ICT that makes the difference
The future of Ambient Intelligence and ICT for Security
International Conference

PROGRAMME
22 – 25 November 2009
Brussel

Themes and Sessions
abstracts, posters & research materials

Suggested citation:
LASTNAME, **INITIAL**. (2009). **TITLE OF PRESENTATION/POSTER**. In *Proceedings of the International Conference, ICT that makes the difference: the future of Ambient Intelligence and ICT for Security*, Brussels 22-25 November, 2009, pp. **PAGE(S)**. ICTethics, FP7-230368.

ICT, health and care

Session 1: Medical access to the brain

Brain gene transfer and brain implants

Rolando Meloni[1], Nicole Faucon Biguet[2], Jacques Mallet[1]
[1] Centre National de la Recherche Scientifique (France)
[2] Institut National de la Santé et de la Recherche Médicale (France)

Information and communication technologies (ICTs), which have an increasing widespread utilization on the daily life, have been shown to have an important impact on brain performances and to be able to improve several cerebral processes. Moreover, by abolishing the brain/machine interface using micro-implants, such technologies are being experimented as new therapeutic approaches for hearing or vision loss as well as for neurodegenerative diseases such as, for example, Parkinson's disease. In a further step, brain implants have also been advocated for correcting behavioral traits and/or enhancing cognition-related brain functions in normal subjects.

Recombinant DNA technologies are also having a profound influence on modern living and their application for gene therapy is revolutionizing the medical approach to several diseases. In particular, gene transfer (GT) in the brain is a promising methodology for restoration therapies in neurodegenerative disorders, but, from a theoretical point of view, may represent also an innovative treatment for psychiatric disorders. Therefore, in a further step, gene transfer in the brain may also be sought as a powerful tool for modifying behavioral traits and/or enhancing mind abilities.

Brain-related ICT and GT have several common features that make their therapeutic utilization in the central nervous system particularly valuable. One of the most important of these features is that brain implants and GT constitute a more reliable and specific alternative to drug treatments, by allowing to intervene in a specific and limited brain region and to avoid the secondary and widespread effects of pharmacological manipulations. Also, their mechanism of action, in its simplest form, is related to the amplification or inhibition of an electrical/chemical signal in the case of ICT and of the expression of a specific gene in the case of GT. Moreover, the outcome of these procedures is, in both cases, not limited to their specific target, but impinges on the target-associated networks that may convey the specific effect to different brain regions. However, albeit these techniques are characterized by fundamental similarities and the pursuing of similar goals for therapeutic purposes in the brain, their development has followed separate paths. Moreover, from the ethical point of view, their utilization and the possibilities linked to their development has generated a series of debates that have tackled somewhat different issues.

Brain-related ICT and GT have also common drawbacks, due, in the case of brain implants, to the inherent relatively low efficiency in adapting a mechanical device to the complexity of the brain neural wiring or, in the case of GT, to the transducing of a limited number of neural cells by the appropriate vectors. However, in several instances, these drawbacks can be theoretically overcome by merging the two techniques. Thus, since both techniques may have similar effects with different mechanisms and are well suited for the brain environment, it is foreseeable that they will be used concomitantly for several applications. Moreover, the combination of GT with brain implants may not only ameliorate the technical efficiency of each method, but also exponentially increase their therapeutic and/or enhancing effects. In this perspective, the introduction of GT at the brain machine interface may represent a net improvement in the field of ICT and, at the same time, it may open new scientific perspectives, as well as raise new ethical concerns.

Session 1: Medical access to the brain

Direct brain-computer interfaces: individual, social, and ethical issues

Elisabeth Hildt[1]
[1] University of Mainz (Germany)

Considerable increase in our knowledge of the structure and function of the human brain has prompted the development and use of neurotechnological approaches such as direct brain-computer interfaces (BCIs) which allow brain signals to be used for communication and control of movement. Currently, there are invasive and non-invasive approaches under development. Up to now, the very promising BCI technology has been used in patients suffering from severe diseases such as amyotrophic lateral sclerosis (ALS), stroke, spinal cord injury or cerebral palsy.

During the presentation, current clinical applications and possible future uses of brain-computer interfaces as a means for communication, motor control and entertainment will be discussed and the EU-funded integrative project "Tools for Brain-Computer Interaction (TOBI)" will be presented. In this, the focus is on non-invasive BCIs for these have several advantages over invasive BCIs: low medical risks and a favourable risk-benefit ratio; accessibility for a large number of persons; and reversibility.

Then, individual, social and ethical implications of direct brain-computer interaction will be discussed. These will include aspects concerning quality of life, independent living, autonomy, social participation and e-inclusion, as well as issues concerning privacy, data protection and distributive justice.

A particular focus will be on possible influences of BCI use on human self-understanding and the idea of man. For in view of the direct interrelation and mutual interdependence between human brain and technical devices, manifold anthropological issues arise that need further discussion. These include concerns regarding a technicalization of the human body, the encouragement of a reductionist or functionalist view on persons and their brains, and speculations relating to *cyb*ernetic *org*anisms; *cyborgs*.

Responsibilities within an Ambient Assisted Living healthcare project

Neelke Doorn[1]
[1] Delft University of Technology (Netherlands)

In this paper I would like to present the results of a series of interviews with researchers within an Ambient Assisted Living (AAL) project: the Dutch ALwEN project (where ALwEN stands for Ambient Living with Embedded Networks). The interviews are part of a so-called embedded ethical research. The idea behind this type of research is that ethical investigations are carried out parallel to, and in close cooperation with, a specific technological R&D project. The ethicists interact with the technological researchers, allowing the ethicists to co-shape new technological developments by interacting with the technological researchers. The particular aim of this ethical research is to identify how the researchers distribute the responsibilities for addressing moral issues, related to the technology under development.

The ALwEN project is aimed at developing a prototype application of a novel technology based on Wireless Sensor Networks (WSN), the combination of body sensors, ambient sensors and wireless networks. In order to capture the whole trajectory of fundamental research to the development of a pilot application and ultimately commercial exploitation, several universities, a consortium of 12 Small and Medium Enterprise (SME) companies, industrial companies and a scientific research centre in rehabilitation technology cooperate. In the project a use case is developed to serve as an example of what can be done with WSNs and to focus the work of the demonstration activities of the project. The prototype application will be developed according to a health care related use case aimed at in-house monitoring of daily activities (patient with COPD). Within the project, end users, including health care professionals, are consulted to clarify their wishes and demands with respect to the environment to be created. After a first experimental set-up of the sensor and actuator network, exploring experiments with real users will be carried out to determine the functional and technical requirements in more detail. Afterwards the experimental WSN will be evaluated both in terms of the technical specifications and in terms of the objectives set to improve quality of life of the users.

At the start of the project ‘social acceptance’ was identified as one of the crucial points for the successful implementation of the technology. In addition to technical and economic goals, the project consortium had therefore set itself the following two goals related to the social acceptance of the application:

- Quality of life: the project will develop a pilot application to monitor and assist the activities of end users. The main ‘societal criterium’ for the success of this application is that it contributes to the quality of life of the end users, in the sense that it helps them to maintain their independent living.
- Security and privacy: even though personal information may be pervasively collected and distributed over wireless communication channels, the security of the information and the privacy of the patient must be guaranteed. As part of the embedded ethical research, it was studied to what extent the researchers within the project agreed upon a definition of social acceptance and how an attempt was made to address it. In addition it was asked whether the researchers did expect any risks or relevant ethical issues stemming from this type of technology and if so, whom they would ascribe the responsibility for addressing these risks to. A first interpretation of the interviews shows the following results:

1. Definitions of social acceptance: When asked about what ‘social acceptance’ means the technical and clinical researchers gave different answers. The issue that was most often mentioned was the invisibility or non-interference with everyday life. The future users should feel comfortable with the application. Most researchers also mentioned that future users should see the added value. Some researchers gave a more ‘technical interpretation’ of social acceptance: the application should be reliable, functional and user-friendly. Privacy and security were mentioned as well, but mainly in a technical sense (i.e. in terms of encryption techniques). One interviewee explicitly mentioned that security also has a more ‘social’ component: how to make the application such that people will use it in a secure way. Some interviewees mentioned that social acceptance is not limited to acceptance by the end user: the social context (including the doctor and the family) should also accept the technology. Lack of stigmatization was also mentioned as a requirement for social acceptance. None of the interviewees applied an assessment of the desirability of the technology external to the user itself: it was up to the end user to decide on the social acceptability. One interviewee formulated it as such: the proof of the pudding is in the eating; if it is being used, than it is apparently being accepted. Most technical partners delegated the responsibility for getting this social acceptance to the clinical partner or the principle applicant of the project (project management).

2. Ethical issues/risks stemming from the technology: the interviewees were asked to identify potential risks and/or moral issues stemming from the particular application being developed within the project and from other potential use of the technology. In addition to privacy and security, which are also explicitly mentioned in the project plan and identified as formal work packages, the following points were mentioned: the (un)desirability of steering behavior due to feedback from the application, waste (electronics in the environment), balance of costs versus security/privacy solutions, relation with law and medical standards, questions related to data storage and access to data, illegitimate use in order to mislead the system, illegitimate use of the data by insurance companies, liability questions due to the availability of new data. Since the present health care application was by most interviewees conceived as a rather ambitious application, no additional risks or moral issues stemming from other type of applications were mentioned.
3. Ethical issues/risks during the development of the technology: when asked about the risks and ethical issues of the wireless technology some interviewees also mentioned the ethical issues *during* the development of the technology. To gain informed consent from the volunteers participating in the test experiments was mentioned as the most important issue. In case of development of an application for mentally incompetent users this is problematic, one interviewee remarked.

The interviews show that the researchers employ a broad range of interpretations of 'social acceptance' and that they are able to identify risks other than the common worries about security and privacy. Most technical researchers ascribe the responsibility for social acceptance and ethical risks of the present application to the clinical partner involved and the project management. For future applications these responsibilities are delegated to the commercial partner that will ultimately deploy the technology.

The next step in the embedded research is to invite the technical and clinical researchers for an interactive session in the *Group Decision Room* (GDR; a room with electronic meeting support systems that allow for a participative approach to complex tasks such as (anonymous) discussion, brainstorming, voting et cetera) and to discuss with them the results of the interviewees. The preliminary results of this GDR session will also be presented at the conference.

An Innovative way of learning: adaptive decision mobile learning system for people with mental disabilities

Saeed Zare[1] , Heidi Schelhowe[1]
[1] Dimeb (Digital Media in Education), University of Bremen (Germany)

Usage of mobile technology is growing and affects other technologies with new motivations of *any time, anywhere*. At the same time, the difference between mobile phones and hand-held computers is becoming less and less apparent. Mobile learning can be seen as a bridge between practical exercises and theoretical knowledge. It can support several functions that enable orientation in context and space of a certain field or task. We considered the idea of mobile computing as a learning context, which is embedded in everyday working environments. The integration of working and learning in one process is supposed to support the acquisition and revelation of tacit knowledge that seems to play a crucial role in this context.

This abstract describes the main ideas and the architecture of an ongoing study of a system called Intelligent Mobile Learning Interaction System (IMLIS) that provides a mobile learning environment for people with mental disabilities (mostly with learning difficulties). The design of this system is based on the idea to adjust its content, the kind of tasks and the mode of display to specific needs of individuals and to engage them for learning activities with new learning motivations due to a dynamic structure and flexible patterns. We want especially to recognize the factors that make limitations and influence the learning processes of people with mental difficulties, in order to improve their learning opportunities. Here we show first results of designing a mobile application for people with special needs (focusing on mentally disabled) highlighting active learning to arouse their interest and to improve their learning results.

Commonly, people with mental disabilities have delay in their physical, cognitive and social activities and have less stamina than normal people. Hence, dividing the learning activities and interactions into smaller and controllable parts, repetition of learning material in a period of time, using an easy language and preparing more visualized material, facilitate the learning process for these people. They should be able to associate perception with concepts and contents. IMLIS firstly analyzes and identifies specific requirements, constraints and conditions of the person through different interactions and then tries to cover such kind of issues dynamically according to the level of weakness. By adapting to mentally disabled learners and their special abilities, the system should be able to prepare an appropriate profile or model for the learners, which can actuate the way for an adapted-learning process in presenting and memorizing the learning material.

This system can take the role of a flexible companion that is embedded in daily life of a person with special needs. As a kind of tutor it guides the learning experiences of the person. By an embedded situated help system, the users should get encouraged to face new tasks with higher degree of complexity. Prospectively, this virtual supported reliability could foster their autonomy and independence from advisers. The development consists on several iterative steps evaluated with tests. In the relevant step of basic system, database with decision engine connected to templates, patterns and the learning data are designed and a mobile client is built.

The system architecture consists of two parts, a mobile client and a server. The client is a mobile device, which is connected via a wireless protocol to the server, and the server is a standalone device that feeds the client with appropriate learning materials. In this mobile learning solution, a user's request is captured by the system, and the analytical material will be sent from the server to the client for analysis. The learner (or his teacher/parent) is asked to answer the questions or analytical games that are produced by the program. This information, gathered during the interaction, is recorded and classified according to a categorizing system based on the World Health Organization (WHO) standards and is sent to the server as an "Analytical Package" (called AP). The server receives the AP from the client, and starts to analyze the package according to predefined algorithms and definitions. A decision engine decides - according to the AP information - about the learning material and the didactical format appropriate for this specific category of learner that is specified and available in the database. A "Learning Package" (called LP) is composed and sent to a mobile client. The mobile client receives the LP and presents the learning material to the learner. An individual portal is also designed for user administration and learning material management.

At the end of the learning process, a feedback test will be offered for the learner to verify the performance of the process. During the feedback test, the results are saved locally on the mobile device, but with the next connection to the mobile server, the data will be synchronized and uploaded on the server in order to be applied for the next decision which decision engine has to make for the same (type of) user.

Our system is supposed to motivate people with mental difficulties for portable access to a learning process, increasing the learning performance with dynamic learning material and finally customize of their own learning based on their abilities and the history of usage. For example if the learner has a slow reaction time, the time for the presentation of the learning material in the output is affected by that factor. On the other hand, the feedback at the end of the learning process and application of results for the next decisions will also influence the process. This is like traditional learning where teachers get familiar with students' background after several sessions and will interact with him/her according to his/her abilities.

We apply knowledge from the field of research and practice with mentally disabled people as well as pedagogical and didactical aspects in the design in order to get an effective result in learning process.

Security and biometrics

Session 1: Security in Danger

The digitalization of the European migration policy

Michiel Besters[1], Frans Brom[1]
[1] Rathenau Institute (Netherlands)

The external borders of the European Union are steadily becoming digital borders. In the past, border control was a matter of a passport and barrier. Today, information systems make the difference being admitted to the European Union or not. For example, since 1995, the Schengen Information System (SIS) is used for registering and tracking wanted and unwanted persons and objects and Eurodac has been implemented to register applications of asylum seekers. With these two information systems already in place, the European Commission has expressed its intention to shape a 'single technical platform' or a unified 'European Information System' to control the migration flow that enters and leaves the area of freedom, security, and justice. Besides SIS and Eurodac, in the near future a database will be ready to register visa applicants in the Visa Information System (VIS). In the mean time, the European Commission has submitted proposals for databases to track persons whose visa is expiring (Entry-Exit System) and to store biometric data complementary to the SIS and VIS 0(Biometric Matching System).

This growing number of information systems has urged the European Commission to present a proposal on the establishment of a regulatory agency for large scale IT systems. Governed by a management board consisting of representatives of the member states and the European Commission, this agency will have several responsibilities. First of all, the agency will be responsible for the operational management for the information systems. Additionally, the agency will publish statistics, arrange training activities, implement pilot schemes and so on. Importantly, the agency will also be responsible for data security and integrity as well as compliance with data protection rules. In the long run, the regulatory agency is envisioned to become a centre of expertise for IT systems in the area of freedom, security and justice. In this paper, the digitalization of the European migration policy will be assessed. Controlling the migration flow by means of digital information is inescapable. Nevertheless, the 'digital fix' of the migration policy produces some side effects that should not remain unnoticed. This paper addresses two issues. The first issue concerns the functional design or architecture of information systems. Who has access to the system? Who makes use of the information and for what reason? The second issue evolves around the position of the third country national. Are the data protection rights (i.e. inspection, correction, and deletion) of the third country national guaranteed in theory and in practice? These two issues will be addressed by taking one information system as an example: SIS.

