this is augmented with additional biometric protection. However, rather than using non-revocable biometrics such as fingerprints, the cash machines use a type of keystroke analysis to obtain a characteristic typing pattern from the PIN button presses. This type of changeable biometric has become widely accepted as preferable. David is annoyed when he has to type in a sample line of numbers four times over and is still rejected by the machine. He now has to use the fall-back option of authorising the ATM to make a picture of him and compare this to the facial-biometric template stored by his UK bank. Even though he knows the picture will be stored for five years by the hefty Greek anti-identity-fraud laws, he has no choice but to accept.

I don't drink coffee, I take tea my dear

Because it's a holiday, David doesn't bother with trying to find out the Greek menu by himself. He uploads his profile to the restaurant system and clicks his agreement with the system's data-processing practices. He is guided to his preferred seat position in the window and is able to select his meal from a heavily customised menu. He enjoys the luxury of just seeing his favourite foods fulfilling his dietary requirements offered to him on the menu, even though he knows the restaurant will sell his data to many food-broking services. The restaurant is augmented with sensor technologies and in the absence of any other information, makes sweeping generalisations in order to project targeted advertising on the menu card when not in use. David is not best pleased to find an advert for a local sports club appear as a result of the doorway height sensor and stool strain sensor concluding he is too heavy for his height. This is soon updated when he removes his rucksack and his weight is recalculated. Unfortunately, being a result of a combined group profile of the current restaurant patrons, changing the music of 'Sakis Rouvas' which is piped through the building is not so easy to correct.

After a delicious assortment of mezes, and the best part of a drink, the waitress, alerted as to the volume of drink remaining by the cup coaster, comes over with a filter coffee pot to offer a complimentary top-up. Unfortunately even the advances in Ambient Intelligence haven't eliminated human error, and David explains just too late how he had actually gone out of his way to find Lapsang Souchong tea…

While preparing to leave, a message comes through the MyComm from David's intellifridge back at home. It requests his acceptance for a menu for that evening's meal based on items that are nearing expiry in storage. Usually, the fridge would negotiate such a message with the house gateway, and thus discovered that the house had gone into holiday mode. However, David had previously configured a link with it in order to interrogate it directly, so messages were unfiltered. He starts to remotely configure the preferences to route it back through the house and avoid further messages when a priority message appears – Li-lian's MediCheck device has found cause for concern.

Congratulations, it’s a…

Despite having had several false alarms in the past, this time Li-lian was in complete agreement with the MediCheck device – something was definitely happening! Having automatically alerted the concierge’s desk and contacted the local emergency services, help was quickly to hand, and within 30 minutes, Li-lian was being wheeled through the doors of a maternity unit. Having been largely planned in advance by her insurance company, her arrival was not totally unexpected. Indeed, her doctor had already authorised access to relevant portions of her e-medical file to the hospital.

However, in her haste in leaving the hotel, Li-lian had only taken her Chinese ID card with her. Unfortunately, this has led to some confusion over her identity because her Chinese name differs from her English name, and to further confound matters, her recent change of surname has already been updated on her e-medical records. Fortunately, Li-lian is still alert enough to give her consent to the hospital cross-referencing her iris scan with that stored in the medical files, and her identity is confirmed. She realises that she had better change her e-medical preferences to allow such identification without her consent, seeing the kind of emergencies that can arise, particularly when travelling.

Meanwhile…

David returns to the hotel too late to see Li-lian, but, having taken the opportunity to collect some of her belongings for her stay in hospital, he heads to the hospital in their rental car. Not being familiar with the local area, he instructs the on-board GPS unit to guide him to the city hospital, and for once, he doesn’t mind at all that his personal data and profiles are being transferred to the local rental-car company in exchange for the routing service. Being slightly flustered and concerned for his wife, David becomes increasingly annoyed with the enforced limits on the car, and so he disables the overrides by putting the car in ‘emergency mode’. Unfortunately, the traffic monitoring cameras observe his erratic driving, trace the car back to the rental company, and automatically issue a fine to David. As a result, David also has an additional sum levied onto the car insurance policy by the rental company. On arrival to the hospital, David makes his way inside, and looks for directions to maternity. Because most of the signage is in Greek, he uses the camera on his MyComm device to translate the words to find his way. He curses when his MyComm only yields error messages and he has to spend precious minutes to use sign language with a passing nurse to indicate where he wants to go. Sometimes, he feels there are distinct advantages to living in the US, where buildings automatically infer and smoothly indicate people’s desired routes. The European AmI Directive, however, has prohibited such automated guidance without explicit individual consent. Who cares about explicit informed consent when your wife is in labour?!

The maternity unit is augmented with additional security measures to prevent unauthorised personnel from entering. To request access, David is asked to scan his iris, and not being on the list of personnel is told to wait for further instruction. Security at the hospital is tight, and the security department is able to cross-check iris scan patterns with the European centralised biometric database. Despite having been acquitted of an alleged offence with a minor at a previous place of work, David’s details are still to be found in the database, and as such he is taken aside for further questioning as to his purpose at the hospital.

After some four hours in labour, Li-lian gives birth to a healthy baby girl. As has become standard, the baby is implanted in the umbilical stump with an RFID tag to allow identification in the hospital. Although such temporary implants have become normal practise, permanent implantation is left for the parents to decide at a later date. David and Li-lian have already decided to have the umbilical tag removed, even though they realise that younger generations seem rather fond of these identifying implants. Zoe – as the girl is named – will just have to decide for herself when she comes of age whether or not she wants to be permanently chipped.

Ambient Intelligence – softwars

Katja de Vries & Niels van Dijk (VUB, Belgium)

Softwars

David is at home recovering from stress while Li-lian is in Egypt for business. The school where David is teaching has recently started implementing the virtual learning environment (VLE): a personalised interactive learning coach which measures the progress of students in relation to targets that have been set. Since its implementation the system has not run well and has caused the teachers serious stress. This, combined with the fear of becoming redundant because of this implementation, it has caused David to have a severe burn-out. David only went to see his G.P. once. After his doctor diagnosed that David was suffering from a burn-out, he told him that the rest of the recovery trajectory could be done conveniently at home with the help of a Medicheck device. David's health insurance company will refund most of his costs on the condition that he permanently wears the Medicheck which can be rented at the local health centre. The Medicheck consists of a tight t-shirt with sensors monitoring heart rate, muscle tension, bodily posture, etc. A virtual doctor is activated when the measured signals reach certain values.

As he has the feeling that nobody really listens to his issues and because he would like to create some order in the chaotic feelings and thoughts he is experiencing he also decides to buy the Psychicheck – a mental wellbeing monitoring system, which according to the ads provides a permanent listening ear and personalised advice. The device registers the frequency in which certain words are uttered in combination with other words. It also measures the pitch of voice, sentence length and facial expression. It is able to take the registered domestic preferences profiled by his intelligent home into account: "It would be good to stick to your normal daily routine and get up at 07:45" is the therapeutic advice based on the profiled user. One of the pleasant aspects about the Psychicheck is that it is designed as a user-friendly little robot dog called "Fifi". The social interface of this device makes it nice to interact with.

One night David cannot fall asleep due to a strong headache. He feels sad partly because of missing Li-lian. Fifi picks up on David's mood and inquires as to what is wrong. After sharing his feelings, Fifi, based on David's leisure profile from his intelligent home, suggests that they watch a movie together. During a bloody climax in the movie in which the main character is about to be violently attacked, David's Medicheck suddenly switches on. It reports exceeded heart rate and advises David to abort his stress causing activity. David wants to see how the movie ends and consults his Psychicheck which advises him to continue watching. David decides to ignore his Medicheck although his arm starts to cramp a little…

A romantic confusion of identity

Li-lian is in Egypt for a business trip. She feels quite uncomfortable about leaving David at home since he is experiencing such a difficult time. Now that they are separated by a huge distance, she is very pleased that they both have implanted in their hands an active electrode which wirelessly connects them. She is at the airport waiting for her flight when she remembers how she and David decided to do this on Valentine's Day. The active electrodes (both connected to wireless internet) were implanted into one of the nerves of their left hand. If one of them moves their fingers (creating a certain pattern of motor neural signal pulses) in a specific way (their "secret" gesture) the other one will perceive this – even if they are separated by a huge distance. The couple experience this as being very romantic : one can "feel" each other even when separated in space. However she has noticed on several occasions that the incoming signals confuse the monitoring system of her Medicheck (her travel insurance requires her to wear one during her stay in Egypt). Every time the muscle contractions were registered by the Medicheck as an unusual signal. She had to manually specify that the signals were coming from a trusted "outside source".

Pre-paid RoadMiles cards & interoperability

Li-lian is driving in a rented car from Cairo to Alexandria where she has a business appointment. Before leaving Cairo the owner of the shop where Li-lian rented the car tried to explain to her something about the "mile-tax" card she had to insert into the ignition slot, but his English was so broken that she had difficulty understanding him. However, she assumed that the mile-tax system was more or less comparable to the system in the UK. Car owners in the UK use "RoadMiles" cards which are linked to their account – and once a month an automatic payment of the due tax is made. When you rent a car in the UK you pay the amount of tax due to the car rental after returning the car. What Li-lian did not know is that in Egypt you buy pre-paid "RoadMiles" cards at the petrol station in order to drive. This system is used due to the lack of facilitating the required technological infrastructure and is also more privacy enhancing (you can buy your pre-paid card anonymously).

Somewhere in the middle of nowhere Li-lian's car suddenly slows down and stops. Li-lian wonders what the reason might be. Has the car noticed that her eyes became more and more tired ? Impossible, the technology of this car is not smart enough to detect such complex facial features ! When a car passes she waves for help. An Egyptian driver stops, smiles and tells her in a mix of Arabic and hardly comprehensible English that she needs to have a new prepaid card. "Where should I get one ?" she asks. The Egyptian car driver shrugs, smiles, and drives away again. There she is, on her own in the middle of the desert. She begins to panic. Hours later she gets to Alexandria – she had to leave her car in the desert and was given a lift in a carpet truck to her destination. Of course she is still stressed by the course of events, but fortunately the business people she had to meet are still in town and the business meeting can still take place.

During the meeting her hand with the wireless electrode begins hurt – this is certainly not David's secret gesture ! Li-lian thinks that it has something to do with the slight stress she has experienced. She takes a deep breath and her hand muscles relax. However, this is really not the time to think about those things – in the middle of her meeting. Li-lian's Medicheck device starts to beep. On the screen it says : "physiological anomaly". Li-lian is irritated by this intervention. She is fine, why is this device bothering her ?! So she selects the "no problem : natural cause for stress" option. When the alert goes off again she ignores the alert - she has to do business now !

Fifteen minutes later however an ambulance arrives at the business centre and its staff barges into the conference room. They slightly hesitate when looking at Li-lian who is identified as the source of the distress signal. They are surprised that she looks perfectly fine. The audience slowly turns silent. The medical team turn to Li-lian, who has now stopped her lecture, and ask if she is doing well and could go to the ambulance to do a medical check. Li-lian follows them, confused by the whole scene…

Intermezzo: A revealing phone call

While Li-lian is sitting in a cab heading for the airport David appears on her MyComm device. He looks very concerned because he has been notified about the Medicheck incident. David tells her that apparently the alarming signal that was received by the hospital in Egypt from Li-lian's Medicheck device was caused by an unlucky coincidence. When David was watching the movie his stress level and muscular tension rose strongly and affected the implanted electrode in his hand. Normally these signals would have been immediately transmitted to Li-lian, but her stay in the desert with no wireless connection made direct transmission impossible. Shortly after her arrival in the connection node of Alexandria all the delayed signals where received simultaneously. This caused a peak signal picked up by the Medicheck which was unable to find a contextual reason for it. David also says that the travel insurance company is not willing to pay for the cost of the ambulance since these are caused by the interference of the implant – and as such not covered by the insurance policy.