The SIS is the largest European database being used by twenty-five member states and containing over seventeen million registrations. It facilitates the exchange of information between authorities responsible for border checks, thereby enabling the free movement of persons and objects within the Schengen area. Due to new technological possibilities, new functionalities have been added to the SIS. The moment when the integration of new member states to the SIS had become impossible, it was decided to built a new generation of the SIS: SIS II. In this respect, it appears that the SIS has been 'under construction' ever since it was introduced. This general feature has enabled to turn the SIS in a multipurpose tool: next to being a tool for registering persons and objects, it is now also used as an investigation tool. Is this a matter of function creep or just making SIS a multipurpose tool? The multipurpose character is the main reason that the SIS II is not operational yet. With another delay or even cancellation to become reality in the near future.

Secondly, since the SIS is under construction all the time, the data protection rights of third country nationals can barely be practiced. The number of authorities with access has grown and the type of authorities has widened, implying that the number of entries to the system has increased. With a clear overview of authorities and entries being absent, it is unclear whether the data protection regulations are being enacted properly. Additionally, the growing number of participating member states complicates possibilities to exercise one's rights to inspection, correction, and deletion. Since a third country national is usually not informed when s/he is registered in the SIS, it is far from clear to whom s/he should turn to exercise his/her rights. Doesn't this lack of transparency unveil a democratic deficit?

In the conclusion, a return will be made to the digitalization of the European migration policy. Which lessons can be drawn from the development of SIS? Two issues will be addressed. First of all, it would be better to restrict the goals of

an information system as much as possible. A database with limited possibilities functions much better than a giant database that serves a broad range of purposes. Secondly, it will be argued that the digitalization of the European migration policy is in need of a clear arrangement to enable a third country national to exercise his data protection rights properly. The regulatory agency for large scale IT systems could be a step forward. But what about the member states? In practice, the member states are in the end decisive for respecting the immigrant's rights.

New security technologies: beyond the privacy-security dilemma

Vincenzo Pavone[1], Sara Degli Esposti[2]
[1] Institute of Public Policies (IPP) – CSIC (Spain)
[2] University Carlos III Madrid (Spain)

Current globalization processes seem to be increasingly characterized by the emergence of global risks, which are now coming to the fore in all their threatening potentiality. Whilst these threats urge national and regional governments to implement new security policies based on the introduction of new technologies, like biometrics, the public perception of these technologies increasingly constitute a benchmark to guide governmental actions. Research on the public perception and the social implications of security technologies has mainly adopted a framework that presents privacy and security as two opposite goods in a trade-off model, according to which citizens may renounce to some of their privacy in exchange for more security. This simplistic model, however, has been recently criticized from three different perspectives. The first group argues that presenting the relationship between privacy and security, merely in terms of a rational trade-off, tends to neglect the technocratic and authoritarian implications often associated with the introduction of these new technologies (Levi and Wall 2004, Zureik 2004, Spence 2005, Liberatore 2007). Inspired by a Foucaltian perspectives, the second group has criticized the trade-off approach for it removes from the critical gaze the implicit power relations associated with the use of biometrics for risk profiling at the borders and the relative issues of social and racial discrimination (Amoore 2006, Cote-Boucher 2008, Muller 2008). Questioning the hermeneutical validity of the trade-off model in the analysis of public perception of security technologies, the third group has expressed three main concerns: the high level of abstraction which does not take into account the variety of national contexts in which security technologies are implemented (Knights et al. 2001, Dourish and Anderson 2006); the one-dimensionality of its approach, which takes for granted that more security necessarily implies less privacy and vice versa (Bowyer 2004, Strickland and Hunt 2005, Riley 2007); but also for the narrow frame in which the 'public' is addressed, which disregards that several publics exist and present different approaches towards both the security technologies and the socio-political institutions in which these technologies are likely to be introduced (Davis and Silver 2004, Gaskell et al. 2004).

This paper draws from the experience and the outcomes of the PRISE Project, "Privacy Enhancing shaping of security research and technology", which was funded under the EU 6th framework programme, DG security research, and came to an end in 2008. Combining quantitative and qualitative techniques in an interview meeting, this paper analyzes the public understanding of new security technologies and offers intriguing insights on the security and privacy discourse in Spain. First, in spite of the March 11 terrorist attack (2004) and the media and governmental emphasis, it seems that terrorism is far from being the main security concern. In fact, the Spanish citizens interviewed seem to be not only aware of the implications of new security measures in terms of political use and control but also afraid of the risk of commercial exploitation. Actually, they seem to hold a different perspective, which emphasizes the quality of security measures rather than their quantity. Second, the people interviewed seem to be aware, to a different degree depending on their personal history and experiences, of the social and political implications suggested by the literature. In fact, despite the significant variety of diverging opinions, all groups not only formulated clear suggestions for the elaboration of responsible and effective guidelines in the introduction of new security technologies, they also remarked that both the participation of citizens and civil society in the elaboration and implementation of both norms and technologies. Finally, they all agreed that the existence of a clear legislative and juridical framework to regulate these technologies and ensure the accountability of politicians, policy-makers, industry and actual operators is vital for the preservation of democracy and civil coexistence.

With regards to the main critiques raised against the security-privacy trade-off from a critical studies on public understanding of science, the interviews, and the data delivered from the survey, suggest that a majority of participants do not approach the relation between privacy and security as a trade-off: rather their opinion on privacy and security seem to be primarily the result of a prior orientation along the trust/concern continuum. In other words, the more they trust government, companies and public institutions the more they see security as a priority, whilst the more they distrust public institutions, companies and government the more they consider privacy as a priority. In this respect, their attitude towards a specific technology may relate more to the institutional context in which this technology is introduced than to the technology as such. If public trust, or mistrust, is mainly oriented towards institutions and operators – those that use these technologies as well as those that are supposed to monitor, regulate and enforce the rules – there is no real trade-off game at stake. In fact, people tend to divide into two distinct categories, trust and concern, with different attitudes towards privacy and security. For those belonging to trust, privacy is not likely to be affected by enhanced

security measures, in fact it is not even an issue: they do not see a trade-off, simply because they do not see their privacy being curbed. For those in the category concern, security is not likely to be enhanced by these technologies; they only see their privacy being restricted. For them there is no trade-off either, because they do not see security being increased while their privacy is affected.

Whilst further empirical studies, with larger samples and ad hoc questionnaires, are necessary to validate this hypothesis – the latter, if confirmed, may have crucial implications for policy-making in security and technology policy. It will no longer be an issue of striking a balance between improving security and protecting privacy through the introduction of new technologies; rather national and regional institutions will be required to improve citizens trust through the introduction of clear norms, effective accountability mechanisms, civil society participation, juridical protection and increased transparency in political decisions about risks, security concerns and relative policy measures.

In a context of rising security concerns, expanding definitions of risk and growing governmental monitoring activities, this paper may cast some light on the persisting gap between the governmental and the lay public perception of security agenda as well as on the political implications of the new public discourse on security.

Security in the danger zone: normative issues of next generation biometrics

Irma van der Ploeg[1]
[1] Zuyd University (Netherlands)

For many years now, biometrics have been the subject of public debate, critical and ethical reflection, and regulatory efforts. The fact that certain developments in pattern recognition and sensor technologies enabled the use of human bodies for identification and authentication purposes in a wide variety of contexts triggered wide enthusiasm as well as worries from the beginning. Now, some two decades further on, we see not only a widespread and large scale use of this technology, ranging from the local and private applications to the gigantic government owned and even internationally coordinated systems, but also a qualitative technical development that leads many to speak of the emergence of ‘second generation biometrics’ In this chapter, I discuss some key elements of this development of second generation biometrics that give rise to a new set of ethical and socio-political issues to be analysed and discussed. The two main elements of recent developments in biometrics I want to focus on here are first, the emergence of new biometric traits, often for multimodal use in combination with more ‘classic’ traits, in particular so-called soft biometrics and physiological biometrics, and second, the shift to embedded biometric systems, which includes an emphasis on distant sensing and ‘passive’ biometrics, and which forms a key element of the wider trends towards Ambient Intelligence (AmI) and ubiquitous computing (UbiComp); I will focus in particular on security related applications. Together, these developments signify a new level of complexity not only of the technology, but also of the critical issues and policy challenges connected with it.

I will first discuss the emergence of `soft biometrics’, i.e. the use of general traits such as gender, height, age, ethnicity or weight for automated classification or as supporting information in identification and authentication applications. Such techniques, I will argue reify social categorisations that are highly sensitive and essentially contestable, thereby closing them off to inspection, debate and contestation. Next, I will focus on the shift towards embedded systems and Ambient Intelligence, in which biometrics are foreseen to play an important, facilitating role. Distant sensing and so-called `passive biometrics’ that require no conscious cooperation from subjects, are at the centre of this development, giving rise to some obvious concerns about covert data capture, transparency and consent. Following this is a discussion of another set of new biometric traits that recently have become research and developed into authentication and assessment tools, namely physiological states and phenomena such as heart rate, body temperature, brain activity patterns, and pupil dilation. These ‘under the skin biometrics’, are so far applied mostly in various security contexts, bring a whole new range of body data within the reach of data controllers, and especially when used in embedded and passive fashion, need to be assessed from social and ethical viewpoints urgently. Drawing the various types of developments discussed together, I next identify and articulate a highly normative assumption embedded in biometrics, that these various new technologies appear to be stretching to unprecedented extent: the assumption of availability. The very idea that one can direct biometric sensors and connected identification, inspection, and assessment tools at people’s bodies, and register ever more, and ever more intimate aspects of even the general public, presupposes the body to be available in ways that perhaps ought not to be simply taken for granted.

Mission impossible? Security and Protecting personal data (including biometrics) of the vulnerable. Cases of theft and loss.

Daniel Nagel[1]
[1] Wirtschaftsrechtskanzlei, Bongen, Renaud & Partner (Germany)

1. Introduction

The German Data Protection Commissioner once stated that on the basis of the German Data Protection Act the use of personal data would be forbidden as long as it was **not explicitly allowed**, thus providing a sufficient scope of protection for personal data. Unfortunately, this statement does not hold true in every respect for two reasons: first of all, the fence which is built around personal data by the German Data Protection Act contains severe loopholes and secondly, the above statement blurs the fact that the term "explicitly allowed" can be seen – and unfortunately is seen by many data controllers - as negotiable.

To put it in other words: as long as there are sufficient means to trick people into disclosing their data – be it just basic information such as their address, gender and date of birth or even biometric information via the taking of fingerprints or blood tests – there is no rule within the German law on Data Protection that prevents data controllers from knowing more about you than you do yourself.

Is the protection of personal data of the vulnerable an impossible mission? The answer is a clear, "it depends"; at least as far as the German regulations on data protection are concerned, as even the sharpest regulation is not worth the paper it is written on if it cannot be effectively be put into practice.

2. Examples of theft and loss

Unfortunately, there is no need to browse dusty archives in order to come across cases of theft and loss. Arguably, the internet boosted the development of new threats to personal data, however, it is still not the only place where information is stolen, disclosed or forwarded: data is e.g. collected via the use of customer cards, CCTV, theft and loss of storage devices and the interception of snail mail.

In addition the fields of personal data where theft and loss occurs are widespread. Recent cases go from loss of standard data, such as addresses over financial data (e.g. bank account numbers, tax details) or personal preferences (monitoring of behaviour) and up to biometric data.

The alarming fact, however, is that the development of these cases seems to keep pace with globalization. Examples from the past year in Germany are a vivid illustration thereof:

- Last December a big regional bank lost credit card data of 130.000 customers (lost in the course of a courier transport)
- In March a subcontractor of a big telecommunications company forwarded details on over 1 million customers to third parties
- In April news broke that the biggest German telecommunications company has been serving the Federal Criminal Police Office with data of several million customers
- In October (the black month of this year)
  - a big financial services company lost data of 27,000 customers (which was solely detected due to the fact that the data was offered to a newspaper)
  - there was a theft of data of a million users (predominantly minors) within the biggest social media network in Germany
  - a book retailer accidentally published half a million invoices
  - a Google update led to the accidental publication of personal documents
  - news broke that two big pharmaceutical companies and a very big automobile company request that applicants submit blood samples

However, the private sector was not solely involved. There were also cases of severe data loss within public authorities during the past few years. These include *inter alia* the accidental publication of criminal records on the internet by a local police authority or the theft of over 500 computers, storage devices and disks which contained biometric data on citizens from a governmental authority.

Specifically, theft and loss of biometric data constitute a major problem. This is due to the fact that biometric data is relatively stable, i.e. it cannot be easily changed. Hence, the loss of biometric data has a long-term impact on data subjects. In addition, if one takes the idea of using biometrics in order to prove identity into account, e.g. with regards to

the introduction of eIdentity cards, the risk of identity theft skyrockets.

This contrasts with the fact that the use of biometrics, e.g. via the use of fingerprints, retina-scans, iris- scans, face-scans or voice-scans is often seen as a **secure mechanism of proof;** however, **this can be doubted** as there are also many weak links within such mechanisms which can be attacked (e.g. via the use of a fake finger, the interception of the data process after a fingerprint has been taken, the change of templates which are used as a reference for the biometrics or the enrolment with vague templates which allow for a variety of matches).

Furthermore, the loss of biometric data also entails additional problems. A database full of addresses is just … a database full of addresses. **A database of iris-scans on the other hand, also includes information on the health of the data subjects and a database of face-scans includes information on the ethnic origin or religion**, etc.

3. MECHANISMS TO SAFEGUARD DATA

There are several acts in Germany which have been passed in respect to the protection of personal data. The most important among them is the Federal Data Protection Act. However, this Act has already been labelled as an act with a near expiry date as the Act unfortunately is **too complex, which in turn entails legal insecurity** and might even render the provisions ineffective. Arguably, the basic principle behind the Act is that the collection, storage and use of personal data is only admissible on the basis of an explicit consent of the data subject, this is a good starting point. Nevertheless, this principle is already questioned by the Act itself as there are considerable **exceptions, which can easily be abused** (it is e.g. admissible to collect and use personal data if it serves as a means for advertising, market research or opinion polling, as long as there is no predominant legitimate interest of the data subject to the contrary). Moreover, there is a rather weak second level protection once a data subject has been tricked into consenting to the collection and use of personal data. Hence, there is not only a problem of real theft and loss, but also the problem of legally non-measurable abuse.

The abuse of exceptions is mainly possible due to the grey area of marketing and the so-called, “list-privilege”, which allows for the transfer of addresses, as long as the data is summarized in a list on members of a certain class which is restricted to business data (name of organisation, profession), names, titles, university degrees, addresses, years of birth and memberships of the respective class. The abuse is effected via tricking people into disclosing their data in the course of e.g. fake lotteries. The data collected is statistically evaluated afterwards and the weak, mainly elderly people regularly receive calls where trust is created via stating data taken from such lists first. Then, the weak are charmed into disclosing more information and coaxed into concluding disadvantageous contracts. This can be partially countered by the statutory duty to inform the data subject about the origin of such personal data - which has recently been included into the Federal Data Protection Act - and by provisions on consumer protection on the basis of the Distance Selling Directive, if the remedy is used in due time.

However, once such lists (which are rarely limited to the legally admissible details) exist, they gather a momentum of their own. The content grows and the chances of tracking down the initial offender decrease. A German newspaper was recently offered data of up to 21 million citizens for 12 million €. This mirrors the market price of such lists on personal data which are usually sold at 0,50 to 1,00 € per data subject.

The weak second level protection makes things worse. Hence, if there is an initial written consent, it is very difficult for data subjects to prevent further developments. Arguably, there is the right to revoke such consent and, moreover, the duty on data collectors to inform thereof. However, the **awareness is relatively low** and the actual execution is rarely fully possible. Once such data has spread, the request to delete the data is a flash in the pan. While deleting the respective data in one place, its clone brothers are happily dancing elsewhere. In addition, even the data protection authorities encounter difficulties to track down the real offenders. Thus, the assertion of fines on this basis is relatively rare and offenders carry on despite the considerable fines.

Furthermore, the laws on data protection have to be able to keep pace with recent developments such as outsourcing or visual storage. For example, it is **unclear how to deal with outsourcing across inner-European borders and, in particular, how to deal with outsourcing outside the EU.** The principle of territoriality leads to severe legal loophole and the principle of an equal level of protection within states that do not belong to the EU cannot effectively prevent a further forwarding of such data. In particular, as both the European dimension and the fact that the applicability of national legislation on data protection stops at national borders would bind German courts to accept the second outsourcing. Consequently, there is the danger that data will be transferred to either the very European state with the most liberal regulation on data outsourcing or to a third state, which might have an equal level of protection but no controls with regards to outsourcing. Consequently, even strict data protection provisions are only as strong as the weakest link.

If the legally measurable cases of theft and loss mentioned at the beginning are added thereto, a grim outlook cannot be seen as surprising.

4. A PROPOSAL FOR FURTHER IMPROVEMENT

Who is to blame ? What can be done ?