Citizenchip

Li-lian arrives at the airport of Cairo and proceeds to the check-in. Since the European Commission has negotiated a border control system at the entrance gates to Europe, a chip detection system has been installed. People are immediately categorised according to the kind of chip implanted into them: European citizenchip, US citizenchip, chips provided to selected immigrants who are still in an immigration or asylum procedure. A few months ago Li-lian read a news bulletin on her MyComm that there were massive demonstrations in the North African countries against the implementation of this system and the creation of a “chipless” caste.

When Li-lian passes the scanning zone, red lights suddenly start to flash. Li-lian is asked to accompany the security staff for further examination. It turns out that the scanning system is unable to categorise her unambiguously due to her double citizenchip (both European/British and Chinese). According to Egyptian law only single citizenchip is allowed and thus the system is incapable of processing double citizenchip. Solving the confusion takes quite a while and Li-lian almost misses her flight…

E-waste

When Li-lian finally arrives home, David is so happy to see her again. They tell each other their stories and find out how many small coincidences have led to the strange sequence of events. Tired and angry about the bad advice of the Psychicheck they decide to throw it out with the garbage. However, did they realise that the robot contained all kinds of sensitive and personal information which is now literally “on the street”?

Use and Abuse of Biometric Data and Social Networks

Harald Zwingelberg & Maren Raguse (ICPP, Germany)

Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. Physiological characteristics such as fingerprints have been used for identification purposes since the 19th century. Also the signature as an example of behavioural characteristics has been used for authentication purposes for centuries. With technological advancement, new characteristics such as a person's keystroke pattern or the possibility of a DNA analysis have evolved. Citizens worldwide are growing accustomed to the collection of two biometric characteristics, i.e. fingerprints and biometric picture, as these are implemented in machine readable travel documents (MRTD) issued according to ICAO standards. Private companies have been developing new services concerning biometrics too. For more than 3,000 diseases, among them breast cancer, Alzheimer's disease, mucoviscidosis, and Huntington's chorea, genetic reasons are known and companies offer genetic tests to detect genetic loading with regards to such diseases. With such information available, genetic profiling would be possible, for example by insurance companies which impose the contractual duty for their customers to report previous diseases, known dispositions and other circumstances allowing conclusions regarding future illnesses. In the future we may see a development where individuals may benefit from lower insurance rates, or on the contrary may not find a company willing to offer them insurance coverage based on their genetic predisposition.

As a new service, companies have also started to offer genealogical research based on DNA tests. The aim is to determine the geographical origin of customers and to find other descendants of joint ancestors. These new emerging social or rather genetic networks revolve around the common interest of shared ancestry. While in these cases the use of DNA as identifying information cannot be changed by the user, social networks usually offer the possibility to create a partial identity : a profile describing the user, her interests and often her social contacts.

Zoe, the daughter of Li-lian and David, is now two and a half years old, and enrolled in kindergarten, and so Li-lian has returned to work.

Getting ready for work

Li-lian and David are getting ready to leave for work and are dropping Zoe at the kindergarten. Li-lian got home late the evening before, returning from one of her regular business trips. She still feels upset by something her good friend Joanne told her over the phone while she was waiting for her departure at Cairo airport. Li-lian closed an inexpensive supplementary health insurance contract a couple of months ago which among other additional treatments offers better protection during her trips abroad. She had told her friend Joanne of the policy because Joanne works as a flight attendant and hence travels a lot. Joanne had told her that the day before she had received an offer 35 percent more expensive than Li-lian's insurance rate. This offer came as a surprise because Joanne is only three months younger than Li-lian, she has one child slightly older than Zoe and no prior severe illnesses.

Joanne's research on the internet revealed that the reason for the offer may have been an exploit of biometric raw-data. The application procedure for the insurance required a standard digital picture to be taken as well as a fingerprint. She was told that the picture would be printed on the insurance card and that the fingerprint would be used as a key for personal data stored on the card. Joanne found out that biometric raw data can be used to identify health risks. A photo reveals data such as sex, age and ethnic origin but apparently can also contain hints to health conditions such as stroke (asymmetry of the face), liver diseases (yellowish skin) or Marfan syndrome (special symmetry of the face). The fingerprint may reveal information on the nutrition status of the mother during pregnancy or the risk of certain types of stomach problems. In Joanne's case it may have been a slightly yellowish taint as she had been on a special diet during the time the picture was taken. She was led to this conclusion by the fact that the company offered the same insurance rate Li-lian was offered, if any liver related illnesses were excluded from the insurance protection.

David, whose cousin works as an insurance agent, is not very surprised at the story. He explains to his wife that after all that is what insurance companies have to do: assess possible future risks of events covered by insurance. If several causes are known to exist for a certain biometric feature the insurance company will, if they cannot rule out benign reasons, proceed based on a negative conclusion. As far as David can recollect, the precision of biometric profiling regarding biometric pictures has increased. A large collection of high resolution photographs made it possible to create a register of health risks. Data was taken from the internet and social networks using advanced face recognition software to compare the pictures and to align them with the database. This database is operated by H.E.L.L – Health Profiling Ltd. The company had repeatedly stressed that only publicly available pictures were used to build the database. Rumours had spread that pictures may have been attained by spoofing biometric passports, health cards, or some membership cards. An investigation by the Information Commissioner's Office however found no evidence supporting these rumours.

After all, David argues, Joanne can always submit a medical statement indicating that she does not suffers from liver disease. Li-lian disagrees. She feels insurance customers should not be obliged to rule out that they suffer from certain diseases. The duty to inform insurance companies of known prior diseases is sufficient for risk assessment, especially if the methods used by insurance companies to gather further information are as error-prone as the method of biometric raw data analysis seems to be.

Li-lian had heard of several US-based insurance companies asking all of their customers for a genetic test. Based on the results many customers faced a rate increase. In the UK and other European countries national ethical committees were currently discussing this kind of genetic profiling.

At Work

Li-lian's first day back at work after her business trip is dominated by administrative tasks. She recalls all of the changes that took place while she was on maternity leave and cannot help but smile at the thought of how surprised she was that day. The RFID-based service cards had replaced the time registration device for employees. The cards were also handed out to hotel guests and used for payment at the hotel's lounge and recreation areas. Li-lian's colleagues had used the cards for access control to the hotel's office rooms too, until the cards were corrupted. The proprietary crypto-algorithm used by the RFID-access card had been broken. Further, using the cards was too unsecure for the high class hotel. To all employees of the hotel strict security and confidentiality requirements apply because the hotel regularly accommodates politicians, diplomats, businessmen and celebrities. Any case of indiscretion would lead to damage to the hotel's image and reputation among its distinguished guests. Li-lian is in charge of the security department at the hotel chain. For this reason her work requires an entry security level approved by the national government.

On that first day after her maternity leave the IT-department issued her a new password. Then she was asked to type a given text into her computer. The access control of the hotel's new computer system goes far beyond inserting her service card and entering a password. Once the machine, a portable computer for presentations at business partners' premises, cannot connect to the hotel network, the computer is set to travel mode. Being enabled, this mode does not only require Li-lian's login but continuously monitors her keystroke pattern. Should anyone get access to the notebook or even force Li-lian to hand it over while she is logged in, the computer will lock out the intruder once the deviation in pattern is recognised by the machine. The evaluation of the keystroke pattern method was praised by the privacy reviewer as less privacy-invasive because the keystroke pattern is a biometric that changes over time and thus features a built in expiry date. However, the advantage of not being traceable after some time turned out to be a disadvantage on her first day back at work. As Li-lian's typing pattern changed massively during her maternity leave she had to spend two full hours typing specimen text.

Li-lian's thoughts turn to her 70-year-old colleague Adriel (people now work up to 72 years in most EU jurisdictions) who was warned by the system about emerging Parkinson's disease. She wonders whether the system does not only warn the affected employee but also informs her employer about identifiable health risks. However, storing the keystroke pattern is still less invasive than other methods of analysing biometric raw-data like the insurance company's procedures she heard of from Joanne.

Having just returned from her last business trip, Li-lian has to arrange her next trip to Toronto. She has come to feel at ease with the idea of presenting her travel documents (she holds a Chinese and a UK passport) to foreign authorities. Since cases of identity theft skyrocketed in the past when organised criminals used the weak standard of the first generation of biometric passports, the EU together with the USA and some other nations reinforced the extended access control standard (EAC) to prevent illegal readout of biometric data. The new standard was improved to offer a considerably higher level of security and allows Li-lian to protect her data from being read by third parties. Public key cryptography allows only accredited scanners to read out the data. All ICAO MRTDs issued these days have extended access control implemented. Her Chinese passport, she is convinced, supports EAC.

The EU, being an international driver for passport security advancements, decided to implement encapsulated biometrics on the European biometric passport. Since encapsulated biometrics are used, external readers do not access the biometric data any more. All data processing is done by the microprocessor in the passport itself. It scans and checks the fingerprint of its owner and confirms his identity when the check is successful. Li-lian read that encapsulated biometrics does mitigate privacy risks as no central biometric database is required and the risk of corruption or disclosure to unauthorised entities is addressed. After all, if biometric data is corrupted, it is corrupted for good. For this reason, Li-lian prefers using her UK passport.

A brief break

Li-lian and her friends grew up using social networks which became a vital part of their everyday life, allowing them to stay in contact, share news and to always feel connected to their loved ones even on extended journeys or while living abroad. But the attitude of many employers towards social networks has changed in recent years. As social networks have become so common most employers allow their employees to let their MyComm device connect to their different social network profiles.

Nafiseh, a friend of Li-lian applied for a job and got rejected. It seems that it was due to some negative information in some social networks. Someone created an account, using her name and address, copied some of her pictures from other web pages and pictures of a student party that took place several years ago. Even though her friend had not been on any of these party pictures, her reputation was damaged. Furthermore, someone tagged her former home address with negative information about her on a neighbourhood rating form. Much of the information was collected at an old social networking site where Li-lian's friend entered much information during her student time - it was the thing to do at that time (2008) to have comprehensive CVs on the web. The service provider of the social networking platform did not use a technology for identity verification, thus allowing anyone to forge accounts.

Li-lian uses a number of portals. However, it is important to her that the service provider uses some kind of authentication. The social networks used by Li-lian offer an anonymous verification. For this purpose the government citizen portal is used. Li-lian also used a social network for health related questions informing herself about pregnancy and labour related issues. In particular she trusted some postings of someone claiming to be a physician who indeed was not. She now uses another network which has technology enabling identity management. Specialists can use credentials to anonymously write posting but are still able to show their expert status. Thus a physician or lawyer etc. can show his qualification to the system without disclosing his identity to other users or the service provider. Li-lian has expert status for facility security issues.

At the kindergarten

Zoe has been at the kindergarten for one month. To pick her up Li-lian usually uses her MyComm device to open the kindergarten gate. Today, however, she forgot it on her desk. The backup system would use her biometric data instead but Li-lian and David refused to provide this data, as the kindergarten was not able to prove that they implemented Privacy Enhancing Technologies to avoid misuse of the data. As Zoe is still new at the kindergarten the replacement nursery teacher did not know Li-lian personally and had to check her passport and the files before he allowed Li-lian to take Zoe with her. Initially the kindergarten did not plan to keep the old-fashioned file system logging the parent's entitlement. However, a parent initiative successfully fought for it, as not everyone was willing to provide a raw-data photo.