There is no single answer. **Multi-layered problems call for a multi-layered approach.** Arguably, the legislator has to stitch up the holes within the existing legal framework. Nevertheless, the respective tailor needs a very big needle in order to form a rag rug of legal protection. To put it differently: if there is **a common European or even a global approach, on both a statutory and a voluntary basis**, the major difficulties can be tackled. The Privacy Promise of the UK Information Commissioner's Office can be seen as a good preliminary step in this respect.

In addition, the data protection authorities need more support, both on a financial and an operational level in order to effectively counter abuse of personal data. This should involve a European or trans-continental cooperation respectively. Even the setting up of a special task force (such as the specialist unit of OLAF) might be useful in this respect.

Furthermore, there is the need to keep pace with offenders technologically. If there are sufficient secure mechanisms involved, such as e.g. the idea on cancellable biometrics via the use of different hash algorithms which prevent the reconstruction of biometric templates, cases of theft and loss might not entail as much damage.

However, one of the most important factors, is the spreading of awareness. This is a task shared by governments, academics and the media. If data subjects are aware of their rights and of the potential risks, they might be less willing to disclose their data in the first place. Such an awareness campaign could be accompanied by incentives such as creating public databases on offenders, or awarding certificates for secure data handling to both the private and the public sector.

Session 2: Emotional Biometrics

Biometric monitoring of behaviour

Dimitrios Tzovaras[1]
[1] Aristotle University of Thessaloniki (Greece)

[**Summary**]

3rd generation biometrics is a further scientific development that goes beyond the hard biometric identifiers (fingerprints, facial image, iris) or combines them with other biometric identifiers promising more convenience and accuracy. Dimitrios Tzovaras presented application scenarios for deployment and prototypes based on research framed by HUMABIO Project Innovations & Achievements (FP6) and ACTIBIO Project Objectives and Innovations (FP7), raising questions on their possible uses and implications for the society. Tzovaras presented research and development of:

- Unobtrusive biometric technologies for person authentication and monitoring in controlled sensor network infrastructures.
- Secure biometric frameworks that address the fusion of multiple biometric characteristics for human authentication and monitoring.

The HUMABIO project addressed the current biometric issues of the increased unobtrusiveness of biometric systems and the biometrics exploited to enhance safety for critical operations. They introduced new biometrics (EEG, ECG, Body anthropometrics) combining them with unobtrusive conventional ones (Gait, Face, Voice), promising accuracy. Furthermore, the introduction of unobtrusive sensors for biometry (Sensing seat, Wireless ENOBIO Cameras, Microphones) and the design of new application scenarios for unobtrusive authentication (airport environment, truck/car environment, office/lab environment) are promising to increase the unobtrusive continuous authentication and monitoring. *The applications of these technologies guarantee trust and privacy concerning the citizen's personal biometric template and data.*

In the following discussion, there were a lot of questions concerning the combination of these authentication systems with identification systems that would increase the citizens' suspicions and limit the rights to privacy and dignity in a surveillance society. The use of a biodynamic physiological profile which is unique for each individual, raises new concerns regarding ethical issues and it is assumed that although the benefits of such technologies (eg. smart house, abnormal events detection) there should be the interaction between scientists and analysts of the ethical, socio-economic, and legal aspects (ESLA) of this science in order to prevent (?) complications and adverse effects.

Related ethical issues:

- Privacy; there are concerns regarding the monitoring cameras that can authenticate people by facial dynamics.

Issues for future analysis and research:

- How and who can guarantee the reasonable use of such technologies?
- The uses of new biometrics, based on our behavioural characteristics, raise concerns about our identity.
- Combining authentication systems, based on behavioural characteristics, with identification systems could have as a consequence we end up in a very intrusive surveillance society.

Session 2: Emotional Biometrics

Limits and possibilities for use of biometrics in public policy

Peter Hustinx[1]
[1] European Data Protection Supervisor, EPDS (Belgium)

[**Summary**]

The European Data Protection Supervisor stated, in the beginning of his presentation, that the existence of both security and privacy in security technologies is not an impossible mission. In fact, the accountability and responsibility of the operators have been increased in order to achieve this goal. Furthermore, Mr. Hustinx stated that biometrics is a very intelligent technology that can protect privacy. The use of biometrics has been criticised but the impact of this technology is depending on the scale we use it. If we ignore the impacts of biometrics in the first steps, where the scale is limited, then, of course later on, the consequences are unwelcome. Referring to Eurodac, he stated that it is a very important tool and EDPS guarantees that reasonable (proportionate) amount of data are stored.

Mr. Hustinx underlined the importance of the data protection. He stated that the European Commission and Parliament get their advice and guidance from the data protection law before they establish any procedures which may impinge on legal concerns and related issues. In addition, EDPS has the role to monitor relevant decisions to make sure that personal data and privacy are protected. There is always a consultation context under which all the Information Systems are regulated. Obviously, biometrics technology is not perfect. This is the reason why there are limits. Fingerprints for example can have the positive/ negative alarm. However there are ways to protect fingerprints as valid data by defining the means of their collection and collecting the adequate number of prints for them to be accurate. It is without doubt that the measures to guarantee valid fingerprints are expensive and for this reason member states have compromised.

European Union established biometric passports that are proven to be good enough but they have consequences due to large amounts of biometric data. Indeed, this is the reason why a central storage with linkages would create problems and the possibility of fraud is one of the major concerns in the implementation. The advantages of the biometric passports use can turn into disadvantages and EU has to deal with these implementations. We have to count the pros and cons applying the new technology, first on a small scale.

The following discussion flagged up concerns regarding, mainly, the specification of the purpose of biometric identifiers and proportionality.

Related ethical issues:

- Privacy; there are many concerns regarding the misuse of biometric identifiers and the exchange of data between the member states.
- Proportionality; how many biometric identifiers are adequate? Which are the purposes of collecting the biometric data into data banks? Who can use the biometric data, and for which reason?

Issues for future analysis and research:

- Mr. Hustinx underlined basically the scale of the biometric data collection. How can we measure this scale when the biometric data are stable, permanent and unique for each person?
- Some of the technical risks were mentioned as well, e.g the people who are not recognisable, what is the regulation for these people? Does this lead to social exclusion and does this fact support the argument about the abuse of dignity?

Legal Aspects

Session 1: RFID. Implants and the Human Body

Legal aspects of ICT implants

Stefano Rodotà[1]
[1] La Sapienza, Fondazione Basso (Italy)

Diane Whitehouse[2]
[2] The Castlegate Consultancy, (United Kingdom)

Penny Duquenoy[3]
[3] Middlesex University (United Kingdom)

[**Missing**: abstract or summary]

Session 2: Privacy: Towards an Electronic Identity?

Legal concepts of human identity?

Stefano Rodotà[1]
[1] La Sapienza, Fondazione Basso, Rome (Italy)

[**Missing**: abstract or summary]

On Interpreting and Constructing (Non-)Human Identities

Rafael Cappuro[1]
[1] International Center for Information Ethics, Karlsruhe (Germany)

"L'homme n'est ni ange ni bête, et le malheur veut que qui veut faire l'ange fait la bête."
B. Pascal: Pensées (Paris 1977, 572)

Introduction

We live in societies whose political, legal, military, cultural and economic systems are based on digital communication and information networks or in societies that are making major efforts to bridge the so-called digital divide. Maybe this is one reason why hermeneutics, the philosophic theory dealing with issues of interpretation and communication, has apparently lost the academic interest it had in the 19th century as methodology of the humanities as well as understanding human existence in the 20th century. Santiago Zabala, editor of a recent book in honor of the Italian philosopher Gianni Vattimo, quotes Hans-Georg Gadamer, the founding father of philosophic hermeneutics, as follows:

> Vattimo has specifically called hermeneutics a koiné: the common language in which philosophical thought after Heidegger and Wittgenstein, after Quine, Derrida and Ricoeur, has spread everywhere; virtually a universal philosophical language. (Zabala 2007, p. 3)

In his book The End of Modernity Vattimo remarks that computer science makes the difference between modernity and post-modernity (Vattimo 1985, p. 22).

Hermeneutics faces the challenge arising from digital technology becoming what I call digital hermeneutics.[1] Every revolutionary transformation in philosophy that leads to the creation of a new type of rationality arises usually from an outstanding scientific or technological breakthrough (Bosteels, 2006, p. 116). This is the case of today's global and interactive digital network, the Internet. The Internet's challenge for hermeneutics concerns primarily its social relevance for the creation, communication and interpretation of knowledge. This challenge implies a questioning of the pseudo-critical rejection of hermeneutics with regard to technology in general and to digital technology in particular.

ICT is an opportunity for the subjects of the 21st century to transform themselves and their relations with nature (including their own) overcoming strong metaphysical concepts, such as identity or autonomy, that were leading for the self-understanding of individuals and societies for centuries. This does not mean that such concepts could or should be let aside, but they can be reinterpreted and implemented not only culturally but also physically as the present debate on nanotechnology, ICT implants in the human body and synthetic biology shows.

On Constructing Human Identities

Who are we in the digital age? What does it mean for humanity to become transformed and/or hybridized by and through ICT? What are the epistemological, ontological and ethical consequences? In which way does this hybridization affect the interplay with other non-human living beings? These questions go far beyond the horizon of hermeneutics as a theory of text interpretation as well as of philosophic hermeneutics dealing with the question about human existence but ignoring the pervading impact of ICT.

In a digitally globalized world interactive communication processes are a key aspect leading to a transformation of individual and group identities. Hermeneutics faces not just a challenge at the level of the processes of understanding and construction of meaning through ICT but finds itself within societies that see this transformation as something obvious, and give themselves a name that has become a slogan namely information society. But ICT is in fact nothing alien to hermeneutics as far as it understands itself as a questioning of what is apparently obvious.

On Constructing Human Identities

While in the last century mass media gave the impression that they were a kind of meta-observer that would guarantee an objective view of all social systems, such vision has become problematic.

This is an important lesson brought about by the Internet as an interactive technology that transforms all receivers of

[1] The story begins, to my knowledge, with the discussions dealing with artificial intelligence (AI) in the 1970s and particularly with Hubert Dreyfus' book *What Computers Can't Do: A Critique of Artificial Reason* where he pointed to the importance of the context of everyday practices in which we are embedded before we start with any kind of knowledge objectivations and their symbolic manipulations in AI systems (Dreyfus, 1972 followed by 1992).

mass media messages into potential messengers beyond the one-to-one technology of the telephone.

The rise of the Internet as an apparently autonomous sphere shows the historical dimension of this cultural invention that spread over the globe becoming soon not something independent of the real life of the people but the very heart of our political, economic and cultural life.

As the Internet and particularly the World Wide Web became a social interactive information and communication technology in the mid-1990s the relevance of its challenge to hermeneutics became even more obvious. In a recent study devoted to Vattimo's "aesthetic pacifism" the Austrian philosopher Wolfgang Sützl remarks that Heidegger worked with a concept of modern technology opposed to modern communication technology that is characterized by small and networked artefacts (Heidegger 1967).

The leading modern pre-understanding of the engine as a metaphor for the process of social construction is being substituted by the one of the network understood as technology and as a medium of communication. Vilém Flusser was sceptical about dialogical forms of human interaction in view of the overwhelming power of mass media and their hierarchic structures (Flusser, 1996). He did not foresee the impact of the Internet that was in its infancy in 1991 when he died.

In a digitally globalized world with societies based on digital networks without a fixed meta-system to which they can refer in their search for truth criteria or ethical and political legitimization questions concerning polarization, misunderstandings, conflicts, oppositions, conjunctions, ambitions, interests and illusions with regard to the processes of understanding at a local and global level become a key aspect particularly considering this from the perspective of the accelerated technological innovation that started with the Internet at the end of the last century and is expanding now on the basis of mobile communication technologies.

The mobile phone challenges changes our conceptions of freedom and space mobility, of independence and vulnerability, of nearness and distance, of public and private, of being busy or being available, of production and consumption, of masculine and feminine. In other words, the mobile phone is an eminently existential device.

On Constructing Human Bodies with ICT

ICT is becoming more and more part of bodily experiences. Computers and they have amplified the extension of language to everyday language in a global scale as in the case of the Internet. The view of computers as something "other" is disappearing, i.e., they are less and less "some-thing" or "other-than-us" and permeate the world in which we – or, more precisely: some of us – live.

Information technology is part of the everyday life of millions of people. Who are we in the digital age? We are "bodies in technologies" (Ihde, 2002, p. 138) no less than technologies in bodies.

If it is true that we change technology then it is also true that technology transforms us. This happens, indeed, at the very bottom of our bodily experience. Ihde writes:

> We are our bodies – but in that very basic notion one also discovers that our bodies have an amazing plasticity and polymorphism that is often brought out precisely in our relations with technologies. We are bodies in technologies. (Ihde, 2002, p. 138)

This is particularly true in the case of the Internet. We are (not just) our brains and thoughts. But it happens that the ways we perceive reality and the thoughts we develop are shaped hermeneutically by our digital technologies and *vice versa*, digital technologies have to adapt to the ways we perceive and interpret reality, otherwise they will be useless and, in the worst case, dangerous. The Internet has brought up changes in our spatio-temporal social experience that were difficult to imagine some decades ago. It would be naïve to speak about this technology just as a tool without taking seriously its impact at the levels of our being-in-the-world. From this perspective digital hermeneutics is in line with Ihde's project of "expanding hermeneutics" (Ihde, 1998) particularly with "material hermeneutics" in contrast to traditional text-focused hermeneutics (Ihde, 2005) as far as the digital text is different from its mate, the printed one, one main difference being that it allows to perform actions in the world including the actions of interpreting material (and visual) phenomena. As Ihde rightly stresses, it would be a "designer fallacy" to believe that as in the case of the author's intentions with regard to the meaning of his text, it is the designer, as an isolated individual who has the control over the meaning of the object without taking into account the inter-relations with the materials being worked with, the uses and users, including their complex and multistable cultural contexts (Ihde 2008; on Ihde see Selinger, 2006).

The question whether ICT takes us away from our bodies or whether it allows us a different interaction and interaction with them can be seen as another form of nihilism but of a different kind than the Platonic/Christian one Nietzsche was fighting against. It could be that there is a new kind of affirmation of the body because we are able to better understand what is going on with it even at the nano level on the basis of digital technology. This new kind of nihilism is related to the fact that our capacity to manipulate digitally our bodies does not provide us with the ethical thinking necessary to manage this capacity to transform ourselves, which also means the very Nietzschean idea of playing with nature not "going back to it" following Rousseau (Nietzsche, 1999, 150). The experience of our groundless existence does not arise out of this or of any other technology but is something that characterizes human life as such.

Being human is an experiment.

According to the theologian Karl Rahner we are our own designers: “homo faber sui ipsius,” Facing the moralist who says that humans should not do everything they can, and the sceptic who does not trust that we will freely give up what we can, Rahner points to the ethical limit of “what does not work” under the very factual worldly conditions (Rahner 1966, p. 59) that would eventually mean our self-annihilation.

On Constructing Non-Human Identities

Genetic biology in conjunction with ICT aims at the artificial transformation of living beings at the molecular level.

EGE Opinion on Ethics of Synthetic Biology (Nov. 19, 2009)

What is synthetic biology?

> This research sector is heterogeneous and results from the convergence of different technological and scientific tools (from information technology to chemistry, engineering, biology, mathematics and computer modelling). Synthetic biology has two main goals:
>
> 1. to be a tool to improve understanding of biological systems, their complexity and emergent properties that derive from the interaction of complex pathways and
> 2. to use the organisms as factories to obtain products which may have a direct, clear and immediate use (pharmaceuticals, bio-fuels, raw materials and biomedical tools (e.g. vaccines), or new bio-defence agents).
>
> This distinction diversifies not only the potential uses of synthetic biology but also the goals on which current research activities are being developed across the world by private or public research bodies. (EGE p. 10)
>
> EGE working definition:
>
> 1. The design of minimal cells/organisms (including minimal genomes);
> 2. The identification and use of biological ‘parts’ (toolkit);
> 3. The construction of totally or partially artificial biological systems” (EGE, p. 16)
>
> Because of the intentional nature of manufacturing Synthetic biology products, modelling is a key factor allowing synthetic biologists to predict how the functions of biological systems will develop, for example how biological molecules bind substrates and catalyses reactions, how DNA encodes the information needed to specify the cell and how multi-component integrated systems behave. (EGE p. 23)
>
> The debate on synthetic biology addresses issues concerning or related to the ethical legitimacy of manufacturing living organisms. Some have advocated the ethical legitimacy of fabricating life while critics have expressed serious concerns about the radical nature of this intervention. (EGE p. 60)
>
> The concept of *life* has different meanings according to the context in which it is used and careful thought must be given to the terminology used to discuss ethical aspects of SB and its products, for instance, ‘artificial cells,’ or ‘living machines’ (EGE p. 60)
>
> The distinction between life in a biological sense and its use in a social context is particularly relevant. Some languages, such as Greek, have two words for this distinction, namely *zoe* and *bios*. *Zoe* applies to life processes common to all living beings, while *bios* refers to human life in its social and cultural dimension. This distinction is echoed today in the two semantic perspectives we can address human life: firstly, as bodies-as-objects (having a body that is linked to all living beings), and secondly, as embodied beings (being a body, linked to the individual and irreducible experience of a self)
>
> In the light of this, some bioethicists have advocated that from an ethical point of view, the human body should not be reduced to the concept of life proper to biosciences and biotechnology since it is also an expression of our social and cultural life deserving particular care and respect, which are at the core of the concept of human dignity. Some authors give *zoe* primacy over *bios.*
>
> But this conceptual distinction does not necessarily advocate a hierarchy. From an ethical point of view, it is crucial to see that morality (accountability and responsibility) is connected to humans’ specific capacity decide upon the course of their actions.
>
> The production and/or modification of simple living organisms and their potential use to fabricate more complex ones raises the questions as to how far we want to assign a mere instrumental value of such organisms and our relation to the biosphere itself. In this regard, the ethics of synthetic biology, addressed

within the framework of ecological ethics, raises questions of uncertainty, potentiality, and complexity." (EGE p. 61-62)

Conclusion

The task of hermeneutics in the digital age is twofold, namely to think the digital and at the same time to be addressed by it. The first task leads to the question about in which way the digital code has an impact on all kind of processes, particular on societal ones. In this regard, digital hermeneutics is at the core of information ethics understood as the ethical reflection on rules of behaviour underlying the global digital network including its interaction with other social systems as well as with natural processes.

The second task refers to the challenge of the digital with regard to the self-interpretation of human beings in all their existential dimensions, particularly on their bodies, their autonomy, their way of conceiving and living in time and space, their moods and understanding of the world, the building of social structures, their understanding of history, their imagination, their conception of science, their religious beliefs.

Ethics deals mainly with one question: who am I? This question is not to be understood as asked by an isolated individual but as a basic human question that is stated implicitly or explicitly in practical life by every human being no less than by groups, states and today in a global dimension: who are we as humankind? This question is anything but academic. It is a question of survival.

Hermeneutics in the digital age must become aware of this situation in order to make explicit the different political, legal and cultural norms and identities, the way they are affected by ICT and the consequences for the construction of human identities as well as for the interaction between nature and society.

Following Foucault, ethics can be understood as the questioning of morality (Foucault, 1983). It works as a catalyst of social processes weakening the dogmatism of morality and law without just striving towards their replacement through another moral code. It is an open or free space that allows a permanent critique of all kind of blocking processes within and beyond the digital sphere.

If this is the case, in different ways and intensities, ICT become a real contribution to humanity as well as to its interaction with non-human spheres. It could weaken the metaphysic ambitions of (Western) *logos* by making it more flexible with regard to the global cultural interplay in which we look for reasons for our preferences in dialogue with different beliefs and desires of other human beings. A future world must be open to an open horizon of understanding in which the "principle of charity" plays a major role avoiding that reasons become dogmatic beliefs to be eventually imposed others by force. The digital network could become the place where such translations between different languages take place in a global scale in this new century. This means to allow the other to articulate herself in the network, looking for nodes of relations, becoming a hermeneutic subject of the digital age. This is the reason for the relevance of intercultural information-

In his "Anthropology from a pragmatic point of view" Kant makes a difference between "physiological" anthropology dealing "what nature makes out of the human being" and "pragmatic" anthropology that concerns "what the human being, as a freely acting being makes, or can or should make of itself." As different from empirical psychology that aims at explaining phenomena, anthropology's goal is knowledge of the world based on reflective judgement that looks for what useful for the world. Its goal is judgement not explanation. In Kantian terms, pragmatic anthropology is not just about understanding ("verstehen") but about playing with ("mitspielen"). Due to the fact that we are not "pure like angels" ("engelrein"), it is not possible to foresee how we will deal with each other in order to become morally better as a whole. In any case, writes Kant at the end of his "Anthropology", in order to achieve this end it is not enough that individual behave morally. It is necessary that they are connected as a system, i.e. "cosmopolitically" as a species.

The question is then how ICT makes a difference in this "playing with" human and non-human identities.

DNA barcoding and personal genomics

Giuseppe Novelli[1], Ilenia Pietrangeli[1]
[1] Università di Roma Tor Vergata (Italy)

For over a century, different means have been used to establish the uniqueness of a person's identity by reference to personal data (name, date of birth, nationality, gender and fingerprints) properly registered by governments of various (but not all) countries. It is claimed that the security of each country is inextricably linked to the possibility of identifying and recognising their own citizens. In the last two decades, the nature and sequencing of human DNA makes it possible to identify people on the basis of a genetic code.. The techniques and procedures currently in use are globally standardised and routinely used by government agencies (identification of missing persons, assignment of biological traces to specific people, recognition of remains in mass disasters, etc...). The evolution of genomics and the increased need for security now make it feasible and desirable in many cases to include such information, together with the master data type currently used on a map and ID.

The complete human DNA sequence and the introduction of new methods in DNA sequencing shows that each person is 99.9% genetically identical to another. Thus the ' unique' characteristics of each individual are discoverable and due to the remaining 0.1% of hereditary material that forms the variability. Inter-individual variability is largely due to small sequence variations consisting of substitutions of single nucleotides that make up our DNA. These are called called SNPs (single nucleotide polymorphisms), hypervariable polymorphic sequences repeated in tandem call strs (Short Tandem Repeats), or copy number variation (CNVs). Overall, each individual has about 10 million of those differences . The analysis of a small portion of this huge amount of data allows for personal identification. Currently, the techniques of personal identification based on analysis of 16 loci that STRS constitute an international standard (CODIS). However, most countries are working to develop an identification system based also on SNPs preferable to STRS for three main features:

- Possibility of increased automation in generating, analysis and data management;
- Greater sensitivity over conventional systems (in practice it would be possible to obtain the genetic profile of a person (only from established loci) from smaller amounts of DNA or in poorer samples condition);
- Increased opportunities for digitisation and international comparisons with electronic systems.

Since 2002, the application of that system was approved by the Chinese government and, recently, by the British and Dutch. Of particular relevance is the possibility, with the techniques currently in use, to extract the DNA of every person from samples taken non-invasively (eg saliva). According to calculations, the definition of the DNA sequence of only 30-80 SNPs (compared to 10 million held by each of us) statistically independent is able to define a single person and, where there are relatively rare SNPs, the number required would be even less.

The increasing availability of personal genomic tests has led to discussions about the validity and utility of such tests and the balance of benefits and harms.

The future of the internet

Session 1: The Internet of X

The social future of the “Internet of X”

Jonathan Cave[1]
[1] Rand Corporation, (United Kingdom)

[**Missing**: abstract or summary]

Session 1: The Internet of X

The approach of the OASIS project

Karel Van Isacker[1]
[1] Access for All.eu - Marie Curie Association (Bulgaria)

[**Missing**: abstract or summary]

Session 1: The Internet of X

Ongoing changes in internet protocols

Rudy Vansnick[1]
[1] Board EURALO (ALAC – ICANN)

[**Missing**: abstract or summary]

Robotics and convergence of the real and the virtual

Session 1: Robotics in Daily Life

Artificial companions? Empathy and vulnerability mirroring in human-robot relations

Mark Coeckelbergh[1]
[1] University of Twente (The Netherlands)

Can robots become companions, and if so, on what conditions and which are the ethical issues that might arise in human-robot companionship relations? In this paper, I argue that the future of robots as companions depends (among other things) on the robot's capacity to be a recipient of human empathy and that a necessary condition for this to happen is that the robot mirrors our own, human vulnerabilities. Moreover, I show that we might have the intuition that this raises the ethical issue of deception but, given contemporary technological developments, it is hard to justify the underlying assumption that 'machine', artificial vulnerability, is less real (and less significant or valuable) than biological, 'natural' vulnerability.

The idea of humans engaging in companionship relations with robots is not science fiction. Whereas companionship with humanoid robots may be 'mere speculation' or at least something that belongs to the distant future (the development of humanoid robots is still in its infancy), it is likely that some of us will live with pet robots as companions in the near future. It is *possible* since there are already people who 'keep' robots in their homes, and there have been experiments with robot pets in care for the elderly (see for instance the baby seal robot Paro – see also other literature). It is *likely* that this increases in the near-future, since there are already many people who live with biological pets and some of them might want to try an artificial pet or even prefer it (for instance because it can be turned off when one goes on holiday).

But when is a robot a good companion? On what does companionship depend? We can think of many conditions, such as (the capability for) a certain level of interaction and communication or human-friendly and safe behaviour. In this paper, I argue that one of the necessary conditions for companionship concerns empathy (as indicated above, it is not a sufficient condition). But who has a capacity for empathy? In human relations, empathy can go two ways. Some might say that in the future humanoid robots will be capable of empathy. I doubt that his will be possible. In any case, to require robot empathy would be an 'unfair' requirement. Young children some adults with a mental disorder do not have much empathy but we still treat them as companions, not as 'mere things'. Moreover, although pets like dogs or cats might be capable of some empathy, we do not demand it as a condition for companionship: it suffices that we humans exercise our empathy towards them. Companionship relations, in contrast perhaps to friendship and love relations, need not be entirely symmetrical in this sense. Therefore, I propose that we agree on the minimal requirement that robots can be *recipients* of human empathy as a necessary condition for human-robot companionship.

What kind of empathy is this? Let me distinguish between two kinds of mental operations which may both be called 'empathy'. The first is a cognitive matter. The question is: What is in the mind of the other? This kind of empathy is less applicable to relations with robots, since (1) generally we do not suppose that they have a mind and (2) *if* they had one how could we know it? How could we know – to employ Nagel's phrase – *what it is like to be a* robot? There are limits to our (cognitive) imagination. (The second scepticism also casts doubt on this kind of empathy in human-human relations: how can we know what it is to like another person? And even the first scepticism applies to human-human relations; this is the famous problem of 'other minds'.) Thus, if we define empathy in a way that renders it a cognitive, epistemological, or mind problem, robots would not be able to be recipients of human empathy. However, there is also a second way of defining empathy: as an imaginative-emotional operation. We can always try to *imagine* the mind of other humans or of robots and here this is not a matter of belief or knowledge concerning mental states but of feeling: we imagine how the other (human or robot) *feels*. If we define empathy in terms of empathy-as-feeling instead of empathy-as-cognition then it becomes possible that robots function as recipients of human empathy. Human 'fellow feeling' (see the moral sentiment tradition of Hume and Smith) imagines robots, animals, and humans as 'fellows' rather than as alien minds that need to be known. The 'other' becomes less 'other'; in the centre of this mental operation is what is shared rather than what different.

But how does this work? What is the 'mechanism' that creates this fellow feeling? On what does it depend? I argue that

a necessary condition for this to happen is that the robot (or, for that matter, the animal or the human) mirrors our own, human vulnerability. Our embodied existence renders us vulnerable beings. Pet animals mirror that vulnerability: they have their weaknesses, their problems, their characters, their little sufferings, their needs, etc. This is a necessary condition for us to accept them as companions. They are the mirror in which we understand that we (humans) are vulnerable, and it is because we see their (animal) vulnerability as related to our own that we come to see them as fellows. The etymology of 'companion' links the word to 'eating the same bread': it refers to shared needs (in addition to shared practices of fulfilling these needs). To the extent that robots can function as 'vulnerability mirrors' they fulfil at least one of the conditions for companionship. *If* they meet this criterion, they can be considered as 'fellows' rather than 'mere things'. If we apply this criterion, many robots will be excluded, of course, but it is likely that many pet robots that are used today will meet the criterion: they are regarded by the humans who interact with them as fellows and as recipients of empathy – partly and necessarily due to the 'vulnerability mirror' mechanism of empathy-as-feeling.

However, here we might object that there is an ethical problem with this kind of empathic relation: since robot pets *imitate* their biological cousins, they seem to *deceive* humans. The human vulnerability might be real, but *they* do not really mirror that vulnerability since they are not living beings. The mirror lies and lies are morally unacceptable. Now there are several possible responses to this argument. First, it is controversial whether or not lying is always morally unacceptable. Second, it is not obvious that there is 'deception' here. Deception is about truth, and truth is a criterion for knowledge. But the kind of empathy at work here is a matter of feeling and it is not obvious that feelings can be 'true' or not; at the very least one would need to specify a criterion outside empathic process that would allow to evaluate the 'truth' of the feeling. Third, the external criterion used in this argument seems to be a reality criterion: it is assumed that only biological, 'natural' vulnerability is real or at least more real than its artificial counterpart. Perhaps there is also the related assumption that biological vulnerability is more valuable or that biological life in general is more valuable. But how can we justify these assumptions? First, there is no doubt that machines are also vulnerable. Whereas cyberspace and some other ICT *aim* at invulnerability (and perhaps immortality), they depend on software and hardware that are very vulnerable indeed. And here there are at least metaphorical parallels to biological vulnerability. Software risks can be described in epidemiological terms (viruses that spread etc.) and hardware is as material as the human body. Why do we have the intuition that biological 'hardware' is more valuable and that its vulnerability is more 'real'? If these technological vulnerabilities are so significant for the way we work and the way we live, how 'unreal' or unimportant are they? Second, the very border between the 'natural' and the 'artificial' is continuously called into question by technological developments in medicine and biology (see for example synthetic biology) that make us 'cyborgs' to some extent (and to a large extent if it depends on some defenders of human enhancement) and that make 'dead' material more 'living' (see also alchemy and the myth of the Golem). Thus, in the future our intuitions concerning the border between 'life' and 'death' and the importance of that distinction might change.

I conclude that the future of companionship robots depends on the development of empathy for robots, in particular on empathy-as-feeling which is conditional on vulnerability mirroring. I have shown that the deception objection to this kind of empathy is intuitively appealing but is hard to justify given contemporary developments in ICT and converging technologies that show how *real* technological vulnerabilities can be (and how important they are for our lives) and that suggest that our natural/artificial distinction might be more 'artificial' than we think it is. Therefore, if we want to hold on to our intuition, we need a (better) justification that answers these objections. In the meantime, some of us will treat their pet robots as companions and grant them their empathy – without worrying about the truth of their (human) feelings or the artificial nature of their favourite vulnerability mirror.

The future of human machine interaction – integrated robots and smart homes

Atta Badii[1], Daniel Thiemert[1]
[1] University of Reading, Intelligent Media Systems & Services Research Centre (United Kingdom)

The demographics in Europe present various challenges for society. The number of elderly people is increasing while the lower birth rates have resulted in the number of younger age groups decreasing. This has strong implications for the social and health care systems which need to remain responsive to future challenges. The elderly as well as their informal carer are at risk of social exclusion.

The answer is increasingly sought in technology-enabled care provision systems. One facet of technology, that is thought to offer some attractive features, is care provision assisted by the integrated robot and smart home solution, as currently being researched and developed by the CompanionAble Project (FP7 grant agreement nr. 216487).

The distinguishing advantages of the CompanionAble Framework Architecture arise from the objective of graceful, scalable and cost-effective integration. Thus CompanionAble addresses the issues of social inclusion and homecare of persons suffering from chronic cognitive disabilities which are prevalent amongst the older age group within the European population.

The objective of the CompanionAble project is to provide a new Ambient Assisted Living (AAL) solution through a combination of a mobile service robot as a companion that is seamlessly integrated with a smart home environment. The combined system will provide support to the Care-Recipient (CR) in their Activities of the Daily Living (ADL), in particular for persons with Mild Cognitive Impairment (MCI). Through the situated evaluation of the CompanionAble prototypes, we will study the interaction between not only a mobile robot as an assistive device, but also computing devices in general, including sensors, actuators, displays and the human user.

The project will inevitably address issues of interest for the wider research community in the field of assistive technology and human machine interaction.

i) Social aspects such as inclusion and activity are of major importance when developing assistive devices for the elderly. How can technology be facilitated not only to assist the user in his daily activities and lifestyle, but also to counteract social exclusion, i.e. by establishing connections to remote family members, social networks, etc.
ii) A comprehensive and integrative methodology for needs assessment and usability evaluation of ambient assistive technologies is essential. This entails a user-centric, interpretivist approach which endeavours to deeply understand the user's statements in the course of requirements elicitation, and, to identify, prioritise and best meet the user's most deeply-valued needs.
iii) The ability for assistive devices, in fact for any device interacting with a human, to show advanced and intuitive interfaciality, e.g. advanced dialogue management, and natural interactions such as vision and speech, etc. will be crucial for its success and its adoption in the wider market and society.
iv) Business models need to be developed that meet the requirements of the market and guarantee sustainability of the provided solution. In the case of assistive robots this could mean a rent-a-robot scheme, a short-term lease or a long term provision by insurance companies to save resources in home care provision.