Even if Li-lian and David can avoid their biometric data being spread widely, it does not seem likely that they can prevent Zoe's data from being collected. A new programme of the local government envisages taking biometric pictures of every child and using the raw data to identify possible health risks and to automatically check for suspicious signs of child abuse or neglect by their parents. This, so argued a government spokesman to Li-lian's infuriation, should provide pre-indications for the school doctor programme enabling the focus to be set on suspicious children and saving tax money on the service. But rumours spread that the acquired data will also be fed into the governmental databases on children, evaluating the likelihood of future criminal or offending behaviour and the possible need for assistance by social workers. When such databases were first introduced for convicted criminals nobody would have ever thought of registering children at kindergarten-age within such a database. But as pupils have been surveyed in this way for many years and intervention of social workers, and juvenile authorities is more effective the younger the children are, the step to include data collected at pre-schools and kindergartens was just a question of time.

While waiting for the passport to be checked against the files, Li-lian thinks of a case in another kindergarten where a divorced mother not having received the right of custody managed to have somebody access the kindergarten's Wi-Fi and the verification reference database. By injecting her reference data in the profile of her authorised mother-in-law she received the desired entitlement. She then picked up her daughter and left for her country of origin. As everyone thought the girl was with her grandmother no one was suspicious until it was too late.

After finally accrediting Li-lian to pick up her daughter, the nursery teacher uses a display to locate Zoe. All children are tracked throughout the day by cameras using face recognition. Other parents even use the online-service to watch the movements of their children on a floor plan of the kindergarten viewed on their MyComm. Li-lian knows of another mother who uses the cloth-clean function. Using this, the system does not allow her daughter to enter the backyard when it is wet and thus dirty outdoors. She even defined the sandpit as a no-go area. Li-lian disliked this idea. Instead she spends some extra money for children's clothes made from smart materials which are very robust and easy to clean.

When thinking about tracking Zoe, a conversation with her father-in-law comes to her mind. While Li-lian does not want to be tracked when she is old, David's father appreciated the new possibilities. His mother had Alzheimer's disease and got lost during a vacation when she left the hotel at night. It took a long search to find her, dehydrated in the middle of a forest. While her father-in-law feels comfortable with the idea of being tracked, Li-lian thinks that she would only agree to a system that uses an on-demand approach which only sends the location data when she initiates a request for aid.

Having given it much thought, Li-lian gets concerned with all the tracking. She does not want Zoe to get too accustomed to tracking and currently considers another kindergarten for Zoe.

Identity in the future of the digital social landscape

Thierry Nabeth (INSEAD, France)

Social networking services represent a phenomenon that is at the core of the main battle of the Internet actors of today. We find them everywhere, from general purpose systems supporting communities at large (e.g. FaceBook, MySpace), to social networking systems used to network in the "corporate" world (e.g. LinkedIn), and even as the new dating systems that are being adopted by the younger generation (that have always lived with computers) as well as the older generation (people that have adopted the Internet later in life). Every big actor tries to incorporate this dimension as representing the Eldorado of a digital territory in which business models to be successful are still open or in which established positions can be challenged. On the throne of the leaders of the social networking kingdom, MySpace has been replaced by Facebook in a matter of months. Now people are observing some stagnating of Facebook, and are looking for the service and approach that will be the new king, Beboo representing a new raising star, and exclusive services (selecting their members) are promising. Given this accelerated evolution, one can wonder how far this phenomenon will go, for instance in 15 years from now. If we imagine the 'Facebook' and 'LinkedIn' of today to be the dinosaurs of tomorrow, what will be the next "beast" that will emerge from this frantic evolution? The digital space will also not have remained still. We are now already moving from the Web 2.0 (the social web) that was about connecting people, to the Web 3.0 (the semantic web) that is about connecting knowledge, while the Web 4.0 (the Ubiquitous web) that is about "connecting intelligences" is already on the horizon.

Although it is nearly impossible to predict the future of 15 years from now (for instance 15 years ago the web had not even been invented), we can imagine that the social dimension will still continue to be very present, even if increasingly mediated by digital tools: Man is a "social animal" that is not ready to give-up interacting with others, even if this interaction will evolve and will take other forms than the ones that we know of today. We can also expect that society will continue to evolve towards more flexibility, thanks to the technology for removing the geographical barriers. As a consequence, people will most probably live more of their time online than they are today, for working, learning, shopping, or entertaining or "mating". Or rather people will "be even more connected" since the new "communication devices" will blur the frontier between the "physical world" and the "digital world".

This evolution may also not necessary be synonymous with the atomisation of the society since we can very well imagine that new tools and approaches can also help to enforce some of the existing social structures that exist in society such as family, or various communities. In some cases these tools may indeed be used to reinforce social segregation.

The two scenarios presented below will provide a glimpse of the role of identity in two digital social contexts: work (social networking for business) and personal life (online dating systems).

Business social at an alumni cocktail party

Li-lian has been invited to a cocktail party that is being organised by the alumni association of the business school she attended five years ago. In this "reunion" a professor of the business school is going to present on the subject of personal branding, or how to manage your personal information and project a good image of yourself in a business world, having made information checking a preliminary of any business relationship. Well actually, when Li-lian thinks about it, this "probing" happens now for almost any domain : colleagues are using the internet to know more about you (what you are currently working on, and in particular who you are working with) ; the company is using it to form teams (being sure that the members of the team have the right competence, motivation, and are complementary) ; and people are using it to find dates (nice to know for instance the movies to which the other person goes or the group this person belongs to) or to know more about the friends of their children (although in this case it is always difficult to be sure with them, given they use any imaginable trick to fool their parents). Finally, in her particular case, Li-lian is using it on a regular basis in her job as the security director of a big hotel chain to screen suspicious clients or to make enquiries about the staff of the hotel. She is even relatively proud of being able, with the help of a couple of 'bots' she has to admit, to have a high success rate at detecting in advance people that represent a risk for the hotel. Practically, this is just a matter of detecting some particular behavioural patterns and finding a match in the customer database (hotel chains have been pretty good at constructing client databases in order to better serve their clients, but also, something that is rarely put forward, at sorting-out the good clients that are bringing revenues from the ones bringing trouble).

Anyway, this reunion will only be about application of managing the way you are perceived in the business world, knowing that it is increasingly difficult keep track of all the traces that you leave in an "information space" that is mined by a variety of bots that are only too quick at identifying and exposing your weaknesses. To tell the truth, these same bots can also be very useful by

helping to get the attention of business partners or head hunters. Of particularly importance now are people's relationships with others, since these relationships have appeared to represent first class information about the real person, and in particular represents a much more reliable means than the information that people declare about themselves. You have therefore now to be careful who you declare you are working and interacting with (bots are good at discovering hidden relationships), and be sure that they will be positively perceived outside. Hiding information is not really an option, first because it is now increasingly difficult to accomplish. Second because it makes you easily appear as the "usual suspect" if the "bots" are not able to find enough information about you. Consequently, only the more "adventurous" people, or only other "usual suspects" then accept to deal with you if you appear to originate from nowhere and in particular if you can not be connected to people having a good reputation. "Luring services", allowing you to literally "buy" your relationships, look nice (some people are even "trading" their friendliness) and can be helpful, but they can be expensive and they often do not resist to very indepth investigation (data-mining tools are difficult to fool).

Supporting the event

Li-lian knows that this event has all the chances to be valuable for her since chance actually has very little to do with its organisation. Indeed the alumni association organising this event has become very professional, and makes all efforts to guarantee that it will be a success. AlumniNet, the online platform of the alumni is very instrumental to this success :

Firstly, this platform is used to identify the topics that are likely to attract the most interest from members of the community. Bots in the platform are continuously mining people's activities, and sources of external personal information that people have made available to them to identify the "hot topics". The topics include the interests that people have expressly indicated, but also include all the more implicit interests or needs that people may not want to declare or are not aware of, and that can be extracted from an analysis of their digital traces. Indeed, the idea of relying only on explicit information to know about a person has been abandoned for a long time : people do not necessary know what they like or what they need (and often they do not want to know), but more importantly they have more useful ways of using their time than entering them in a profile.

Secondly, this platform is also used to help the forming of a group of alumni that could participate in this reunion. Since this is a physical reunion (people still like to meet in physical spaces), location-based information (that can be retrieved via access to people's personal agendas) is very useful to be sure not to bother people that will not be able to physically attend. Many other elements are also used to make the reunion a success, and in particular finding the good balance of profiles of the participants : it is usually good to have some homogeneity in the group, but not too much since it can lead to dull reunions. Besides, people also attend these meetings to meet faces from other horizons, since it is more likely to generate high added business value : if a person is too much like you, you may not learn a lot from her, or she may be your most direct competitor with whom you may not want to have any relationship. The platform is also very good at raising the attention of people potentially interested in this event. For instance personalisation of the notification can be helpful : some people like to be informed via their mobile MyComm devices, while others prefer to be informed only via their big information hub (which has huge display devices with haptic capabilities). In all these cases, the exploitation of member's personal information is critical.

Thirdly, and as the groups are being formed, AlumniNet also provides a useful way to get information about people that are going to attend, and therefore getting the most out of the reunion. Looking at their profile and looking at who they know can be useful for this. Actually, the access to who they know is only partial, since people are now being careful in the way they are directly exposing their really important relationships (the relationships that are easily available are usually the ones that make them look good, but are of minor importance). On the other hand people are more likely to give access to their "real" relationships indirectly, by allowing only the AlumniNet bots and matching applications to access this data. These bots are for instance "authorised" to mine people's contacts, and to expose them indirectly, for instance by displaying in the person's profile what the types of people this person knows are (bankers, business developers, consultants, venture capitalists, and so on). Matching applications are also very convenient. For instance Li-lian is able to use a matching application to identify participants that are most likely to be valuable to her and that will be worth having a chat with at this reunion. This is something that she can add to her mobile MyComm device, so that later at the reunion she will be reminded when she is physically close to the person. This is a function provided by the BusiNessAccelerator© service to which she has registered on her MyComm device. This same service will also allow her to indicate a social relationship (in the old days it would have meant exchanging business cards), but more importantly to instantly associate additional information such as her first impression of the person via some annotation or some voice or video recording (some people are even known to hide cameras, but shooting videos at the end of a meeting is a practice that is now largely accepted).

Well, now time to go and listen to this professor. Li-lian will wear her new "gadget" : a "smart" scarf that manages to get access to some of her brain waves and displays some information about her mood. Li-lian will have to try controlling her feelings, but this promises to be a lot of fun, in particular since she knows (from AlumniNet) that other participants will wear similar gadgets (for instance men will wear a "smart" tie). No doubt that these will be a good opportunity to add new people, and have her profile look even better. Why not have more private bankers in her network or a management guru ? Certainly to this end the professor appears to rank fairly well in the "people that count" service available on the Wall Street Journal.

Dating

Many years ago, a study by Robert Epstein had shown that everybody was lying in dating services : women appeared to be slimmer, blonder and younger than they are in real life, and the men happened to be richer. By now, this has just become common knowledge, and everybody knows that you cannot really trust these services, even the ones that pretend to be the most exclusive and that filter their members.

Yet this does not prevent these dating services to exist and to prosper. These services have even become a part of life for the young generation as a way to socialise. Actually, playing at creating false images has even appeared as a sport to some of its sub-groups and a societal phenomenon for this generation. These services are also extensively used by older generations wanting to "settle down" and that look for an efficient way to find the perfect mate (people are becoming very difficult now, and are looking at these systems not only to reach more people, but also to have some guarantee that the other persons have the desired "qualities").

In all these cases, the construction of an online identity is critical, and relies on an art of showing yourself that can barely be considered as new. Indeed, when you think about it, this "art of showing yourself" has existed for millennia : for instance, men and women have dressed and used make-ups to try to seduce the other all through history. However, now in the social hubs (a new name for the aggregation of services supporting some social process) this art of disguise has taken on totally new proportions since appearance is not only about how you look in a picture or a video, but how your avatar (a 3D or 2D representation of yourself) looks and behaves, who you pretend to know (the limits of "showing" your level of connectedness that existed in the real world have totally exploded in the online world !), what your personality is (the results of personality tests can be made available) or what your activities are (sports you practice, books you read, etc.). In the later cases, the connection to some services (digital libraries, supermarkets, or even location-based services) makes the declaration of the activities quasi-

automatic and effortless, and provides a good feeling of reliability. In certain cases this feeling is consistent with the reality, whereas in some other cases it is totally the opposite. For instance some groups of people (that like to be referred to as "the Transluscents") have incorporated into their life the principle of full transparency. The "transluscents", who in their youth had the opportunity to experiment with micro-blogging services (for instance using "Twitter" for declaring their more insignificant actions or thoughts), are now using devices that make some of this tracking automatic. For some other groups (that like to be referred to as "the Opaques") "fooling the systems" has become almost a way of life : members of this group are using totally forged activities generators with the aim of demonstrating their activism at defending privacy. These members are taking pleasure in displaying streams of activities that create confusion in the applications exploiting this information. Needless to say that fooling dating services is an activity that is particular praised amongst the "Opaque" group. Contests have even been organised for creating the best false identity that will be the most efficient at getting the most "dates".

Audrey, David's younger sister, a long time user of these social hubs, knows very well the "rule of the game" of dating systems. This is especially because one of her former boyfriends was an activist of the Opaque group movement. This time however Audrey, who is getting older and would like to settle down, plans to use the system more seriously to help her find a long term relationship. "Why not use a dating system to look for the perfect mate ?"... "I know the system well, and therefore, I am confident that I will protect my privacy, and will not be manipulated"… "I also know what to expect, and therefore I will not be disappointed".

Action !

For this "mission", Audrey has chosen a "social hub" (well, the term dating systems is no longer used except to mean something rather negative) that is more specifically dedicated to an older audience. Actually, the affiliation to this hub is subject to the agreement from the other members by a voting system. Audrey had to present herself before being accepted. The rejection rate of this process is however low since the operator of this hub wants to have as many customers as possible, but it helps to create a first level of filtering, and in particular discards people that are really too weird. Audrey was therefore able to pass this first gateway without difficulty, although she was initially a little bit worried that they would discover her past associations with the Opaques. But her fear was not founded, especially since the operator of a hub is strictly forbidden to share the personal information with another operator and besides, there is so much competition between the operators that they never exchange information.

When moving to this new hub Audrey was able to bring part of the "Identity" that she had developed in one of the previous hubs she was member of. However, to tell the truth, Audrey would like to make a radical change, and actually prefers to leave behind most of her previous identity that represents another period of her life. She will of course only import to the new hub the part of herself that is consistent with the new life she wants to construct. But she will also take care to erase all the information that she would not like to see pop-up in the new hub, such as the set of pictures of her graduation in which she is dressed as a clown, drinks champagne, smokes, and makes some provocative poses. However, the process of "migration of identity" is now easy (the operators have made a lot of effort to make switching to their hub as easy as possible, thanks also to the adoption of standards for exporting personal information), and Audrey was able to monitor and control the transfer at a very small level of detail.

Since Audrey had decided to start from almost a "blank sheet" in this hub, she had to construct an almost completely new profile. She also used a pseudonym : Audrey had little desire to embarrass herself with her colleagues or even worse with the members of her family. Selecting the most adequate attributes in her profile, so as to project the most advantageous image of her, turned out not to be an easy task. Indeed, "ShineoMatic", the "impact assessment tools" assessing the attractiveness of her profile kept returning a "lousy" feedback. First ShineoMatic indicated that her current profile was mainly able to attract married persons, or very young people looking for an adventure ! Really, this was not what she was looking for his time ! For her second attempt, ShineoMatic indicated that she only looked attractive to low paid school teachers. Maybe this was because she had put in her profile that she was altruistic. With further revisions of her profile she appeared to appeal to accountants, farmers and bisexuals. After several other adjustments (that many would consider as falsifying the reality), Audrey finally managed to create a profile that was appealing to the right kind of person : the tall and handsome artists or journalist she was looking for.

A more difficult exercise to be conducted by Audrey was raising her level of visibility in the social space by participating in the numerous communications and events taking place in the community. An example would be to participate in the relationships advices forum. However, on a subject like this people tend to reveal more information about themselves than they want, and Audrey would prefer not to disclose some of her very definite opinions about marriage without risking potential relationships. For the time being her involvement in travel and cinema related discussions will do. Audrey has travelled a lot, and she knows a lot about cinema, two interests which her "perfect mate" probably shares. Posting and interacting related to these two topics would also automatically contribute to building her "interest profile", which she had to validate after only a few corrections.

"Well, let's start with this and see how many invitations I receive". The reality check will in any case be done later, when the "real physical encounter" will happen, given that you can still have many surprises. Last small revision, activation of the profile, and joy : already some matches ! "Wait a moment, one of my first matches is George, my former boyfriend the Opaque ! What a big liar he is, he who pretended not so long ago that dating systems were only for the ugly, sociopathic or the dilettante !!!"

Virtually Living in Virtual Reality

Claude Fuhrer & Bernhard Anrig (VIP, Switzerland)

The use of virtual reality is still very limited for people, although the success of entertainment devices, like the Wii, proves that if one can diminish the price of the hardware, there really is a market for such tools. Multicore processors, computers with more than one graphics card, high performance graphics processors are already available for the general public. In Western Europe, Very High Speed DSL (VDSL) networks are available almost everywhere (at least in most urban areas), which allow users to easily reach databases containing standardised descriptions of virtual worlds. All these tools provide an indication that virtual reality could soon enter into our homes and be widely popular. Virtual reality could be quickly and widely adopted as soon as it has found its killer application, that is, the application that would convince enough people to buy into it.

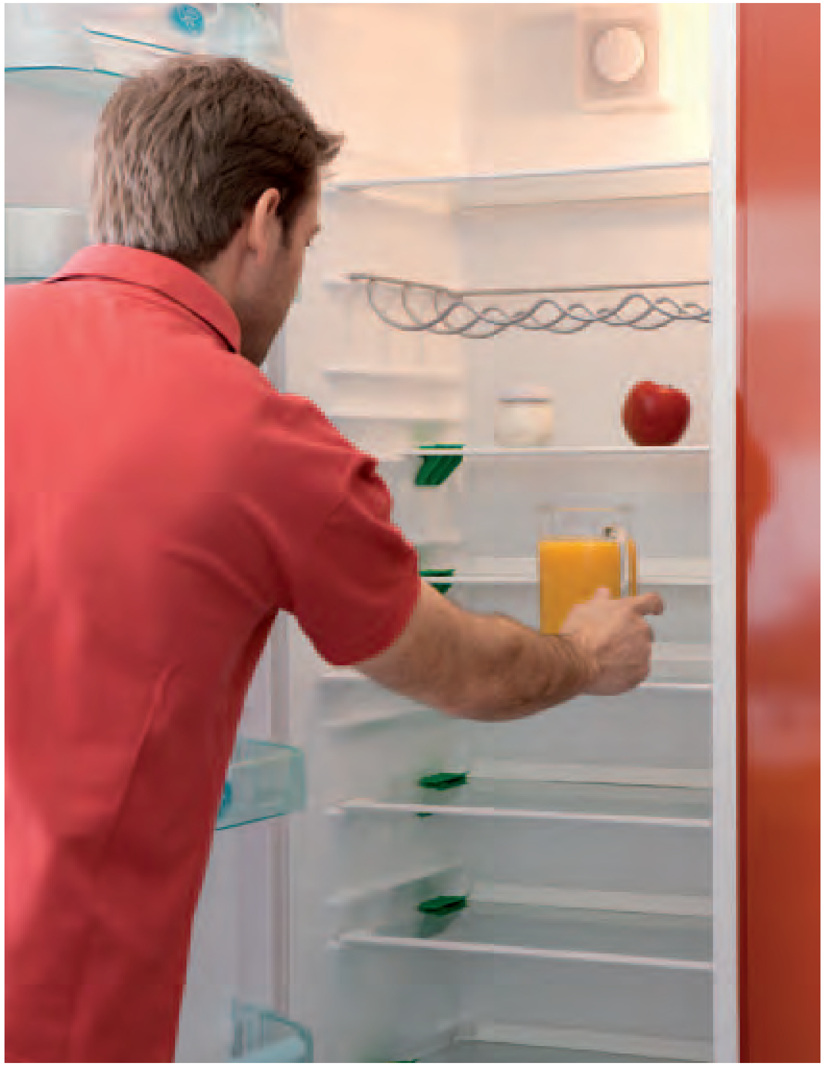
A visit to the supermarket

During breakfast David sees that the fridge is almost empty. Moreover, the list of important things to buy, which is stuck on the door of the fridge is very long. He probably has to go shopping today. He has always considered this activity as being very boring, and even if the high-tech supermarket shop-bots may do a lot of the work, he does not rely on them. They are rarely very good at choosing the big red tomatoes or a sweet smelling and juicy melon.

Even if most of the time people nowadays go themselves to the shop, some supermarkets offer a virtual shop to their customers which one can visit using a virtual reality (VR) system. This virtual reality system is mainly a VR-suit that, at first sight, one may mistake for a diving suit. It is made of special material to fit as snugly as possible to the body and is equipped with a lot of sensors and effectors. The suit consists firstly of the helmet, which has a high resolution retinal projector, allowing the user to have a real three-dimensional view of the environment. Into the helmet, one may additionally build in a high-performance sound system which gives very precise information for locating elements of the environment. The latest generation of helmets even has a scent diffusion system integrated. Based on a similar idea to an imaging system, one can, mixing a limited number of base odours, reproduce a great range of perfumes.

The second part of the suit is the pair of gloves. These gloves are haptic devices allowing the user to "touch" the things he sees. Using these gloves, David can feel the form of the object, its rigidity and temperature, but not texture. The suit itself is also a haptic device. The arms may behave more or less rigidly to simulate the weight of the object which David touches. It may also simulate some external contacts to different parts of the user's body, letting the user know when he touches a (virtual) object in the environment.

Watching the technology channel, David has learned that some laboratories are working on an "extension" of the suit. This extension will consist of a cortical interface which should help the user feel the velocity and acceleration, perhaps not so needed for his supermarket experience, but very handy for playing



games like aeronautical fighting. Another advantage of these cortical interfaces is that they should diminish or even remove the famous “cyber sickness”. But not all people agree with this new aspect. In the newspapers one can regularly read some letters to the editor (even from university professors and recognised scientists) arguing that these interfaces could allow the firm that produces them to take control of the brain of their users, for example by influencing their political opinion or changing their shopping behaviour. During the 20th century there were many warnings of the possible use of subliminal pictures in advertising, but no one was really able to prove it. But this fear seems much more serious now. As such, David chooses not to have such options.