This talk will outline the multi-faceted challenges that future assistive and intimate systems will face, from development stage to adoption and wider deployment in the European and global market place.

Implants, chips and transhumanism

Fernand Doridot[1]
[1] ICAM de Lille (Engineering School) (France)

As a result of technical progress, as much as that of the search of interesting profits by some specialized companies, the use of a wide range of ICT implants has grown in recent years. Several kinds of devices already exist, with medical, identification, inspection or localization uses. Among them the example of the VeriChip™ chip is probably the best known and the most widely publicized. Used as payment in some trendy bars, as a receptacle for medical records — in particular in the United States where it obtained approval from the Food and Drug Administration, or as a means of identification for certain administrations and companies, it is the subject of an intensive lobbying by its developers, who do not hesitate to suggest controversial uses such as mandatory implantation of homeless people or migrant workers.

In the tradition of early experimenters such as the British scientist Kevin Warwick, some dream to improve human capacities by the use of these kinds of implants. Against them, the development of chips and implants has also led to the emergence of a broad social opposition, with various trends from religious conservatism to technophobe libertarianism. The multiple stakes of the topic of ICT implants have now and already resulted in the producing of several reports — such as that produced in 2005 by the European Group on Ethics in Science and New Technologies — and several legal decisions — such as the laws passed by several U.S. states, which prohibit employers from making of a chip implantation a prerequisite for getting a job.

We propose in this paper to provide an analysis of the philosophical and ethical situation surrounding chips and implants, by addressing several areas:

1. A reconstitution, in the mode of historical and strategic analysis, of the social force field surrounding the issue of chips and implants, between zealous proponents and irreducible opponents.
2. An analysis of the tacit philosophies which motivate the various positions, and in particular, by exploiting the example of Kevin Warwick, an analysis of the transhumanist ideology that forms the backdrop to many enthusiastic pronouncements on the issue of corporal implants.
3. An exploration of the fundamental antinomies which, we believe, determine the possible approaches of the issue of corporal implants. We will try to show that any position or policy decision on the issue of implants requires and reflects an option on some questions such as: Does one think in terms of a "body-sanctuary" or of a "body-resource"? Does one want to cure or to improve? Does one consider the question from the angle of freeing or from that of alienation? Does one consider the question in terms of deterioration or in terms of revelation of the identity? In terms of possession of a body or of possession of data? etc. We will explore the implications of each of these antinomies and we will make explicit some of their paradoxes.
4. Then, we will try to explore how some distinctions in contemporary philosophy of technology—e.g. That between structure and function of the technical devices—can be applied to the case of corporal implants, and we will examine whether nanotechnology in itself is likely to upset the ethical issues of implants in a radically new way.

Finally, we will try to identify some paths for a successful governance of these new technical devices.

Brain-computer interfaces: the challenges ahead

Bert Gordijn[1]
[1] Dublin City University (Ireland)

Brain-computer interfaces (BCIs) intercept neural signals in the brain and establish a direct communication pathway with a computer. These signals can be registered either by electrodes on the scalp, the cortical surface, or by a brain implant. An important objective of BCI research is nonmuscular communication with and control of devices. This might evidently benefit people who are paralyzed. Consequently, BCIs are currently being studied and tested in humans. In 1998, Kennedy and Bakay were the first to install a brain implant in a human that enabled a patient with a 'locked-in syndrome' to control a computer cursor. Recently, another patient, paralyzed from the neck down, became the first person to control an artificial hand using an invasive BCI. In addition, there is considerable interest in developing BCIs for the purpose of enhancing human performance. In the short run, the bulk of the BCIs will likely continue to focus on curing disease and reinstating lost functions. In the medium or long term, however, the focus of BCIs might slowly but surely shift from therapy towards enhancement. Although BCIs have a huge potential to relief suffering, their further development and widespread use are likely to trigger difficult ethical questions as well. The ethical analysis in this paper focuses on the ethical challenges that might ensue from this development.

Interaction metaphors for the exploration of ubiquitous environments

René Reiners[1], Marc Jentsch[1], Christian Prause[1]
[1] Fraunhofer FIT (Germany)

In ubiquitous environments computers disappear and users are supported to concentrate on the tasks they actually intend to perform without having to focus on how the required devices are to be operated and connected. In our point of view, this vision on the one hand further encourages the miniaturization of devices and new design concepts. On the other hand, however, it also implies some disadvantages. In ubiquitous environments it is not really clear to the user which objects possess special capabilities.

They also do not easily reveal their spectrum of functionalities. This work discusses three different approaches to interaction metaphors for smart environments based on scenarios. Currently, this happens on a conceptual level by presenting first scenarios. Prototypes are under construction so that first evaluations will follow during the year.

1. INTERACTION METAPHORS

In the vision of ubiquitous computing created by Mark Weiser, the standard metaphors of mouse and keyboard interaction should be overcome and the computer as interaction device itself disappears in an augmented environment [4]. Users in ubiquitous environments should be able to concentrate on their tasks at hand and not have to care about the devices' usage.

In order to connect a physical device to a virtual pendant and enabling the user to interact with it, a mediating instance is needed. In the following, three different interaction metaphors are described. Scenarios are intended to support a vision of regarded approaches and to provide first insights about situations in which specific metaphors are better suited than others. The visualization concepts are also addressed and will be exploited in much more detail in future work.

2. UBILENS

The interaction metaphor resembles classical point-and-click adventures in which the player has to explore the current screen with his mouse cursor. Objects of interest are highlighted and actions can be started by selecting them. The approach presented in this work lets the user explore a real environment with a mobile device. As a starting point for this interaction metaphor, a mobile device like a PDA or mobile phone is used. The camera shown on the device's screen is used to provide additional information on recognized objects by displaying it as video overlays. The selection of an object is performed by centering it and holding the image still. Depending on the object's functionalities, a contextualized menu is generated. Figure 2 shows an example screen of the intended application.

3. UBITORCH

For this interaction metaphor we assume to have a mobile phone equipped with an integrated projector. A first model already hit the market and it is expected that more will follow within the next years [1].

First, a media file is selected on the mobile phone. The media has some requirements which can be matched by devices to a certain degree. The user now points his mobile phone through the environment. When there is a device in

Figure 1: A possible example screen of the intended UbiLens application showing the ubiquitous functions of a coffee machine.

the line of sight, the integrated projector highlights the particular device by surrounding its borders with light. It displays the percentage of how well it supports the selected media. This information is also available by the color of highlighting. Green means a complete match, yellow means an average one and red means that the device cannot handle the media at all. Another approach is to visualize the matching with symbols that show speakers or cameras in order to illustrate the current device's capabilities to play the media. The concept is illustrated in figure 3. In order to play the media on the device the current beam selects, the user selects a menu item from the mobile device's touch screen.

Also non-technical devices can be taken into account. White spaces on the wall, e.g., can be used to project the video upon while the audio track of the video is played via the mobile phone's speakers. In this case, the matching rate would be lower than the optimum or, respectively, a camera icon would be projected on the wall and a speaker symbol together with an arrow pointing towards the a mobile phone icon. So, the audio and video track of the media can be played but not with the optimal quality.

4. UBIGRAB

The starting point for the interaction based on RFID tags is derived from the MICA project1. In this project the focus lay on supporting warehouse workers during their picking tasks. A special cart was designed equipped with RFID readers to different sections so that all the items that were collected and put inside the cart could be identified. Each object was also equipped with an RFID tag (cf. [2]). MICA recognizes the worker's actions without explicit interaction and is therefore capable of supporting him with the information she currently needs.

An extension to this scenario is presented by Voong [3]. There, a glove is equipped with RFID readers so that objects are directly identified at pickup time. Wrong picks are already identified before the item was put inside the cart. The glove is shown in figure 4.

This approach is currently being extended to find different situations in which it could be applied. One of the main advantages of that technology is that many objects can be tagged. The tag can even be hidden inside an object. Although there are still technical problems on metal surfaces or objects surrounded by water, the RFID technology can be used for recognition tasks and the provision of information via other devices. It is mature and easy to use in many situations.

Figure 2: A conceptual drawing of the intended UbiTorch approach. The matching rate of the current media to a device is directly projected onto the device.

Figure 3: The RFID glove prototype. The reader is hidden in the wrist part.

5. REFERENCES

[1] A. Hang, E. Rukzio, and A. Greaves. Projector phone: a study of using mobile phones with integrated projector for interaction with maps. In Proceedings of the 10th international conference on Human computer interaction with mobile devices and services, pages 207–216. ACM New York, NY, USA, 2008.

[2] A. Schneider, A. Lorenz, A. Zimmermann, and M. Eisenhauer. Multimodal Interaction in Context-Adaptive Systems. In Proceedings of the Second Workshop on Context Awareness for Proactive Systems, CAPS 2006 Kassel, June 12-13, 2006, page 101. kassel university press GmbH, 2006.

[3] N. K. Voong. Rfid-handschuh zur kommissionierung. Master Thesis at Fraunhofer FIT, 2008.

[4] M. Weiser. The computer for the 21st century. Scientific American, 265:94–104, 1991.

Learning from convergent technologies

Session 1: Learning from convergent technologies

A tentative methodology for responsible planning of nano-research

Lieve Goorden[1], Marian Deblonde[1]
[1] University of Antwerp (Belgium)

New and emergent nanotechnologies are surrounded with many uncertainties. The complexities of many new nanotech products in the field of 'ambient intelligence' and biomedical applications, introduce new complexities both at the technoscientific and the societal level. Expanding human knowledge seems to add to uncertainty by allowing for new technological applications and products that induce a) changes in ecological systems of which the impacts for human health and for the ecological systems themselves are not well known are even not known at all, and b) changes at the cultural, social and economic level that are at odds with current ideas of the good life among various groups. Within scientific communities awareness is growing that researchers and research managers constantly have to make strategic choices within contexts of uncertainty and complexity.

Nanotechnologies for tomorrow's society – NanoSoc (www.nanosoc.be) is a Flemish research project, funded by IWT and executed by a research consortium that consists of nanoscientists (IMEC, University of Antwerp) and social scientists (University of Antwerp, KU-Leuven), working together in close cooperation. The researchers develop and apply—as a final stage in a series of interactive exercises with nanoscientists and civil society—a methodology for strategic planning of nanoresearch activities at the level of research institutions. In the proposed paper the author will present 1) the points of departure which influenced the design of the methodology, 2) the methodology itself, and 3) first experiences with the use of this methodology in the institutions of the consortium partners IMEC (Interuniversity Research Centre for Micro- and nano-Electronics, Leuven) and EMAT (Electron Microscopy for Materials Science, University of Antwerp).

We consider the development of a methodology for strategic planning of nanoresearch activities as an experiment in integrated roadmapping:

1. The methodology is based on an approach of social appraisal which precedes a process of social choice of technology (Stirling, 2005). Activities of social appraisal in the governance of technology are epistemic processes of learning and communication (Webler et al, 1995; Wynne, 1995). Discourses that mediate this learning will shape the way in which the various social actors come to understand and interpret the available 'alternatives'. The roadmap exercise as an exercise in social appraisal, is ment to be oriented towards the 'opening up' of technological choice. This means that the 'outputs' of the appraisal exercise are presented in terms of 'plural and conditional' policy advices.
2. The methodology is focusing on the mutual interaction of upstream (what R&D to authorize and fund) and midstream (how to implement R&D) modulation of technological trajectories (Fisher, 2008).
3. The methodology rests on the tradition of participatory technology assessment, especially on distinctive discourses about the participation of stakeholders and citizens in upstream processes of knowledge production (Wilsdon&Willis, 2004).

Lessons from the Genetically Modified Organisms controversy case for ethical issues in ICT and future technologies

Philippe Goujon[1], Catherine Flick[1]
[1] Facultés Universitaires Notre-Dame de la Paix Namur (Belgium)

This paper seeks to develop the lessons that can be drawn, for the ICT field, from the analysis of the precautionary principle and its role in the GMO controversy case study.

What is at stake, at a time of globalisation and the expansion and domination of technology, market forces, and calculating rationality, is the capacity of societies to regulate themselves. The feeling that there is something automatic about the growth of technology and economic and administrative rationalities is all the more widespread since their political origins are masked, reinforcing the impression that the prospect of democratic supervision of social sub-systems is barely credible, if not to say irrational.

Yet the growing desire shown by citizens today to be involved in a certain number of decision-making mechanisms is tangible. This is notably the case with regard to situations perceived as presenting risks: people are unwilling to run risks that they have not been warned about beforehand, that they have not accepted, or that have not been debated in a democratic manner. The questions this raises are bound up with governance and ethical issues, as well as with technological, economic, and financial stakes.

Arguments involving the semantics of risk or danger are today commonplace in modern societies and now dominate discussions of governance. The scale of each risk is virtually global, presents potentially gigantic mortal dangers and, above all, involves much public debate about current assessments of the risks involved. These risks pose huge challenges in the realms of politics and governance. To understand them is essential, all the more so since supervision of the norm is no longer limited to State-type supervision alone. These questions relating to the role of governance in a context that is uncertain and involves risks cannot seriously be addressed without posing the question of normativity and of the links between society, norm, and law.

Today, the State has de facto forfeited its monopoly on social regulation and the production of judicial norms. If one takes as given the functional differentiation of society and the multiplication of sub-systems, each employing its own rationality and each running the risk of closing in on itself, the question arises not only of communication between these subsystems, but of where the legal system stands in relation to them. As G. Teubner sees it, “the law cannot monopolise the epistemological authority pertaining to other forms of knowledge and alone assume full responsibility for all the constructions of reality. . . . It cannot, however, delegate all epistemic authority to the other forms of social discourse,” with the attendant risk of conflicts emerging between these different systems.

Faced with conflicts of this kind, there is a danger that positivism will end up presenting itself as the only genuine form of knowledge. Hence the growing importance of experts and the depoliticisation of civil society. Hence also the force of technocratic ideology, an unacknowledged domination that hides itself behind technological rationality. In this context, expertise becomes the indisputable new source of normativity, and the problems revealed are confined to a scientific perspective alone

For the law to retain a legitimacy, it must participate in the search for a procedure aimed at resolving such conflicts. G. Teubner indicates one path: the solution to conflicts between the judicial system and other systems should be found in a proceduralisation of knowledge. Opening the realm of law to other sub-systems in this way poses problems, however, notably in the relation of law to scientific and technological sub-systems.

Where techno-science is concerned, relations are strained between, on the one hand, the judicial realm and, on the other, sub-systems characterised by their lightning growth and imperialist pretensions—biotechnology, for example. Though law is duty bound to reorganise itself in response to the progress of these sub-systems, this does not mean that it must submit to them.

The example of biotechnology is revealing in this respect. In the controversy surrounding GMOs, it might seem that the law has helped set out answers to the problems at issue by imposing a minimum of caution. Where the tensions between law, science and society are concerned, the precautionary principle would seem to have made a major contribution to the search for an answer to the problem posed by the lightning growth of technological innovations and the conflicts between sub-systems. Nevertheless, it cannot be the definitive solution to the questions raised by the progress of science.

Faced with the problem of regulation and social order in a society characterised by the multiplication of sources of normativity and taking the principle of precaution as a case study we will try to determine the possibility of relativizing instrumental rationality and of determining its political control trying to escape to the traditional expertise source of normativity.

In this paper, which reflects the work we are doing within the EGAIS and ETICA projects, our first step will be to contextualize the issue raised by the condition for an ethical reflexivity. For our second step, drawing lessons from the

precautionary principle, we will use the normative criteria that came out of our analysis of the application of the precautionary principle in the context of the GMO (genetic modified organism) case study in order to evaluate real- orld experiments of risk assessment. Firstly, we define the principles for evaluating these real-world experiments. In a second time we use these principles for drawing lessons from successful and non-successful cases that can guide further institutional design.

We conclude our analysis with an interpretation of the concept of precaution that considers the precaution as a cognitive principle that can open up new possibilities. Here, precaution can be understood as a process of permanent collective inquiry in the face of uncertainty. We will develop the lesson that can be drawn from our analysis for the ICT field, a field where the precautionary principle still needs to find a real place.