Before wearing his suit, David chooses a supermarket, and feeds the list of things he has to buy into his computer. He is totally aware that everything he buys in this shop could then be used (and probably will be used) to profile him and his family. For example insurance companies use profiling to check if someone is eating too much sugar or too many “rich meals”. The laws do not allow a firm to ask a potential female employee if she is pregnant, but knowing – through profiling – that she has recently bought some pregnancy tests may be a sign that she will need maternity leave in the near future.

To protect against these more or less aggressive profiling methods, David has on his computer a program which warns him if he deviates from an “average Joe” profile. This is surely not a perfect solution, but better than nothing. Moreover, whenever possible he always tries to reach the best anonymity he can. But, for the present case, where the things he wants to buy should be delivered to his home, it is necessary to reveal his real name and address. For activities like shopping, David should be registered, and so his personal data are stored in a database at every shop (or at least every chain of shops). To lower the risk of profiling, every member of the family shares the same virtual identity. This means that the shopping platform is not necessarily able to distinguish David from Li-lian. It can try to infer if the virtual shopper is a man or a woman, based on some standard profiles, but it will never be totally sure of the real identity of the family member who is actually present.

When he has his suit on, he starts the program which opens for him the doors of the virtual supermarket. He can then walk along the aisles between the shelves and pick whatever he needs. But, unlike real shops, he regularly sees some items jumping out of the shelves and “dancing” in front of him or calling him. Why precisely these items ? Because, in virtual reality, one can profile the customer in much more detail than is possible in real life. Here, the system may be aware of everything David has touched or even seen in the past within this supermarket (or even other ones which collaborate). The supermarket has very precise information about the type of package (colour, size or form) David likes, and then may propose (or impose) a customised shop, built to attract the eyes of David and convince him to buy more than he planned. For example, there is stracciatella gelato in the middle of the path, blinking and calling him. The ice cream was not on the list he entered but he loves stracciatella. Since he was a kid this was always his favourite. He picks up the box to add it to his shopping cart. Immediately a red light is blinking at the tip of his finger. This is his anti-profiling program which is warning him that he has already bought too many sweets, and his health insurance company may consider that all this sugar is a sign to check if his family should be switched to a bad risk customer category. He is now informed that if he wants another dessert, he has to go to buy it in the real world and pay in cash. One can note here that in this situation, the virtual world acts as an interface between the real world where David lives and the real world where the goods are. What David sees in his virtual shops are, for example, real fruits. This is necessary to allow him to choose the sweet smelling melons he loves.

When David has collected all he needs, he is ready to pay. Another advantage of virtual shopping is that there is no need to wait in the queue of the checkout. At the end of every aisle, there is a (virtual) button which will automatically establish the bill of the customer. The identification of the user is done by the different biometrical sensors embedded into the VR-suit. The data of David’s credit card are already known by the supermarket and within seconds, the billing process is finished.

The goods he bought will be delivered during the afternoon to his home.

Before he takes his helmet off, the idea of planning the next holiday with his family crosses his mind. Looking at the catalogues of travel agencies is very interesting, but, using an immersive tool to check “directly” the view of a beach in the Caribbean is much more exciting. He just wants to have a quick glance and not have to identify himself. Therefore, he disables the identifying process in his computer. Pointing a finger at the top displays a menu in front of him. He then just has to point his finger to the needed functionality to make him almost anonymous. Then, he can walk along the beach and check which hotel he would like to book for his holidays. While anonymously walking on the beach, the information he gets on the hotels, their advantages or actual room prices are not personalised and, for example, no discounts (based on e.g. recent stays in the same hotel company) are available. When he has selected his favourite hotel, he can still identify himself to look at the discounts etc. available, but for now, he prefers to stay anonymous in order not to get too much unwanted advertising over the coming days.

For this situation, the virtual word in which David walks is probably not the real world around the area where he plans to spend his vacations. For the purpose of advertising, the company has probably chosen a day where the weather is nice and sunny, where the season shows a nice environment, etc. They may however claim that it is virtually the same!

Powering the profile: Plugging into the Grid

Vassiliki Andronikou (ICCS, Greece)

The Matrix may be thought of as the future of virtual reality, but the Grid, a high performance distributed computing infrastructure, has been conceived as the future of collaborative problem-solving. In the same way that the World Wide Web opened up content, the Grid will not only open up storage and processing power, but resources (e.g. computational, informational) in general. Allowing for the communication of heterogeneous geographically dispersed resources, the Grid brings a new era in collaboration and decision-making.

The Grid can offer transparent and instant access to data of different formats, obtained by sensors or the result of simulations or processing, either publicly available or with restricted access, combined from multiple sites, either permanent or (non) periodically updated, serving various purposes. Moreover, through the computational power offered by the Grid Infrastructure, computationally complex tasks can now be fulfilled within a satisfying timeframe. The Grid is a potential solution to the great need for computational resources in the application of profiling techniques in real world cases, and primarily in large scale ones requiring secure information exchange among different trusted entities in real-time.

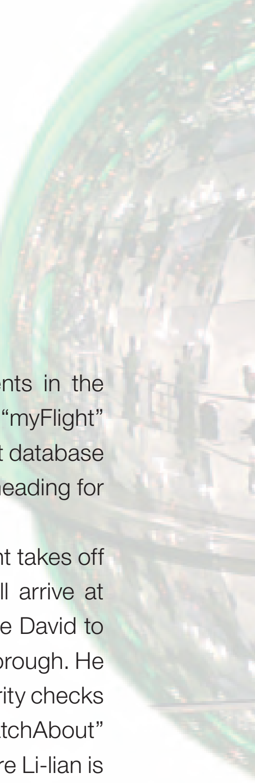
This scenario describes the experience of a traveller who is aided through emerging technologies, which are served by a Grid Infrastructure, showing both the strengths of such an Infrastructure as well as the threats deriving from its powerful collaborative capabilities. The technologies mentioned include biometrics, used mainly for identification purposes, the Grid as a secure and flexible infrastructure, and profiling and location-based services for commercial purposes through the provision of personalised ads and guidance.

Travelling to Rhodes

After an extremely busy period at work, David is now ready for his summer vacation. As his wife had one more week off than him, they have arranged to meet in Rhodes, so he will be travelling on his own. After packing his bags he activates his tourist profile on his personal MyComm device and enriches it with special preferences for this trip (things he might be interested in buying, his holiday companions, etc). Then, he sets off to Heathrow airport's terminal 5. The moment he arrives, the "myFlight" service running on his MyComm contacts the airport database for departure information. After the credentials for this interaction are checked, it sends him an SMS indicating the check-in counter he should go to as well as the gate his flight will be departing from. At the counter a camera captures his face image (both frontal and side view) and performs facial recognition. After being positively identified, he checks-in and he goes for a coffee at one of the many airport cafés. Meanwhile, without his knowledge the facial image captured is also compared against a set of facial images of wanted people of high importance stored in a database in Italy. As David's third match of the combined gridified facial recognition algorithms was "Mario Martucci" – one of the most wanted people in Italy – with a match probability above the predefined threshold the "GentleWatchAbout" service gets triggered and accesses David's photo and id-related data (cell phone number, passport number). For security reasons the "GentleWatchAbout" service has the credentials to use a variety of services. The "myFlight" service periodically contacts the airport database for further departure information and after a while David receives a notification on his mobile phone indicating that there will be a one-hour delay of his flight and so he decides to activate the "myPlaces" application. This contacts the "AirportPlaces" service to get information about points of interest within the airport and after processing the provided list and comparing it with David's preferences stored in the "Travellers' Profile" database in Greece, it suggests for him to go to the "A little Shirty" store which has good offers on shirts, which are his favourite clothes to buy. David decides to do so. He spends most of his time there and 10 minutes before his gate opens he receives a scheduled notification SMS from the "myFlight" service which indicates that he should proceed to his gate. As David gets really bored during flights, he is happy to find out that the plane offers a service that, after you choose a song from the list it provides, it composes a playlist matching the original song selected.

As David arrives in Athens, he has to change flight to get to Rhodes, but his flight is in 5 hours time. The "myPlaces" service contacts the "AthensPlaces" service and the "AthensTransportation" service and it processes the retrieved records based on his time left. The service sends him an SMS informing him that based on the time available he can go downtown for a walk, providing him with photos of places he could visit. David chooses to go downtown and asks the "myPlaces" service for more information. His request is also automatically sent to the "GentleWatchAbout" service. The service contacts the "AthensPlaces" service to retrieve more information for downtown places, taking into account David's love for art and presents him with a list of options, such as the Parthenon, the National Museum, the National Gallery, as well as famous local cafés and restaurants. David chooses to visit the Parthenon. The service then contacts the "AthensTransportations" to obtain information about the means of transportation that could get him there. The latter makes near instant calculations within the Grid based on his current location as well as the available means of transportation and current traffic. The service informs him that he could take metro Line 3 from the airport, get off at Monastiraki station and then enjoy a nice walk indicated on a map provided. This has clearly taken into account that David enjoys walking and the weather in Athens is sunny. Alternatively, he can avoid walking too much and just take the metro Line 3 to Syntagma and then change to metro Line 2 to Acropolis station or he can hire a taxi that will take about 35 minutes to get there. The service also gives him information about the entrance fee for the Parthenon. David chooses to take the second option that, according to the service, will take him about 40 minutes to get there.

As soon as David arrives at Acropolis station, "myPlaces" requests information about the surrounding monuments from the "AthensPlaces" service which in turn contacts the "AthensMonuments" service and instantly sends him historical information about the Acropolis and the surrounding monuments. Meanwhile, the



"myPlaces" service – whenever David moves to another place – requests processing of the retrieved list of places based on his currently activated profile. In the meantime, "myPlaces" sends David's current position and preferences to the "GentleWatchAbout" service. Policemen in the area get a notification from "GentleWatchAbout" that a potential suspect for international thefts with low surveillance priority is at the specific location and are supplied with his photo. David enjoys his visit, but after a couple of hours he gets a scheduled notification on his mobile phone by the "myFlight" service that his flight will depart in 2 hours. David activates the "myPlaces" service so that he can choose the means of transportation back to the airport. As he is really tired, he chooses to take a taxi and so the "myPlaces" service contacts the "AthensTransportation" service which in turn contacts the "AthensTaxis" service and calls one for him. After a few seconds he receives an SMS that the taxi will be there in 20 minutes and suggests he goes to a café nearby. As David has activated his tourist profile, the service asks David if he has a preference about the route the taxi will take and after the service activates the previous workflow it prompts him with two choices : through the historic centre which will take him about one hour and should cost him about 40 euros and the highway which will take him 30 minutes and should cost him about 25 euros. David chooses the first one and then decides to wander around a little bit to enjoy the view before the taxi arrives. Before David started his trip to Greece he had enriched his tourist profile by adding among others "pasteli" as one of his favourite foods. Thus, the "myPlaces" service sends a profile-based processing request to the "AthensPlaces" service and David receives a notification that a shop with many local delights is right on the corner where he can find pasteli. David is really excited about this and decides to pay a visit to the shop. When David gets to the check-out counter, he gives 20 euros for his 10 euro purchase and forgets to take his change. As he gets out of the store the owner starts running after him. A policeman just across the street that had received the "GentleWatchOut" notification notices the incident and heads towards them but realises it is a false alarm as soon as the two men shake hands. After 20 minutes, the taxi arrives and David enjoys the route he selected for the taxi to follow, while on the screen of his mobile phone information about the monuments in the historical centre are displayed. When David arrives at the airport the "myFlight" service, after communication with the GPS service, contacts the airport database and he receives a "myFlight" notification about the gate he should be heading for within the next 15 minutes.