Technology, its users and society

Session 1: Identifying new social issues

A framework for identifying emerging ethical issues in future and emerging technologies

Bernd Carsten Stahl[1], Kutoma Wakunuma[1]
[1] De Montfort University (United Kingdom)

The ETICA Project[1]

Discussions on future technologies will to a large extent usually centre on how an already existing technology or technologies can be improved upon and/or on how new and emerging technologies will improve and better lives. Rarely, if at all, is there a discussion on identifying potential ethical issues as future and emerging technologies are being developed or how ethical issues will be tackled as they come to light during the process of their development. The expectation is twofold, either that ethical issues will be dealt with when the technology is already in existence and in full use or that research and development of future technologies will follow some form of ethical guidelines as work commences. For example, when we look at the European Commission's ethical guidelines for undertaking Information and Communication Technology (ICT) research in the Seventh Framework programme (FP7), emphasis is on conduct of ICT research which calls for the researcher to be aware of the dignity, rights and freedoms among other concerns of those that may be involved in the research. The guidelines also call for privacy and informed consent when involving research participants. In addition, the guidelines also touch on the issue of security of personal health data for those whose research centres on health care among others. These are mostly guidelines that researchers should adhere to and check as they embark on their ICT research. However, little is outlined in terms of how researchers and indeed developers of future and emerging technologies can go about identifying ethical issues as they arise when the technologies are being developed beyond fulfilling the initial ethical guideline requirements. Granted, the guidelines warn researchers to be aware of dangers associated with the process of ICT research that may be encountered during research. However, as a way of guarding against the potential dangers, researchers are advised to carry out prior assessment risks and then identify precautionary actions against any potential risk in the research. This implies that the risks should be handled well before the developers embark on developing the technology/technologies.

However, in order for any future and emerging technologies to make a difference, this paper argues that potential ethical pitfalls are bound to surface not only at the planning stages of a future technology but during the process of development as well. As such, rather than just deal with the ethical issues at the start or planning stages of a technology development, developers should be more proactive and identify ethical issues during the process and up to the time the technology is ready for use. This means that a lot more ethical problems that would have been missed at the planning phase of the development of the future technology could potentially come to light during the development process. As a result, this lessens potential ethical problems in the future. In addition, identification of any ethical problems during the development process ensures that technology developers are more sensitive to users needs and therefore develop technologies that users find more suitable. Furthermore, identifying ethical issues during the process of development ensures that developers not only think of meeting the ethical requirements as outlined in a standard ethical guideline but that they become accustomed to being alert to any ethical pitfalls throughout the development stages of future and emerging technologies.

To this end, this paper proposes a discussion on identifying future and emerging technologies and their subsequent ethical issues. The paper is based on the fundamental ideas that are being developed in the ETICA project. It will discuss the merits of identifying potential ethical issues as future and emerging technologies are being developed. It will discuss a potential framework within which arising ethical issues may be identified. By starting this discussion we can ensure that future and emerging technologies will really make the difference when their subsequent ethical issues are proactively identified and dealt with not only during the planning stages but during the development and implementation processes as well.

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (*FP7/2007-2013*) under *grant agreement* n° [230318].

Conditions for a critical perspective on Ambient Intelligence: ethical and social issues

Philippe Goujon[1], Catherine Flick[1]
[1] Facultés Universitaires Notre-Dame de la Paix Namur (Belgium)

The use of Ambient Intelligence (AmI) technology in highly sensitive environments produces specific challenges that are inextricably linked to ethical and societal issues. Proactive AmI systems will make decisions without direct human supervision, placing the technical system in a position of authority. The ethics of interactive computer systems that focuses on how such systems are (or can be) used by human users has been discussed at length, but taking into account the possibilities of these emerging technologies, it becomes urgently necessary to consider the implications of decisions made by or influenced by computers. As explained by L. Venter, M.S. Olivier and J.J. Britz, "the integration of mobile technology, wireless networks, ubiquitous computing and artificial intelligence with thousands of embedded devices such as sensors and actuators may result in networks that can proactively monitor and respond to human behavior without human interaction and with little supervision. Decisions that can influence or alter the environment will be made at faster-than human speeds." Ethics as applied to current interactive computer systems will not be adequate.

What we propose is to review the state-of-the-art with respect to the ethical analysis of ICT developments and in particular of Ambient Intelligence applications. Practically, the main problem consists of a deep lacking of background: the strong push for technology development too often obscures the need for any deep ethical consideration before a technical project is funded, developed and deployed. Some efforts have begun to consider ethics and ICT in the AmI domain that adopt different approaches: analysis from scenarios (e.g. PEACH), or "ethical review" panels (set up after the project has started, e.g. MINAmi[1]) consisting of "ethical experts". This, however, results in the "technical" community being typically separated from the "ethical" community[2].

The reflexive articulation of ethical norms and cultural contexts also raises many problems, the first of which is the set of conditions for reflexivity[3]. This is natural since the researchers and technical developers of AmI systems focus mostly on the technical and economic challenges before them. In focussing this way, they are not usually aware of potential ethical issues, especially when they consider the act of ethical consideration and analysis as an obstacle to the technical and economic development. In short the problem we must first analyse is not so much the determination of a solution to ethical problems as a settling of the conditions for raising ethical questions, and for a new approach authorizing a real reflexivity and allowing the questioning of the integration of ethics in complex technical systems. The obligations of economic constraints, interests concerned the influence of experts, impression of the inescapability of technical projections, social requests, and needs for the consumers makes it increasingly difficult to define the conditions of a critical perspective respecting moral autonomy requirements.

We do not mean that existing criticisms don't allow for a certain reflexivity. However, these criticisms generally show a tendency to restrict ethics to a categorical field by sacrificing the existence and its tension in the name of a flattering pragmatism, being satisfied with ad hoc answers to artificially isolated specific contexts and being conditioned by the reigning instrumental rationality. Consequently, there is a strong need for the inclusion of ethical considerations before, during, and at the end of technical and scientific projects, so that the technology 'incorporates' and tackles the ethical side the entire duration of its conception and implementation.

The risk is that by not analysing the conditions (institutional, rules, cognitive) for the effective integration of those considerations in the context of a technical project, the ethical considerations will be excluded from the technical rationale, and treated as a totally separate domain. The consequence of this separation is a loss of impact, and an undermining of the integral role of ethics in the application of technology. This is quite understandable since the technology can only be limited to the set of its rules (objectivity, and technical rationality which frames its vision and conception).

The same risk also relates to ethical references. To analyse the ethical issues raised by AmI systems one needs to analyse which ethical references are suitable. In general these references are presupposed in all ethical analysis and are not questioned.

However, having done these analyses is not sufficient because the determination of ethical issues doesn't, by itself, lead to their resolution. Most of the time ethical analysis seems to imply that the ethical justification (by itself) leads to ethical resolution as if the reason contains in itself all the conditions required for its application. In the last part of this paper we will question that presupposition and analyse the governance conditions leading to a real account of ethical issues and reflexivity. In particular we will demonstrate the importance of the contextual conditions for the normative constitution of ethical reference and for their application.

The structure of the proposed conference and article is as follows:

The objective of this proposed conference presentation and article is to review the ethical and societal problems

related to AmI technology. To reach that objective, we will first analyze the conditions from a critical perspective. In the second step we will analyse the ethical references used as a possible foundation for the analysis of the AmI ethical issues. In a third step we will specify the ethical issues raised by AmI. In the last part we will determine the governance conditions that could allow the resolution of those ethical issues.

[1] MINami (MIcro-Nano integrated platform for transverse Ambient Intelligence applications, an FP6 project).

[2] For example noted in the Human Report Ethical Audit produced in December 2004 (Editors: Peter Goldie, Sabine A. Döring and WP10 members). http://emotion-research.net/deliverables. Humaine (Human-Machine Interaction Network on Emotions) was an IST FP6 project.

[3] Reflexivity may be defined as the capacity of actors and institutions to revise basic normative orientations in response to the evolution of economic, techno-scientific or political systems and to shortcomings in current modes of regulation. This reflexivity is not given, however, as is clearly shown by the growth of science and technology.

An inquiry into the ethical analysis of ICTs: an innovation systems perspective

Aygen Kurt[1], Penny Duquenoy[1]
[1] Middlesex University (United Kingdom)

Technological innovations are embedded in complex sets of other technologies; hence knowledge created within innovation processes is an outcome of an accumulation of existing knowledge. For this reason, new technologies and their production trajectories involve various actors and relations among those actors; all making up a complex and an uncertain environment. In such an environment, our current understanding of the patterns of technological change and economic growth suggests that a new set of technological systems, information and communication technologies (ICTs), has gradually come together being capable of guiding the diffusion of technological innovations (Perez 2004). However, this whole process has raised certain social, cultural and ethical questions as the escalating power of ICTs has changed the societal, market and industrial structures immensely since the 1980s due to a cluster of innovations (Freeman and Louca 2002). This presentation centres on the inquiry about understanding ethical issues associated with generic technologies, particularly ICTs, from an innovation systems perspective.

We base our understanding within the fact that the European Commission's attempts to issue strategic plans in relation to information society and its technologies have accelerated in the last decade, especially with the issue of Lisbon Goal. Moreover, the Commission has been highlighting the contribution of ICT investment as the major factor driving the growth of a European economy, and the role of research and development (R&D) and innovation in ICTs in all aspects of industrial sectors (e.g. Rodrigues 2003). It is also obvious that the whole analysis of a European Research Area (ERA) at normative level is framed within the co-evolving two key trends of economic thinking for the last two decades: knowledge economy and innovation systems.

In order to analyse ethical issues associated with specific technologies, we need to understand all the key elements related to the production and innovation of technologies, i.e. the circumstances, regulations, political frameworks, cultural contexts; namely the innovation systems, in which those technologies are produced and even utilised by various stakeholders. Therefore, we need to follow the "trajectories" or the paths of specific technologies (Dosi 1982).

Technology and social change, and the degree to which technology and society affect each other, has taken a significant debate among scholars striving to follow technological trajectories. The social construction of technology (SCOT) approach, for instance, suggests that design and development is a social, negotiated process by relevant social groups from the initial idea to the end-product (Bijker 1995). Before and after the technology comes to the market, the user-producer relation creates a co-shaping interactive process. By looking closely at the relevant social groups (who are involved in shaping a specific technology), with this approach, we may understand the social process development of technology through its historical examination.

However, although SCOT provides us with an analytical approach to how social groups are involved in the design, development and even the stabilisation processes of technology, a systems approach to innovation gives us a more comprehensive framework to go into detail to realise "how" innovations come to life within a geographical territory, an industrial sector or a technological field. First of all, the systemic approach to innovation perceives innovation as an interactive process (involving learning among all the stakeholders and actors of innovation) (Lundvall 1992). Second, it involves time and space, i.e. innovation occurs over time in a given space or under a technological terrain. Moreover, organisations and institutions (as the engines and shapers of innovation processes) constitute the major elements of a system.

The idea that a policy framework and a technological regime within which specific technologies are produced and utilised would significantly affect the innovation process of technology, which would also suggest that certain technological systems are available in specific contexts and their trajectories are directly relevant to the perception of those technologies by stakeholders. In this respect, we need to understand particular technology artefacts and their "stories" about coming to life in order to realise context-driven paths of ethical aspects related to those technologies. Using an innovation systems approach, our aim is to find the right questions leading us to an ethical analysis of technological fields, especially within the realm of ICTs, through identifying major actors and stakeholders involved in the innovation process.

For this reason, we aim to address

- how we could understand ethical issues and ethical governance associated with a specific technological field;
- whether and to what extent the innovation system (together with all the actors, institutions and organisations related to innovations in ICTs) could help us establish basic norms for a Europe-wide ethical analysis of specific sets of technologies; and
- whether analysing innovation processes could give us sufficient insight into formulating a means of ethical analysis for ICTs.

Key words: ethical analysis, innovation system, ICTs

References:

Bijker, W. (1995) *Of bicycles, bakelites, and bulbs*, Cambridge, MA: MIT Press.

Dosi, G. (1982) 'Technological paradigms and technological trajectories: a suggested interpretation of the determinants and directions of technical change', *Research Policy*, Vol. 11, pp. 147-162.

Freeman, C. and F. Louca (2002) *As time goes by: from the industrial revolutions to the information revolution*, New York: Oxford University Press.

Lundvall, B.A. (ed) (1992) *National systems of innovation: towards a theory of innovation and interactive learning*, London: Pinter.

Perez, C. (2004) 'Technological revolutions, paradigm shifts and socio-institutional change' in E. Reinert ed. *Globalisation, economic development and inequality, an alternative perspective*, Cheltenham: Edward Elgar.

Rodrigues, M.J. (2003) 'Introduction: for a European strategy at the turn of the century' in M.J. Rodrigues ed. The new knowledge economy in Europe: a strategy for *international competitiveness and social cohesion*, Cheltenham: Edward Elgar.

The CONFIDENCE system: older people's input at the requirements and conceptual model evaluation stages

Narciso González[1], Anna Kämäräinen[1], Outi Kalla[1], Igone Vélez[2]
[1] University of Jyväskylä (Finland)
[2] Centro de Estudios e Investigaciones Técnicas de Gipuzkoa (Spain)

Globally, the population is growing older. This situation imposes new demands at the individual, social, and political levels. Concomitantly, information and communications technology (ICT) develops at unprecedented pace being present in every sphere of our life and throughout our lifespan. It can be argued that we live in a context of benefit from and dependency on ICT. The CONFIDENCE project aims a providing an ICT support to older people who want to live independently for longer periods before a sheltered accommodation would be adopted. Similar research activities have been carried out also in Italy and Sweden. In this paper we only present the results obtained from individual interviews carried out in Finland. Older people (n =23, average age 75.5, range 65-92, female = 12, male = 11) were interviewed at the beginning of the CONFIDENCE project and at a second stage (n =10, average age = 75, range 68-88, female = 6, male = 4) when the system model had been described with greater detail. Briefly described, this system will be able to reconstruct the user's posture and detect abnormal situations, such as falls or loss of consciousness. The intelligence of CONFIDENCE will be able to discriminate changes in the user's typical behaviour that could entail impending health problems or functional deterioration. When a fall is detected, an alarm is transmitted to a designated alarm receiver or the emergency services. When atypical behaviour is noticed, the user receives a warning informing them about the possible risk and enabling him or her to seek medical consultation. The smartness and predictive capabilities represent some of the main innovations of CONFIDENCE. The users will be able to control whether the alarms are forwarded to the alarm receiver or not. Also, warnings can be dismissed by the users if these are not considered relevant. The technology supporting these functions is based on wearable radio frequency (RF) sensors/tags and wireless communication channels. The hardware components include RF sensors/tags, a processing unit or base station, and a portable device. The portable device serves as the interface between the user and the base station. Ethical principles are considered exhaustively from the concept formation through the technological development and up to the contribution of older people and other stakeholders as research participants.

Early in the project, 23 older people participated in structured individual interviews aimed at eliciting user requirements to feed the technical specification of the system. Ten of these users also participated in structured individual interviews which sought to collect their opinions about a more mature model of the system than that described in the requirements stage. In the requirements elicitation stage, health and aging effects were important factors that a design-forall approach must consider with sufficient detail. These affect the functional ability of older people. Physical and functional abilities in turn affect how older people can interact with ICT systems. Previous experience with the use and their attitudes towards technology may influence the possible ability of the end-users to operate present technologies. These capabilities can also influence whether they are willing to learn and use the system or not. Ubiquity was clearly demanded by the end-users. In other words, the system should work any time and anywhere. The results suggested that older people are active, but fears and barriers exist which might restrict their possibilities to participate in the society. Other important requirements for CONFIDENCE included an immediate and reliable operation in the case of sudden problems, and being otherwise unnoticeable. Undoubtedly, the point of view of the end-users represents an important step towards achieving usable and acceptable ICT solutions, supporting the independence of older people.

In the second stage, 10 of the end-users who had participated in the elicitation of requirements, were shown graphical representations of the components of the system. These were supported with textual information and supplemented with explanations of the interviewers. Questions first addressed the system as a whole, and then each of the different components. When prompted about their estimation of the price of CONFIDENCE, the answers were diverse. Three did not make any estimation, one could not afford it, and another would like to rent it for a monthly fee of less than approximately 50 Euros. The remaining participants made estimations between 200 and 1000 Euros. Two participants reported that they did not want to dedicate too much time to learn how to use the system. Two participants thought that learning would not take many hours. Three participants were not willing to contribute to improve the intelligence of the system to identify normal daily activities from adverse events. However, five participants felt capable of doing this. Nine participants thought that they could learn how to use the system. Eight participants reported that their health condition did not cause any obstacles which may prevent the use of CONFIDENCE. One participant using a pacemaker asked whether the system could affect negatively the function of the pacemaker. With respect to the portable device, 5 answers referred to the possible complexity of using the portable device. The participants were a bit worried about

being able to use the device. Also 5 answers indicated that participants believed that the portable device is simple enough and that they would be able to use it. When asked about the preferred dimension of the portable device the size of a mobile phone was the most representative. However, not each of the participants would like to carry it continuously. In general, the opinions about the portable device were either positive or neutral. The natural speech control/interface was described as an important feature. Most importantly, the participants desired to have voice interaction between themselves and the alarm receivers. The participants showed doubts towards false alarms and thought that false alarms could be frustrating. One participant expressed that he or she could not trust the operation of the system straight away without sufficient evidence. The general opinion towards the system and its monitoring function was that monitoring would not bother them if they really needed it. The older people interviewed wanted a system which is as simple to use as possible. Five participants reported that, in general, technical devices did not raise any fears or concerns on them. Three indicated that learning to use technical devices is difficult. The devices employed by CONFIDENCE did not raise any special fears or concerns. One participant asked whether the radio waves of the tags and sensors could cause health problems in the long term. Eight respondents reported that they felt confident with the system presented. Some of the participants would prefer automatic alarms without confirmation of the user. Some preferred confirmation and alarm if the user does not react to the alarm. Seven participants mentioned health care, alarm centre, or other public service as alarm receivers. Close relatives and the spouse were also mentioned by seven participants. Responses did not vary between the indoor and outdoor situations. One participant pointed out that the legal aspects should be considered carefully (e.g., “who is allowed to investigate the location of the user?”). At the end of the interview, the question about the price was repeated to assess the consistency of the first answers to this. The answers seemed to indicate that the participants were not actually willing to acquire the CONFIDENCE system at their own expenses. Instead, they pointed out that the health or social care services should provide them with such technology. In Finland, assistive devices and social services for older people are supported by the national welfare system. This situation is different form country to country across Europe. Consequently, it must be taken into account when a prototype system aims at being commercialised.

In conclusion, the older Finnish people interviewed in these studies were interested in CONFIDENCE. However, they also revealed doubts about it. Eight participants demonstrated interest in following this research and development activity and to participate later in usability studies and validation trials when the prototype becomes available. According to the results, it seems that the participants are willing to accept the system in their lives and homes. The general attitude towards devices monitoring their activities of daily living was mostly neutral. Older people reported that they would feel safer under continuous monitoring if they could trust that the system works reliably, and that they obtain help quickly in the case of an emergency. Eight of the participants indicated that they would remain living at home with the support of CONFIDENCE rather than moving to a sheltered accommodation. The participants reported that the system would not violate their dignity, integrity, or privacy. The contribution of the older people to these studies is an invaluable resource towards the development of usable and acceptable technologies to support their needs. Continuing efforts must be invested in bringing older people and technology closer to each other in efficient ways.

Session 2: Inclusion and exclusion

Dealing with disruptions: providing internet access to mobile users on a train

Olaf Bergmann[1], Stefanie Gerdes[1], Jörg Ott[2], Nils Seifert[3], Caleb Carroll[4], Nigel Wallbridge[4]
[1] University of Bremen TZI (Germany)
[2] TKK Comnet (Finland)
[3] Lysatiq GmbK (Germany)
[4] Nomad Digital, Ltd. (United Kingdom)

At the time the Internet was designed, end systems were stationary and interconnected through permanent, wired links. Support for highly mobile hosts that frequently switch access technologies hence was neither a design objective for protocols nor for applications that make use of this infrastructure. Since then, the level of integration for electronic circuits increased significantly, leading to high performance, low battery power radio chips at low cost. In addition, the operational expenses for broadband wireless infrastructure have dropped to a level that allows for providing wireless Internet access in most urban regions.

As a result, the role of mobile hosts and nomadic computing in particular becomes more and more important. With growing market share, there is also a high demand for ubiquitous connectivity as users of mobile devices are accustomed to networked applications. Still, in the foreseeable future, the goal of providing "always connected" network access for mobile users will not be met, as wireless links are always subject to limitations: in geographical coverage, due to interference, and obstacles on the radio link, but also for economic reasons.

Thus, despite of the high data rates and increased coverage of modern wireless networks, applications still cannot rely on seamless and ubiquitous connectivity. The quality of Internet access for mobile users may suffer from highly variable communication characteristics (packet loss, delay, throughput) and from temporary disconnections. The former occur as a result of changing radio properties, handovers, or variable system load, the latter whenever wireless coverage is insufficient. While quite some research has tackled improving radio coverage to keep users always best connected and numerous approaches to improve wireless performance and robustness were pursued, these often assume a greenfield deployment or a tight integration with operators.

To mitigate the impact of disruptions, and to enhance disconnection tolerance of mobile user communications, the CHIANTI project has developed an architecture and a protocol to handle network outages independent from the actual access technology and network operator being used. While existing solutions for host mobility or performance enhancements of challenged links often depend on specific deployments or the network operator's assistance, our approach uses a network overlay that can be operated by an independent service provider, and can be deployed step by step.

With user mobility being the major application scenario, the project targets two specific use cases: First, nomadic users who are stationary in a fixed location while using a wireless access network, e.g. being at a WIFI hotspot at a train station. When changing locations, the applications are suspended, i.e. the computer actively disconnects from the network and will actively try to reconnect when the session is resumed. In this use case, there will be no significant change in the network conditions once the network session is set up. In the second use case, mobile users run their computer while moving around. The applications hence are exposed to uncontrolled and unpredictable changes in network connectivity, especially when in a car or riding on a train. In this case, both use-cases could be intermixed as users may suspend their devices when they leave.

To investigate the requirements of these scenarios, a detailed statistical analysis of the Internet usage in a commuter train line has been performed. The Internet service offered on that train relies on WiMAX and UMTS where available and uses GPRS as a fall-back. Within the coaches, clients can connect to the network via WIFI (IEEE 802.11) for free. The device configuration is reduced to a minimum to facilitate use even for casual users.

Under these preconditions, the data collected at the trains' WIFI hotspots show that Web traffic makes more than 85%, 4/5 of which are HTTP and HTTPS. Other traffic such as mail (SMTP and POP3/IMAP4) and various VPN technologies as well as DNS make up approximately 15%. Although the network provided an acceptable link latency of approximately 100ms for an idle HSDPA connection and 400ms for GPRS, a significant increase has been observed with additional background traffic caused by the download of a large file via HTTP. In this case, the HSDPA link latency grew to 1000ms and in some cases reached a maximum of more than 10 seconds. With significant background

traffic, the mean completion time for a Web page that consists of multiple objects in our experiments has been determined to rise up to more than 100 seconds. Interactive pages that require frequent data exchange might even stop working under this conditions.

These results show that application performance suffers badly from rapidly changing round-trip times at the transport level. Although there are several enhancements to the TCP congestion control algorithm that specifically address wireless communication in mobile environments, these form only one building block to improve the performance of mobile end-to-end communication. As this approach requires changes to the end systems' TCP stacks just to address a very specific use case, no wide deployment is anticipated for the near future.

A way to deal with the lack of support for TCP optimizations in end systems is to place intermediaries into the communication path and split end-to-end connections at that network entity. Acting as an end-system, an intermediary then can implement certain optimizations that were not available otherwise.

The CHIANTI system architecture fosters this design to not only improve the performance of TCP but also to address the robustness of application layer communication. The rationale behind this is the observation that disruptions cause a larger decrease of productivity when (networked) applications are terminated because of lost connectivity compared to applications that can survive outages and users do not have to resume their workspace manually. Aiming at mobile and nomadic use of networked applications, the main focus of the CHIANTI project was laid on an easy integration with existing applications and incremental deployment by service providers and access network operators. To do so, real-world constraints such as the existence of network address translators (NATs), firewalls and required pre-authentication have been taken into consideration during the design phase. As a result, a protocol has been developed that can be run on top of the existing communication infrastructure either by the access network operator or by an independent third party service provider. The protocol includes functions for multiplexing distinct data flows over a single TCP connection, fast link detection and automatic recovery to help improving situations where applications rely on having a persistent network connection, even when this is known not to be the case.

The CHIANTI protocol has been validated on a train line with wireless Internet service from Nomad Digital, Ltd. While the CHIANTI proxy server is run at the service provider's data center, traveling users can either bring their own protocol client installed on a private notebook or utilize the CHIANTI client that is installed at the train's on-board unit that also acts as the default gateway for outbound traffic. To facilitate tests with existing applications, communication with the CHIANTI client is done via a SOCKS interface. This also allows to chain modules that implement various optional functions of the CHIANTI suite such as HTTP pre-fetching or caching of RTSP streams. The initial trial phase with the CHIANTI software has revealed that various applications with SOCKS support can benefit from this service especially during long network outages and when roaming between access points caused high round-trip times. Applications thus can recover faster from network outages as the connection is re-established at the transport layer by the CHIANTI software as soon as network connectivity is detected. Still being a proof of concept, the CHIANTI protocol currently does not take much advantage of the underlying transport characteristics. The project consortium therefore has created a test-bench to emulate the characteristics of the wireless link as encountered during the test phase. This allows for systematic evaluation of new protocol features under reproducible network conditions and can help to identify the limitations of the CHIANTI service without actually exposing the production environment to serious service interruption.

ICT that makes the difference for marginalised youngsters

Jan Dekelver[1], Wouter Van den Bosch[2],
[1] K.H.Kempen - K.U.Leuven (Belgium)
[2] K.H.Mechelen (Belgium)

In this paper, we explore the potential of social software tools to support the social inclusion of marginalised youngsters.

Can ICT, and more specifically social software, support the social inclusion of marginalised youngsters? This is the main research question of INCLUSO, a research project funded by the European Commission's 7th Framework programme [1]. INCLUSO aims to deliver a verifiable proof that ICT, and more precisely, social software tools, can facilitate social inclusion of marginalized young people. INCLUSO will make suggestions for future research and development, based on desk research, expert input, pilot projects in 4 countries, the development of a measurement tool to screen evolution in social inclusion/exclusion, and a business and sustainability model for organisations working with ICT in the area of social inclusion.

The pilot projects will be initiated in strong, existing organizations with little or no experience in the use of social software, but already working with marginalised young people, and with a high potential to succeed in successful ICT implementation.

Feedback from the pilots will enhance the white-book that presents implementation scenarios for ICT as a tool for social inclusion. Pilot feedback will also strengthen the business and sustainability models and the measurement tool that screens social inclusion/exclusion.

E-inclusion is one of the current priorities for Europe, as stated by the The Riga Ministerial Declaration of 2006 [2] and confirmed at the Ministerial e-Inclusion Conference and exhibition in Vienna of November 2008 [3].

As more and more information and services are available in digital form today, socially disadvantaged people and those less favoured find themselves at risk of being excluded from the potential benefits of our ever-growing information society. One of those groups at risk of being excluded from today's information society are youngsters that due to socio-economic, legal, cultural or geographic reasons have limited or no access to these tools and the benefits associated with them or lack the skills to use them properly.

All over Europe, welfare organisations working with marginalised youngsters face the reality that social software has become an essential communication tool for many youngsters.

This creates both opportunities as well as challenges for organisations that work with these disadvantaged youngsters. While youngsters quickly become natives in this fast-evolving world of online, social interactions, many welfare organisations are still migrants here.

The question remains on how these organisations can extend their work into these digital environments as they struggle to adapt to the organisational, financial, personal, methodological, cultural and communication issues that arise.

Additionally, social software is all about the social interaction of individuals, who need to be skilled in the proper use of these tools in order to make use of them successfully. While acquiring these skills seems to be less of a problem for most youngsters, this is often different for staff members of welfare organisations. While trained and experienced to work with youngsters in more traditional ways, they find themselves faced with the need to bolster their ICT-related skills in order to make use of a wide range of fast-evolving online tools.

Getting involved on social software platforms to interact with youngsters has the potential to connect to a world where marginalised youngsters need not necessarily be marginalised. The Internet seems to be an ideal place for both youngsters as welfare organisations working with them to find each other, removing the need to travel to a specific location and thus negating both practical as psychological barriers. Some social software tools have the potential to facilitate interactions between welfare organisations and youngsters and between youngsters themselves due to the disinhibition effects related to the use of these tools [4]. Additionally, when used correctly and with the right purpose in mind, these tools could assist marginalised youngsters to transcend their current social identities by extending their social networks and thus increasing their social capital [5].

On the other hand, although access to Internet and ICT in general throughout Europe has steadily increased over the past years, it is often exactly this group of marginalised youngsters that have little or no frequent access to ICT, which puts them even more at risk of social exclusion. Moreover, it is important to recognise that access to ICT is only one

aspect of the Digital Divide today. In order to make use of the full potential of ICT and social software in specific, those making use of these tools must also know how to use them and how to use them *in such ways that it benefits them* [6].

REFERENCES

1. More information available at http://www.incluso.org
2. Ministerial Declaration of Riga, 2006. Available at http://ec.europa.eu/information_society/events/ict_riga_2006/doc/declaration_riga.pdf
3. Presidency conclusions of the Ministerial e-Inclusion Conference of Vienna, 2008. Available at http://ec.europa.eu/information_society/events/einclusion/2008/doc/conclusions.pdf
4. Suler, J (2004). *CyberPsychology and Behavior*, 7, 321-326
5. R. D. Putnam (2000). *Bowling Alone: The Collapse and Revival of American Community*. Simon & Schuster.
6. Hilary Silver, "Social Exclusion: Comparative Analysis of Europe and Middle East Youth," Middle East Youth *Initiative Working Paper* (September 2007), p. 15.

Developing new research

Session: Work in progress

Forensics software for detecting online paedophile activity

James Walkerdine[1], Phil Greenwood[1], Awais Rashid[1], Paul Rayson[1], Corinne May-Chahal[1], Penny Duquenoy[2], Patrick Watson[2], Matt Jones[3], Margaret Brennan[4]
[1] Lancaster University (United Kingdom)
[2] Middlesex University (United Kingdom)
[3] Swansea University (United Kingdom)
[4] University College Cork (Ireland)

Recent years have seen a rapid rise in the number and use of online social networks. Such social networks vary in nature from chat systems, for example, MSN, Skype and IRC, to online communities, such as, MySpace and YouTube, through to file sharing systems, for instance, peer-to-peer networks: Gnutella, BitTorrent, FastTrack, etc. Amongst the many types of 'risk' on the internet as mentioned in the Byron review in the UK and Internet Safety Technical Task Force in the US, these social networks pose two significant risks in terms of child exploitation.

The first major type of risk is paedophiles and other child sex offenders predating on children. Children actively participate in social interactions using forums such as chat rooms and web-based communities. Offenders can use such forums to predate on children, or even to plan the commission of sexual offences against children. These concerns are reflected by the formation of the Virtual Global Taskforce and specialist UK enforcement agencies and Scottish legislation to criminalise the 'grooming' of children in chat rooms in October 2004.

The second risk is the offence of distributing and sharing child abuse media. Child sex offenders can formulate their own social networks using mechanisms, such as file-sharing systems, in order to distribute and share child abuse media. The scale of distribution of illegal media (including child abuse media) on such file-sharing systems was highlighted by a recent study at Lancaster University, which found that 1.6% of searches and 2.4% of responses on the Gnutella peer-o-peer network relate to illegal sexual content. Given the system's scale, these results suggest that, on the Gnutella network alone, hundreds of searches for illegal images occur each second. The study also found that, of those users sharing illegal sexual content, 57% were solely devoted to such distribution while half of the material shared by another 17% involved such content.

The EPSRC funded Isis project aims to help tackle these risks by developing an ethics-centred monitoring framework and toolkit that will support law enforcement agencies in the task of policing online social networks for the purpose of protecting children. Specifically it seeks to tackle three significant research challenges:

1. *How to identify active child sex offenders across online communities?*
   Distinguishing between "innocent" interaction amongst children or children and adults, and the predatory advances of paedophiles and other child sex offenders who will often masquerade as a child or friend in order to gain a potential victims trust
2. *How to identify the core distributors of child abuse media?*
   Accurately identifying child abuse media from the plethora of material that exists within file sharing systems; media that offenders often describe using specialised vocabulary that evolves and changes over time.
3. *How to ensure that any technical solutions maintain ethical practices?*
   Balancing the benefits of using technology for child protection with the need to protect innocent users from the potential of falsely being identified as child sex offenders and safeguarding their privacy.

Given the vast amount of information that is communicated within online social networks, new monitoring and analysis technologies are required. Within Isis novel techniques are being developed that will support the analysis of chat logs and the non-invasive real-time monitoring of file sharing networks by drawing upon natural language processing practices. These can be used, for example, to help determine whether certain terminology repeatedly crops up, or whether users have trademark phrases that they use. Sophisticated statistical analysis techniques allow for the creation of language profiles for certain group types or even for an individual. These have already been successfully used to

automatically distinguish between speech from males and females, from over 35 year olds and under 35 year olds, and also speakers from different regions within the UK. As part of Isis these techniques will be extended to allow the differentiation of child and adult language, and by extension the detection of adults masquerading as children. Law enforcement personnel will also be able to build language profiles of known paedophiles, which could then be used to assist in determining if they are re-offending. It should be noted, however, that our goal is not automation but to provide support for detecting potential sexual offences through analysis of large amounts of data which cannot manually be analysed in an efficient manner.