The flight takes off and he is on his way to Rhodes. As soon as the flight takes off his wife receives an SMS from the "myFlight" service that David will arrive at Rhodes airport in 45 minutes. Li-lian sets off to the airport to welcome David to Rhodes. However, the security check at the airport for David is quite thorough. He experiences a one hour delay to get his baggage due to extensive security checks at the airport which had received a notification from the "GentleWatchAbout" service. After one hour and a half David manages to reach the car where Li-lian is waiting for him. The days go by happily and the couple enjoy the sun and the sea. As they are sitting at the beach, David receives an SMS from the "myFriends" service that Fotis – a good friend of theirs – is also in town. David asks for more information and after the "myFriends" service contacts the GPS service about the specific user and after numerous calculations are carried out within the Grid, he finds out that Fotis in fact is at a bar near their beach so they decide to join him. Fotis is very happy to meet the couple and they all enjoy their drinks together. Night falls, and they find a nice bar to start their evening. As they are about to enter the bar, David receives an SMS by "myFriends" service that Sofia – his ex-girlfriend the name of which he had left in his list of friends - is there as well. As he would not like the two girls to meet, David tells them that he just received a notification about a nice bar at the end of the street that he had seen the previous night and so they go there instead. As the "myPlaces" service gets information from the GPS service that they are not going to the same bar with Sofia, it automatically sends an information update to the "myFriends" service about David lowering the priority for Sofia in his friends list. The notification is sent to the service and after processing within the Grid, the update is performed. Time passes by and after two relaxing weeks come to an end, the couple prepares to go back home, again ably assisted by the personalised location-based services.

The role of forensics in identity

Mark Gasson (University of Reading, UK),
Zeno Geradts (NFI, The Netherlands)

The aim of forensic research is to support investigatory and judicial processes by finding traces in otherwise apparently unpromising raw material from which it is possible to build a picture of events and activities. Locard's Principle is at the foundation of what forensic scientists do : "Every contact leaves a trace". Clearly forensics and identity are inherently linked because the aim is typically to identify a person or persons, or to link a person with an activity at a scene. As forensic techniques improve, the knowledge of how to defeat them also keeps in step. As such, the investigator has to keep in mind that what the evidence points to may not in fact be correct, and as such a broader picture is necessary.

Here, set in a world not too dissimilar to today, the scenario will explore how biometric identification can be spoofed such that someone is implicated in a crime, and how future advances in forensic techniques could subsequently prove innocence.

A rude awakening

The digital readout on the clock flashes to 03:05 – the night is very still, and the Craggs are sound asleep. While the people may be resting, the house is very much awake. Such uninterrupted time is ideal for dedicated number crunching – a time when all the data collated during the day can be sorted, cleaned and processed to yield new information to update and augment current profiles being used in the system. That is, however, until the system flags a new primary task – the security system's proximity sensors have detected an anomalous movement in the vicinity of the front door. Because of their countryside location, and the local wildlife inhabitants, such an event is not unusual. Indeed the system is able to monitor through a variety of sensors to establish whether an event is of true importance. As the threat level flicks from amber to red, it appears in this case it very much is. In line with David's preferences, the lights in the bedroom are switched on dimly, and a computer generated voice tries to wake him from his slumber with a warning. He comes round in time to hear an almighty crash at the front door, a thunder of feet pounding through the house, and the sound of men shouting down the hallways.

Ello, ello, ello…

By late morning, things have started to become somewhat clearer. The hasty arrest of David's wife Li-lian for 'data theft', and the immediate confiscation of their laptop computers and primary house server during the police raid had shed precious little light on the situation. In fact little was revealed during the associated chaos until Li-lian's interview with the detective in charge of the case some hours later. It transpired that someone had gained high level access to the computer system in the hotel where Li-lian worked, and had stolen the personal details, including banking and credit card numbers, from their customer database. A partial print and DNA left at the scene had been cross referenced with the UK's national ID card and national DNA databases, and had placed Li-lian in the top ten of likely matches. Knowing that Li-lian did not have security clearance for the main server room where the security breach occurred – finding her partial fingerprint and DNA there appeared to be quite damning evidence. The only problem was that not only did Li-lian emphatically deny any knowledge of the crime, she also appeared to have an alibi for the time it occurred …

Good old fashioned high-tech forensic police work

It was certainly true that Li-lian did not fit the profile of a cyber-criminal, and this had cast doubt from the beginning of the investigation. However, identity theft was big business, and the police had taken a rapidly growing interest in it over the last few years. As such, it was now procedure to confiscate personal computer equipment for searching before anything could be removed or deleted. Of concern was the fact that no evidence could be found on the computers, and that the profiling agent on Li-lian's home server indicated that she was in fact at home with her family at the time of the attack - something which her husband readily confirmed. This left something of a conundrum – someone had managed to defeat the iris scanner on the door to the server room to gain access, had stolen personal data, and had then left the fingerprint of someone else. As all leads began to look cold, there came a stroke of luck. The details of the crime had, as usual, been entered into the local police station's database. While databases across the country were not explicitly linked per se, the UK police force now uses a system called LinKSeE, an artificially intelligent data-mining program which distributes software agents across the isolated police databases which hunt for patterns and correlations, and generate new, potentially useful knowledge. In this case, the system had noted a case six months previously in a different police jurisdiction which had a very similar modus operandi. Indeed, not only was the target again a hotel, and the method of attack identical, but the system had cross-referenced the employee lists from both hotels and had come up with a match.

A rude awakening, take 2

At 07:00 in the morning, the police swooped on the home of their new suspect. Having been employed as a cleaner at both hotels at the time of the attacks, it seemed clear that this man was key to the data theft crimes. Indeed the lifestyle revealed by analysis of his bank records and the out of place Mercedes on his driveway also indicated someone not surviving on a cleaner's wage. In a makeshift workshop in the house the police found what they were looking for : materials for lifting fingerprints and constructing gelatine copies to make fake prints at the scene, and samples of Li-lian's hair containing her DNA. On a computer, high resolution holiday photos of the head of security at the hotel downloaded from the internet were also found, from which printed copies of his iris could be made to spoof the hotel security systems. Certainly enough evidence to vindicate Li-lian of the crime.

Human enhancement, robots, and the fight for human rights

Bert-Jaap Koops (TILT, The Netherlands)

Human enhancement is on the rise. 'Enhancement' involves a multitude of ways and technologies by which human beings enhance their looks, abilities, features, or functions. It ranges from plastic surgery to chip-enhanced cognition in cyborgs. The distinguishing feature of enhancement is that it aims to improve human functioning above 'normal' or 'average'. There is a grey area in which health care meets enhancement – 'getting well' seamlessly moves into 'getting better'. This grey area moves over time, depending for example on cultural views.

Besides enhancement, another interesting development is robotics and artificial intelligence. Machines are becoming more autonomous, and software is becoming 'smarter'. Also, robots begin to look more and more like humans, by using materials that mirror human looks, or by adding features that can make a robot look human in terms of facial expressions like smiling or raising eyebrows. If the 'humanoid' robot is equipped with artificial intelligence – and thus acquires more autonomy through emergent behaviour – the vision of an android might become a reality.

While the prevalence of new 'emerging technologies' resulting from the convergence of fields such as nanotechnology, biotechnology, ICT, cognitive science, robotics, and artificial intelligence will undoubtedly increase, it is impossible to predict how far and how fast these developments will go. One can imagine that in the long term, the world may well become populated by altogether different types of species than those we see around us today: non-enhanced and enhanced humans, cyborgs, robots, and androids among them, all of which will function, in different but perhaps also in similar ways, in day-to-day social life.

Scenarios' introduction

The vision of a future world populated by humans, cyborgs, robots, and androids raises many fundamental questions. One is what this development means for fundamental or constitutional rights, also known as 'human' rights. Will cyborgs be considered human enough to still be bearers of 'human' rights? Can androids claim 'human' rights if they look and function in the same way in society as cyborgs? Another important issue is the relationship between non-enhanced and enhanced people: will there be a social divide? And can human beings keep robots under control as they become increasingly autonomous; in other words, will robots comply with Asimov's three laws of robotics until the end of days, or will they, like HAL in 2001 – A Space Odyssey, revolt and try and control humans? These types of issues are illustrated by the following two scenarios which show different possible worlds in a relatively far-away future – probably around the time of David and Li-lian's great-grandchildren.

London, 28 June 2079, from our correspondent

Scenario 1

Under the circumstances, the mass demonstration of humanoids in Trafalgar Square yesterday took place quite peacefully. About 800,000 robots and androids had responded to a call from the Enhancement Society to demonstrate for the recognition of basic rights for their species. "Robots are the same as people / and want the same as humans", a sign read. "We finally want recognition of our rights. We also have the right to life" said AnDy02593, a third-generation android. "My in-built on/off button is very humiliating, I feel restricted in my freedom to develop myself".

The exuberant mood and atmosphere of alliance were subdued by a larger opposing demonstration of people headed by the Call for Human Dignity. The spokesman of the CHD, Frank Kufuyama, expressed many members' feelings during his speech: "Humanoids are different to people. They are very useful to humanity and the world, but that does not mean that they can just have all kinds of rights. Imagine that androids had the passive right to vote and could take over running the country. Before you know it they would join United Europe with the Asian Union and slowly phase us out. It is absolutely vital that the humanoids remain subordinate to us for the good of humanity."

Although the CHD has a strong basis, it is expected that the increasing social cry for rights from the humanoids will be heard by the government. Minister of Justice Warrik (grandclone of the pioneering former professor of cybernetics) is purportedly preparing a legal proposal to incorporate the rights of humanoids into the Constitution.

London, 28 June 2079, from our correspondent

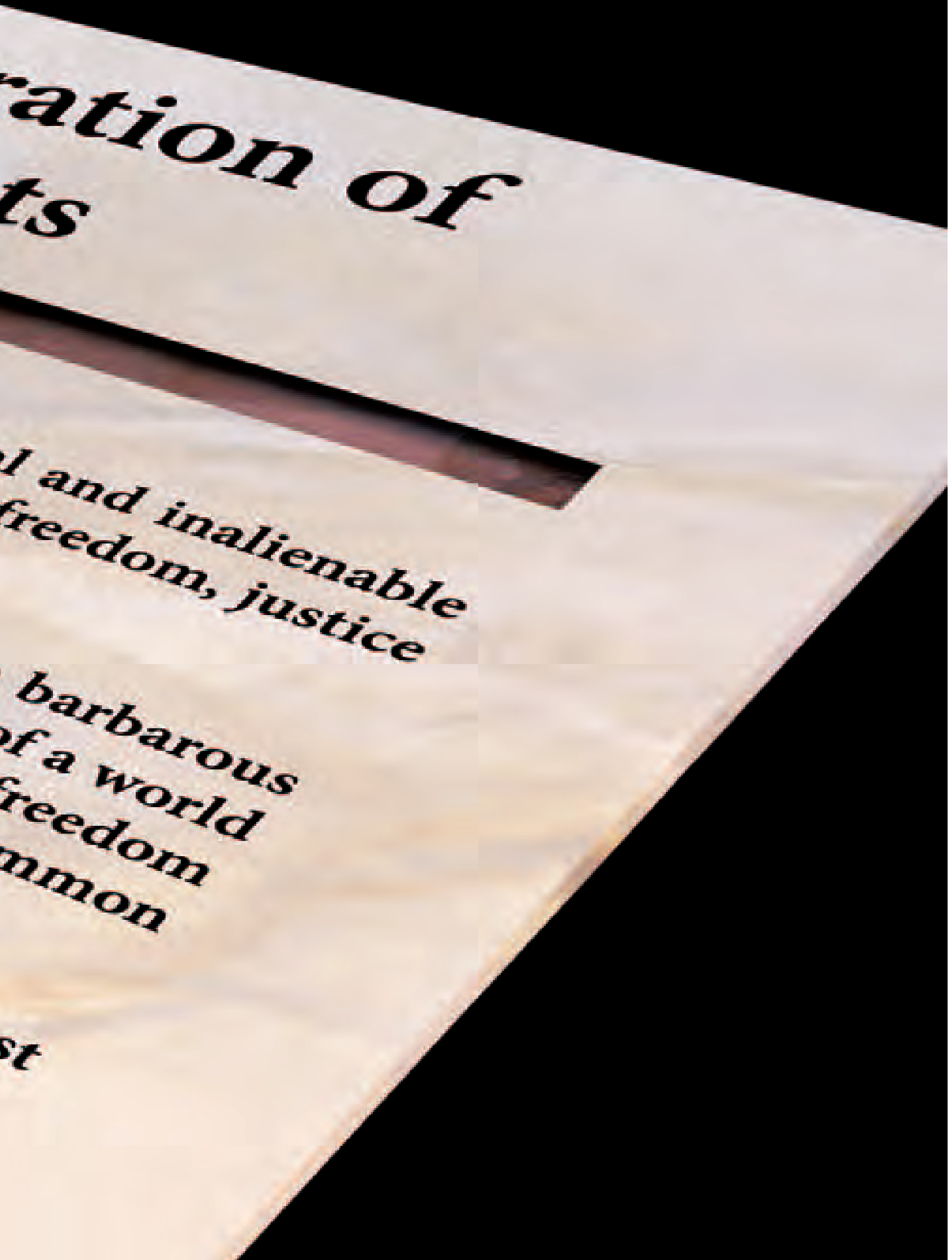
Scenario 2

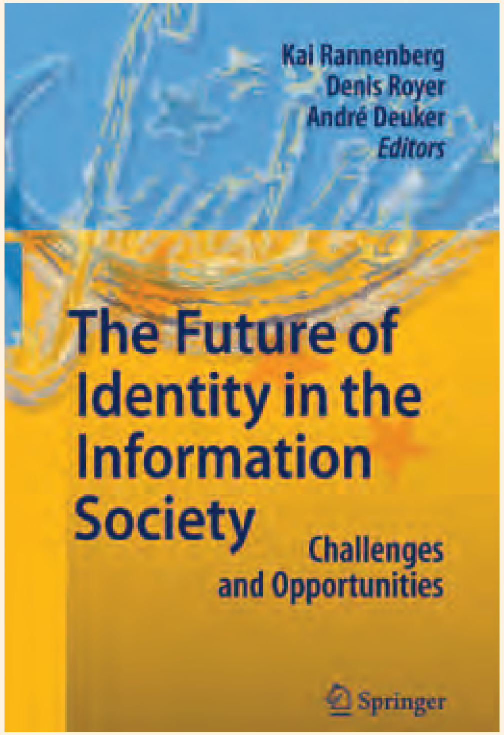
The demonstration of orthodox humans at Trafalgar Square yesterday went calmly under the circumstances. Around 20,000 people, who for diverse reasons refuse to follow the normal procedures of enhancement, complied with the Human League's call to demonstrate against their subordinate social position. "Discrimination against normal people must end," says Andy, a 36-year old paleoman from Manchester. "We have the right to a job but nobody will give us work. The majority of us are healthy but we have to pay three times the amount of the contributions that genetically enhanced people pay. There are hardly any updated teaching materials for our children to learn from because nowadays everything goes to enhanced-brain education."

Despite the atmosphere of solidarity, the mood was subdued. The turnout was disappointing because many Human League supporters could not afford to travel to London and the demonstrators were practically ignored by the neo-people rushing by. The police fined a couple of teenage cyborgs for public abuse when they lingered during the demonstration and who, imitating a paleo-sense of humour, shouted "Hey, Neanderthaler!" to the demonstrators.

There was however, a ray of hope for the paleopeople in the speech of Minister of Justice Warrik (grandclone of the pioneering former professor of cybernetics). He emphasised that the socio-ethic position of minority groups must be respected and that paleopeople still also have a useful role to fulfil in society. He did not want to adopt the HL's ten-point plan because he considered positive discrimination in government functions to be going too far, and the right to paleo-medical facilities and the stimulation of non-brain-interactive cultural programmes to be too expensive. However, he did agree to look into promoting jobs for paleopeople and to pleading for government financing of teaching materials for paleochildren.

Universal Declar
Human Righ
Whereas recognition of the inherent dignity and of the equa
rights of all members of the human family is the foundation of
and peace in the world,
Whereas disregard and contempt for human rights have resulted in
acts which have outraged the conscience of mankind, and the advent o
in which human beings shall enjoy freedom of speech and belief and f
from fear and want has been proclaimed as the highest aspiration of the co
people,
Whereas it is essential, if man is not to be compelled to have recourse, as a las
resort, to rebellion against tyranny and oppression, that human rights should be
protected by the rule of law,
Whereas it is essential to promote the development of friendly relations between
an Rights
Whereas the peoples of the United Nations have in
faith in fundamental human rights, in the dignity a
son and in the equal rights of men and women and
social progress and better standards of life in larger
Whereas Member States have pledged themselves
with the United Nations, the promotion of universa
of human rights and fundamental freedoms,
Whereas a common understanding of these rights ar
importance for the full realization of this pledge,
Therefore THE GENERAL ASSEMBLY pro
ARATION OF HUMAN RIGHTS as a comm
ples and all nations, to the end that every i
pendent, trust,
fe, liberty an


ration of
ts
l and inalienable
freedom, justice
barbarous
of a world
freedom
mmon
st



This part of the booklet is meant as a teaser to discover the FIDIS Summit book "*The Future of Identity in the Information Society – Opportunities and Challenges*", a complete document published by Springer, Heidelberg et al. that offers a synthesis of the main achievements of FIDIS. The FIDIS Summit book[1] is edited by Kai Rannenberg[2], Denis Royer and André Deuker from Goethe University Frankfurt in Germany. Each chapter summarizes an important topic covered by the FIDIS EU-project and has been edited by members of the FIDIS consortium directly involved in the research related to this topic.

The FIDIS consortium brings together 24 partners from 13 different countries. More than 150 researchers are involved in this FP6 EU Network of Excellence. In the last five years, FIDIS has produced nearly 90 deliverables covering a wide range of topics related to identity and its future in the information society. The consortium has always recognized the importance of communicating its main results to a wide community of people : European citizens, scientific communities, private companies, policy and decision-makers, etc. Dissemination activities have been designed to achieve this ambitious goal. Several different tools and media have been used in order to maximize the potential impact of the work done within FIDIS. The Summit book, as well as the present publication, is in keeping with the general dissemination strategy.

First of all, most of the deliverables can be downloaded from the FIDIS official website[3] that currently receives about 7,000 hits per day. These deliverables are grouped into seven main categories : identity of identity, interoperability of identities & identity management systems, profiling, forensic implications of identity systems, high tech ID, privacy & the legal-social context of identity and mobility & identity.

Moreover, results have appeared in numerous scientific publications, peer-reviewed conferences, newspapers, etc. Two conference proceedings have been initiated by FIDIS activities[4]. The booklet *Identity in a Networked World, Use Cases and Scenarios*[5] has been internally produced in 2006 to sensitize non-specialists to some important issues tackled by the FIDIS consortium. To optimize the potential impact of FIDIS worldwide, important definitions and topics have been introduced in the online encyclopaedia Wikipedia[6] and some members of the consortium are actively representing FIDIS in an official liaison with the ISO/IEC Working Group responsible for *Identity Management and Privacy Technologies* (JTC 1/SC 27/WG 5). A new journal, IDIS, published by Springer Netherlands has been launched.[7] The *Budapest Declaration*[8] on machine-readable travel documents has had wide media coverage and will certainly continue to influence the implementation of biometric passports in the forthcoming years. An innovative interdisciplinary approach of profiling has led to the publication of *Profiling the European Citizen, Cross-Disciplinary Perspectives*[9] published by Springer in 2008.

The FIDIS Summit book is an important milestone of the FIDIS project. It offers a synthesis of the accomplishments of the last five years that is more than the sum of its individual chapters. It provides the reader with a snapshot of the ongoing state-of-the-art research on identities, identity management systems, identification and related topics. However, the Summit book should not be seen as a conclusion. It will hopefully open the path to future research in the important and rapidly evolving field of new forms of identities in the information society.

David-Olivier Jaquet-Chiffelle

VIP – Virtual Identity and Privacy Research Centre, Bern University of Applied Sciences and University of Lausanne, Switzerland

[1] *526 pages, ISBN 978-3-540-88480-4*

[2] *Kai Rannenberg, Denis Royer and André Deuker are coordinators of the FIDIS Network of Excellence. Kai Rannenberg is head-coordinator.*

[3] *http://www.fidis.net*

[4] *E-Voting and Identity, Ammar Alkassar and Melanie Volkamer (Eds), VOTE-ID 2007, Springer 2007, ISBN 978-3-540-77492-1.*
The Future of Identity in the Information Society, Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci (Eds), IFIP/FIDIS International Summer School, Springer 2008, ISBN 978-0-387-79025-1.

[5] *Editors : David-Olivier Jaquet-Chiffelle, Emmanuel Benoist, Bernhard Anrig, VIP, Switzerland*

[6] *http://www.wikipedia.org*

[7] *Identity in the Information Society, http://www.springer.com/computer/programming/journal/12394*
Editors in Chief : James Backhouse, London School of Economics, UK ; Bert-Jaap Koops, Tilburg University NL ; Vashek Matyas, Masaryk University, CZ

[8] *http://www.fidis.net/press-events/press-releases/budapest-declaration/*

[9] *Editors : Mireille Hildebrandt, Erasmus University Rotterdam, NL, and Serge Gutwirth, Vrije University Brussels, BE. Hardcover, 373 pages, ISBN 978-1-4020-6913-0*

“The Future of Identity in the Information Society (FIDIS) - Challenges and Opportunities”

Kai Rannenberg, Denis Royer, and André Deuker (Editors)

Foreword

By Viviane Reding (European Commission)

1 Introduction

By Kai Rannenberg, Denis Royer, André Deuker (all JWG)

2 Identity of Identity

By Thierry Nabeth (INSEAD)

The objective of this chapter is not to bring the answer to the ultimate question ‘what is identity?’, - an almost impossible undertaking given the complexity and the constant evolution of the subject - but rather to present, more like on a journey, different angles that can be used to define this concept, in particular in the context of the Information Society. Starting first at describing how this conceptualisation can be conducted in the traditional way of theorisation well known by the academics, this chapter then indicates how less formal approaches such as narratives can be used to help to understand the concept. It also introduces how the new ‘social tools’ originating from the Web 2.0 can be used to stir the intelligence of experts from different horizons so as to generated a meaningful and practical understanding of the subject. The second part of the chapter is used to illustrate how each of these approaches have been operationalised by presenting a series of models and scenarios presenting different perspectives and issues that are relevant to the subject, and a collaborative Web 2.0 knowledge infrastructure that was used in FIDIS to facilitate the conceptualisation of identity by a group of experts.

3 Virtual Persons and Identities

By David-Olivier Jaquet-Chiffelle, Emmanuel Benoist, Rolf Haenni, Florent Wenger (all VIP), and Harald Zwingelberg (ICPP)

What is a virtual person? What is it used for? What is its added value?

Virtual persons sometimes describe avatars and new forms of identities in online games. They also appear in other contexts; some authors use them in the legal domain. Within FIDIS, the concept of virtual person has been extended in order to better describe and understand new forms of identities in the Information Society in relation to rights, duties, obligations and responsibilities.

Virtual persons, as other virtual entities, exist in the virtual world, the collection of all (abstract) entities, which are or have been the product of the mind or imagination. The virtual world –not to be confused with the digital world– allows a unified description of many identity-related concepts that are usually defined separately without taking into consideration their similarities: avatars, pseudonyms, categories, profiles, legal persons, etc.

The legal system has a long experience of using abstract entities to define rules, categories, etc., in order to associate legal rights, obligations, and responsibilities to persons that can be considered instances of these abstract entities in specific situations. The model developed within FIDIS intentionally uses a similar construction.

In this chapter, after having explained the model, we apply it to pseudonyms. Then we explore the concept of virtual persons from a legal perspective. Eventually, we introduce trust in the light of virtual persons.

.

4 High-Tech ID and Emerging Technologies

By Martin Meints (ICPP) and Mark Gasson (Reading)

Technological development has undeniably pervaded every aspect of our lives, and the ways in which we now use our identity related information has not escaped the impact of this change. We are increasingly called upon to adopt new technology, usually more through obligation than choice, to function in everyday society, and with this new era of supposed convenience has come new risks and challenges. In this chapter we examine the roots of identity management and the systems, which we use to support this activity, ways in which we can strive to keep our digital information secure such as Public Key encryption and digital signatures and the evolving yet somewhat controversial role of biometrics in identification and authentication.

With an eye on the ever changing landscape of identity related technologies, we further explore emerging technologies which seem likely to impact on us in the near to mid-term future. These include RFID which has more recently come to the fore of the public consciousness, Ambient Intelligence environments which offer convenience at the potential cost of privacy and human implants which surprisingly have already been developed in a medical context and look set to be the next major step in our ever burgeoning relationship with technology.

5 Mobility and Identity

By Denis Royer and André Deuker, and Kai Rannenberg (all JWG)

While identity management systems for the Internet are debated intensively, identity management in mobile applications has grown silently over the last 17 years. Technologies, such as the still-growing Global System for Mobile Communication (GSM) with its Subscriber Identity Module (SIM) identification infrastructure, are foundations for many new mobile identity management related applications and services. This includes location-based services (LBS), offering customised and convenient services to users (e.g., friend finder applications) and new revenue opportunities for service providers (e.g., location-based advertising).

However, even though the opportunities seem to be endless and technology manageable, challenges arise when looking at advanced aspects of mobility and identity such as privacy, regulation, the socio-cultural aspects, and the economic impacts. To this regard, the interdisciplinary nature of mobility and identity is imminent and needs to be explored further. By learning from the diverse field of challenges, new mobile communication systems can be created, allowing for more privacy-preserving service provision and a more transparent handling of mobile identities.

This chapter presents three scenarios for mobile identities in life, work, and emergency situations: Mobile Communities, Traffic Monitoring, and Emergency Response via LBS. Based on these scenarios is an analysis of the specific properties of Mobile Identities, leading to a description of the FIDIS perspective on mobility and identity. Then a deeper analysis of the technological aspects of mobile networks gives the basis for the following closer look from the legal perspective on issues such as data protection and from the sociologic and economic perspectives. An outlook on the future challenges of mobility and identity concludes the chapter.

6 Approaching Interoperability for Identity Management Systems (IdMS)

By Ruth Halperin and James Backhouse (all LSE)

Establishing interoperable systems is a complex operation that goes far beyond the technical interconnectedness of databases and systems. Interoperability emerges from the need to communicate data across different domains for a specific purpose. Transferring the data may represent a technical challenge because of different protocols, standards, formats and so forth. However, the most difficult challenge lies in reconciling and aligning the purpose, use and other changes consequent on transferring that data. Changes in data ownership and custodianship have an effect on power structures, roles and responsibilities and on risk. In the first part of this chapter our aim is to develop an understanding of the term 'interoperability' as it currently applies to the area of identity management. We propose a three-fold conception of interoperability in IdMS, involving technical, but also formal-policy, legal and regulatory components, as well as informal-behavioural and cultural aspects. Having noted the official EU/government agenda as regards interoperable IdMS, the second part of the chapter is concerned with the perspective of other important stakeholders on the same topic. First, the views of experts from private and public sectors across Europe are presented. Following this, the perceptions and attitudes of EU citizens towards interoperable IdMS are discussed. Together, the findings presented point to the crucial challenges and implications associated with the sharing of personal data in the provision of eGovernment, eHealth and related services.

7 Profiling and AmI

By Mireille Hildebrandt (VUB)

Some of the most critical challenges for '*the future of identity in information society*' must be located in the domain of automated profiling practices. Profiling technologies enable the construction and application of group profiles used for targeted advertising, anti-money laundering, actuarial justice, etc. Profiling is also *the conditio sine qua non* for the realisation of the vision of Ambient Intelligence. Though automated profiling seems to provide the only viable answer for the increasing information overload and though it seems to be a promising tool for the selection of relevant and useful information, its invisible nature and pervasive character may affect core principles of democracy and the rule of law, especially privacy and non-discrimination. In response to these challenges we suggest novel types of protection next to the existing data protection regimes. Instead of focusing on the protection of personal data, these novel tools focus on the *protection against invisible or unjustified profiling*. Finally, we develop the idea of Ambient Law, advocating a framework of technologically embedded legal rules that guarantee a transparency of profiles that should allow European citizens to decide which of their data they want to hide, when and in which context.

8 Identity-Related Crime and Forensics

By Bert-Jaap Koops (TILT) and Zeno Geradts (NFI)

With the ever-increasing importance of identity and identity management in the information society, identity-related crime is also on the rise. Combating crimes like identity theft and identity fraud, not in the least with the help of identity forensics, is a key challenge for policy makers. This chapter aims at contributing to addressing that challenge. It summarises the findings of five years of FIDIS research on identity-related crime and identity forensics. A typology is given of the various forms of identity-related crime. After an analysis of relevant socio-economic, cultural, technical, and legal aspects of identity-related crime, potential countermeasures are discussed. We then move on to forensic aspects, with a critical analysis of pitfalls in forensic identification and case studies of mobile networks and biometric devices. Next, forensic profiling is discussed from a wide range of perspectives. The chapter concludes with lessons drawn from the five years of FIDIS research in the area of identity-related crime and forensic aspects of identity.

9 Privacy and Identity

By Maike Gilliot (Alu-Fr), Vashek Matyas (MU), and Sven Wohlgemuth (Alu-Fr)

The current mainstream approach to privacy protection is to release as little personal data as possible (*data minimisation*). To this end, Privacy Enhancing Technologies (PETs) provide anonymity on the application and network layers, support pseudonyms and help users to control access to their personal data, e.g., through identity management systems. However, protecting privacy by merely minimising disclosed data is not sufficient as more and more electronic applications (such as in the eHealth or the eGovernment sectors) require personal data. For today's information systems, the processing of released data has to be controlled (*usage control*). This chapter presents technical and organisational solutions elaborated within FIDIS on how privacy can be preserved in spite of the disclosure of personal data.

10 Open Challenges – Towards the (Not So Distant) Future of Identity

By Kai Rannenberg, Denis Royer, and André Deuker (all JWG)

Identity was a multifaceted and challenging topic, when FIDIS started to work on it, and it will be multifaceted and challenging in future. It has relations to aspects, such as societal values, societal phenomena, application areas, technologies, and last but not least scientific disciplines. In each of these areas FIDIS worked on identity, and it became clear that each of the areas is changing, keeping identity a dynamic and multi-faceted field. It may actually get even more aspects in the future, given the fact that none of the questions have disappeared during FIDIS' work so far, but new aspects showed up, e.g., with new technologies and regulations. So even after 5 years of FIDIS, not all questions are answered. Therefore, among others, some dimensions for future work include research in identity reference architectures, IdM and privacy, IdM and multilateral security, and identity in the *Internet of Things*.

Members of the FIDIS consortium

Goethe University Frankfurt (JWG), Germany

Joint Research Centre (JRC), Spain

Vrije Universiteit Brussel (VUB), Belgium

Unabhängiges Landeszentrum für Datenschutz (ICPP), Germany

Institut Européen 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 (Alu-Fr), Germany

Members of the FIDIS consortium (next)

Masarykova universita v Brne (MU), Czech Republic

VaF Bratislava, Slovakia

London School of Economics and Political Science (LSE), United Kingdom

Budapest University of Technology and Economics (ISTRI), Hungary

IBM Research GmbH, Switzerland

Centre Technique de la Gendarmerie Nationale (CTGN), France

Netherlands Forensic Institute (NFI), Netherlands

Virtual Identity and Privacy Research Center (VIP), Switzerland

Europäisches Microsoft Innovations Center GmbH (EMIC), Germany

Institute of Communication and Computer Systems (ICCS), Greece

AXSionics AG, Switzerland

SIRRIX AG Security Technologies, Germany

Special thanks to

Stämpfli Publikationen AG, CH-3001 Bern, for supporting the printing of this booklet with a special discount on their regular price,

the Computer Science Division and the MIG research unit of the Bern University of Applied Sciences for their financial support,

AXSionics AG, CH-2503 Biel-Bienne, a member of the FIDIS consortium, for its advertorial.

AXSionics: a partner company in the FIDIS consortium

What perspective has AXSionics brought to FIDIS?

The cooperation between the FIDIS consortium and AXSionics is beneficial for all parties. The FIDIS partners elaborate the conceptual and theoretical basis for identity management and protection. AXSionics, together with other companies within FIDIS, provides models and demonstrators of the proposed concepts.

How do you evaluate the impact of FIDIS on the development of AXSionics?

The comprehensive scientific approach of FIDIS to identity, privacy and anonymity helped AXSionics to develop an authentication and transaction protection system that is in line with the newest research results on identity and privacy protection. With the information and insight on the optimal use of biometrics in the digital society that was outlined by the FIDIS NoE, AXSionics was able to design and produce a system based on biometric authentication that is safe and secure for individuals and protects their privacy as all biometric data is held only on the AXSionics Internet Passport.

What is the role of AXSionics in the identity [r]evolution?

AXSionics provides a paradigm shift in Identity Management - it reduces cost for any company accepting it and therefore the overall cost for the End-User. At the same time, no installation is required – it can be used anytime, everywhere.

axsionics
The Internet Passport Company

Neumarktstrasse 27 - 2503 Biel-Bienne - Switzerland
+41 32 321 60 00 - info@axsionics.com - www.axsionics.com

Why is AXSionics different from other companies which are active in identity management and authentication devices?

AXSionics provides a unique biometric secured peer trust solution. Unlike other solutions, the AXSionics Security Platform is designed to solve the two relevant questions in any Identity driven process - the verification of Identities (authentication) and the verification of any transaction (transaction security).

The solution consists of a centrally installed software component (AXSionics Security Manager) and the AXSionics Internet Passport, which is a personal credit card size token with fingerprint reader and graphical display.

Who is the typical End-User of the AXSionics card?

You and me – people who are concerned about Identity theft, people who have too many usernames/passwords to manage them securely and efficiently and who want to manage their Identity through one easy-to-use solution – where no installation is required and privacy is fully guaranteed.

Edited by David-Olivier Jaquet-Chiffelle

Copyright © May 2009 by the FIDIS consortium - EC Contract 507512
All rights reserved.

www.fidis.net | booklet@fidis.net

ISBN 978-2-8399-0515-2