In parallel the Isis project is also studying the ethical and social implications of the technology that is being developed and, as a result, further informing its development. To date there has been a lack of suitable case studies in the computer ethics literature and appropriate guidance for technology developers to incorporate ethical considerations within the development cycle. Within Isis we are also developing new understandings of user-centred development methods for highly sensitive systems. These, in turn, will benefit future related developments and help mitigate the effects of adverse outcomes that impact on public acceptability.

Session: Work in progress

Breaking the dual function of scientific journals: an *arXiv* case study

Karim Gherab-Martin[1]
[1] Harvard University (United States)

1. Introduction

Digital technology and the Internet have had a strong impact on various sectors of society, as well as on science, of course. In scientific communication, the advent of the Internet has been crucial to the expansion of the movement known as Open Access (OA), which advocates universal and cost-free access to all scientific articles—those, at least, that have been financed with public or non-profit funds.

On the basis of an *arXiv.org*[1] case study, this communication proposes that the system of scientific communication and publishing must be tailored to the new technological (Internet) and social (OA) realities. This would mean that the mission of academic journals must be revised and adapted to the new needs of science and society. Subject-based repositories (SRs) must acquire politico-scientific status in their own right and be recognized as *e-agoras* where *science is happening*. It is becoming urgent that they obtain institutional recognition in the form of scientometric studies.

Let us briefly describe the situation in scientific communication prior to the Internet. The founding of scientific societies in the seventeenth century shifted science from the private to the public realm. This was the birth of *science as institution*, and it was accompanied by the appearance of academic journals whose objective was to disseminate the results obtained by researchers belonging to these societies. Over time, the peer review process emerged, and these journals began to have a dual function.

The first function was related to communicating the results of research studies. Journals were an efficient complement to researchers sending each other letters and private preprints. In this way, journals served to support research by giving it broader dissemination, so we will refer to this as the *research function* of journals. The increase in the number of researchers, universities, and research centers that was seen following World War II generated a formidable increase in the number of articles published as well as an increase in the degree of specialization. As a result, the top journals began to filter articles and select them on the basis of ever more exacting standards of quality which, in turn, made it easier for researchers to locate high-impact articles. The impact of a particular scientific article was conditional on the impact factor of the journal in which it was published. This brings us to the second function.

The second function of journals has been institutional. Since the top journals published the best articles, then researchers were interested in reading and publishing in those journals. Moreover, researchers who were publishing in those journals were valued more highly by institutions and research evaluation committees, which culminated in grants, stable employment, awards and honors, greater funding, etc.

Starting in the 1960s under Garfield's initiative, journal impact factors were created for the purpose of measuring science and those who were doing it. The political, military, social, and economic power science had demonstrated during and after World War II spurred bibliometric studies to measure the performance of researchers as well as to give the scientific policy makers a tool for allocating human and financial resources to the various fields of research. We will call this social and political dimension of the journals' function their *institutional function*.

Our *arXiv.org* case study shows that the Internet and OA have started a transition that is clearly separating the *research function* from the *institutional function*. SRs (rather than the journals) are beginning to fulfill the first function, while the second still remains in the hands of the journals. Digital technology and the Internet are imposing a new logic on communications that should spur us to consider a new organizational model for scientific communication—in the case of physics, at least, which is the discipline analyzed in this case study.

2. OA, SRs and the political value of journals

There are basically two kinds of digital repositories that allow for open access (i.e., cost-free) papers. In both cases, scholars self-archive their works as a final step in their research projects (Harnad, 2001). Subject-based Repositories (SR) usually contain *preprints* (i.e., articles that have not been peer-reviewed yet), and Institutional Repositories (IR) usually contain more *postprints* (i.e., articles that have already been peer-reviewed).

Physicists have developed mechanisms whereby preprints are exchanged prior to submitting them to journals; this is a successful cultural practice that has resulted in the percentage of physics articles rejected by leading journals being much lower than in other scientific fields. This culture has also meant that physics preprints look very much like postprints (Harnad, 2003).

Hence, physicists view the SRs as a place to exchange, file, and deposit their preprints. The most well known example is *arXiv.org*, an SR that was created by physicists. This online preprint repository contains more than 553,888 papers[2] and is an arena in which physicists, mathematicians, computer scientists, quantitative biologists, and statistics scientists self-archive and exchange articles.

SRs have two interdependent objectives: a) to enable the researcher to present and discuss preliminary findings with peers prior to submitting the finalized copy to a journal, and b) to establish a researcher as the first to discover a scientific finding. In contrast, publication of an article in a journal constitutes officialization (or institutionalization) of peer-reviewed results, which is crucial for obtaining recognition and prestige within one's academic community. The peer review process continues to be important in the sense that it represents a line of demarcation between *official science* and the science that is still being done in laboratories and workshops.

OA has been focusing more and more on (and giving greater importance to) articles as units instead of journals as wholes. Digital publishing, however, is retaining journal titles for branding reasons: "journals matter only to differentiate between peer-reviewed articles and non-peer-reviewed publications and to provide symbolic value […], journals contribute to the impact of individual articles by their prestige—a dimension generally associated with the notion of 'impact factor'" (Guédon, 2004, p. 316).

SRs are gradually shaped by the participants' interventions and become trading zones when researchers of different subcultures exchange files. They are a daily meeting place for the exchange of knowledge in the form of ideas, proposals, and empirical data, with different sections for different kinds of subjects. They are "markets" in which scholars, following specific self-archiving protocols, deposit the products they want to show their peers. Therefore, Srs are the proper place to carry out the *research function* of scientific communication.

IRs have a very different mission: they are online archives set up by academic institutions such as universities and research councils to make articles by their own researchers universally accessible on the Internet at no cost. Thus, Irs have an institutional role that mirrors the *institutional function* of scientific journals. The articles in an IR are practically the same articles that have been reviewed and accepted by academic journals (postprints). Thus, the type of OA Stevan Harnad has been arguing over the last decade is very different from the type of OA we are proposing here. Harnad has been promoting IRs to make articles that fulfill the institutional function accessible. Our proposal here is that the use of SRs be promoted and that this be linked to the OA movement so as to encourage the free exchange of preprints that fulfill the research function.

3. Conclusion

Our case study shows that much information of interest was lost in the abyss between the *research physics* carried out in *arXiv* and the *institutionalized physics* published in physics journals.

The journals should revise their model for publishing articles. Peer-review should not be a process used only in selecting individual articles—journals should provide state-of-the-art information, a critical account and a unified narrative of what has happened thus far with a particular scientific problem. Borrowing software technology language, we could say that SRs are the beta version of science, while journals are the equivalent of "finished" products.

The analysis of an *arXiv.org* case study shows the importance of the preprint exchange culture and proposes that journals be converted to institutional and political platforms for: (*a*) the interdisciplinary transfer of knowledge; (*b*) evaluation of a researcher's professional career; and (*c*) making strategy decisions in scientific policy.

The conclusion is that, while the journals' peer review process is still important for institutional purposes, it must be revised and adapted to the new epistemic and social (OA) needs and to the new technological tools (Internet). In physics, at least, SRs are the new *trading zones* and, therefore, should be included in scientometric and bibliometric analyses.

4. Bibliography

Guédon, Jean-Claude (2004): "The 'Green' and 'Gold' Roads to Open Access: The Case for Mixing and Matching", Serials Review 30(4), pp. 315-328, doi:10.1016/j.serrev.2004.09.005.

Harnad, S. (2001). "The self-archiving initiative," Nature 410, pp. 1024-1025.

Harnad, S. (2003). "Electronic Preprints and Postprints," Encyclopedia of Library and Information Science. Marcel Dekker, Inc.

[1] http://arxiv.org/

[2] August 17, 2009

Session: Work in progress

Beyond good and evil? Morality in computer games

Geert Gooskens[1]
[1] University of Antwerp (Belgium)

One of the main attractions of computer games is that they allow us to do things we cannot not do in the real world; they extend our possibilities. In TopSpin 3, for example, we can play the finale of the Wimbledon tennis tournament, although we absolutely lack the qualities even to make it to the first round in real-life. What is perhaps more interesting, however, is that computer games not only enable us to do things we cannot do, but also things we should not do in the real world. One should not, for example, drag people out of their cars, shoot them in broad daylight, and drive away at high speed running over several innocent pedestrians; this is ethically wrong. But in the famous and notorious Grand Theft Auto-series, it is exactly what the player can do. And very recently, a Japanese computer game caused commotion, since it encouraged players to rape virtual girls. In the light of these phenomena, philosophical reflection on the moral status of the virtual actions realized in computer games becomes inevitable.

This paper provides the groundwork for this reflection by asking the following question: Can we apply the predicates of 'right' and 'wrong' to actions realized in computer games? Or do these games bring forth a domain 'beyond good and evil' in which there are no impermissible deeds, i.e. a realm where everything goes? This question will be developed in the three sections, drawing mainly on Edmund Husserl's philosophical analyses of the image, imagination, and theatre.

In the first section, the necessary condition for the application of the predicates of right and wrong to virtual actions will be discussed: freedom. Analogous to the actual world, the player should be able to act freely, before we can judge the player's actions to be right or wrong. In this sense, open-world games like Grand Theft Auto are the most interesting ones, since the player is offered an almost life-like freedom. She is, for example, not forced to murder pedestrians, but can refrain from this. A notable trend in game-development is the tendency of programmers to build-in situations that require some kind of ethical deliberation; that give the player a moral choice. In Call of Duty 5, for example, the player, who incarnates a Russian soldier fighting in World War II, is offered the opportunity to murder unarmed German prisoner's, but can also let them go. This gives rise to the following question: When there is freedom of choice in computer games, why not simply use our normal, non-virtual ethical paradigms for determining the 'rightness' or 'wrongness' to virtual actions?

In the second section, however, it will be explained why this necessary condition is not sufficient to morally judge virtual actions. From philosopher Edmund Husserl's point of view, being and acting in a virtual game-world can be described as a form of image-consciousness: we are perceiving objects, and deal with them, through a mediating object: the image. Imageconsciousness is, according to Husserl, characterized by the so-called 'as-if'-modification. When I am, for example, intending a picture of my grandfather, I am not really perceiving him: it is only as-if I do. It will be argued that, when we apply the 'as-if'-modification to virtual action, it challenges both consequentialism and deontology as ethical paradigms to label virtual actions right or wrong. When we kill someone in Grand Theft Auto, this act has no real outcome (disqualifying consequentialism), nor is it grounded in an actual intention to kill someone (disqualifying deontology). Hence, the game-world appears to be 'beyond good and evil', since there are no actual consequences or intentions there. Computer games seem to provide the player with an extra-moral playground, where she can do whatever she wants. Not so much because it is hard to govern the virtual game-world legally, but because everything going on 'in there' is absolutely harmless. Still, many of us may have the feeling that raping a virtual girl is not right at all. But why is it that we are not comfortable with excessive violence or sexual assault in computer games, if it so obvious that everything happening in the gameworld happens only 'as if'?

This question will be dealt with in the third and last section, where an analogy between the computer game and the theatre will be drawn. With regard to the theatre, the American philosopher Robert Sokolowski makes an interesting distinction between depiction and imagination. Depiction implies that an actor is portraying a certain person and its actions, for example, Marcus Brutus attempting to murder Caesar. Imagination, on the other hand, is a far more serious, less playful, activity, in which someone not merely depicts a particular person, but imagines to be this person and acts like her. Whereas in depiction, the emphasis is on difference ('I depict someone else'), in imagination it is on identity ('I coincide with whom I depict'). We are, for instance, not discomforted by an actor depicting a murderer or a rapist, but we are by someone who looses track of the distinction between her actual self and the immoral character she depicts and, in loosing track of this distinction, imagines to be this character. With this distinction between depiction and imagination in mind, I shall return to the problem of the moral status of virtual actions. Although we have argued in the

previous section that it impossible to label these acts right or wrong, some of them seem not right at all. My hypothesis will be that this ‘ethical discomfort’ is caused by the collapsing difference between the actual person sitting behind the screen, and the ‘immoral’, depicted character. We are not at ease with a person playing a Japanese rape-game, because we suspect this person of not merely depicting arousal and aggression, but of imagining - and therefore becoming - aroused and aggressive. The distinction between the actual person and what Husserl called the ‘image-world-I’ [Bildwelt-Ich] fades away, causing the ‘immoral’ virtual acts to contaminate the actual person.

Session: Work in progress

ICT and overcoming the vulnerabilities of human life

Orpheus as a metaphor for the abolition of man and human relationships

Hendrik Opdebeeck[1]
[1] University of Antwerp (Belgium)

In spite of the many advantages of Information and Communication Technology(ICT) in an era of globalisation, crucial ethical questions raise about the impact of ICT on the organization of work, government and family life. In this paper, we intend to explore how one can prevent the flaws of dark sides of this ICT process from leading to ever-greater ethical decay. By ethical decay, we mean specifically the threat the ICT process poses to what is referred to as the longing for being and solidarity with the other(s). The current globalisation goes hand in hand with an ongoing revolution in ICT. We need to extrapolate to what these technological developments will lead if they are allowed to pursue an autonomous course.
Against this ethical background, in this paper the central role of ICT at the individual and organizational level, is revealed by a hermeneutic approach of the well known myth of Orpheus and Eurydice(1). The fact that in this paper we bring technology in connection with literature, and ethics, is to situate within the Aristotelian tradition in the classification of philosophical subjects. Like M. Nussbaum in her also by Aristotle influenced Upheavals of Thought, we consider a series of poetic subjects, especially technology, aesthetics and poetics, besides theoretical and practical (e.g. ethics, politics and economics) subjects. More concrete we focus on the first European opera on Orpheus and Eurydice, composed by Claudio Monteverdi and for the first time performed in Mantua in the beginning of the 17th. century. Four hundred years later, during this conference on the future of ambient intelligence and ICT, we want to explain how the essence of the leading practical influence of technology on individual and organizational systems can also be discovered in Monteverdi's Orpheus. The theme of this myth and opera indeed is the power of technology, more concrete the power of the technological rationality behind music. This power can soothe all troubled hearts, and now with noble anger (thymos), now with love (epithymos), inflame the coldest minds. Indeed, as music is based on technical instruments (e.g. the lyre of Orpheus, the technique of the voice etc.), one can recognize in this metaphor the power of technology. By his lyre and his voice, Orpheus not only becomes the leader of heaven, hell and earth but also risks to lose the ultimate meaning of his life and work, Eurydice. The (technique of) music of this first opera in European history gives us the chance to be sensitive to the use or abuse of technology and ICT.

> In the myth of Orpheus one discovers a typical description of living and working in antiquity which essence remains very relevant to our times. On the occasion of his marriage Orpheus sings a hymn for Eurydice and in a Heideggerian pastoral landscape shepherds live, work and rejoice in song and dance. All this is shattered by the sudden entrance of the messenger Silvia whose tale slowly emerges. Eurydice has died from a snake-bite. Thanks to his famous music technique Orpheus resolves to recover from Hades. Speranza (Hope) leads Orpheus to the gates of Hades, where she must leave him, for inscribed on the rock at the entrance to Pluto's kingdom are the words (from Dante): "Abandon all hope, ye that enter here". Orpheus reaches the river Styx and encounters the boatman Caronte, who refuses to let him pass. Orpheus summons up all his musical singing technique. As Caronte remains unmoved, Orpheus changes tack, adopting a much simpler music technique. Eventually the boatman is lulled to sleep and Orpheus takes the oars. The chorus comments on the power of man to triumph over all obstacles, applying this technology. Pluto, king of the underworld has heard Orpheus' lament and grants that Eurydice returns to earth, with the condition that Orpheus leads her without looking back. But as he moves earthwards, he has doubts and turns to see, only to find her disappearing before his eyes. Orpheus returns to earth alone and the final chorus comments on the paradox of a man who can conquer Hades with his technique, but not emotions.

When philosophers of technology often conclude that not technology but a misuse of technology leads to problems in the organization of work, government and family life, it is precisely our argument that the ever more presence of technology in economics and society, makes it harder and harder to control ones desires in such a way, one does not prevent becoming the victim of technology. For man it is really hard to resist technology. To remain indifferent is not possible. It becomes apparent that ethics that starts from a neutral or purely instrumental role of technology, is not evident at all. Technology, in the myth of Orpheus the technique of music, both affect man's thymos (willpower, anger) and epithymos (desire, love). In his recent work Zorn und Zeit, the German philosopher Peter Sloterdijk refers to these two fundamental forces, thymos and epitymos, which according to Plato, should be controlled by human reason as two horses behind a racing car. Together as a tripartite (tymos, epithymos and reason) they form the soul of man. The question that we engage in this paper is how the contemporary western society still has the reins in hands. To what extent increasingly driving forward the racing car, does not implicitly admit that the epithymos horse is so shaken up

that it allows the car, another metaphor for technology, to become unmanageable.
For practising ethical performance to build thriving organizational systems, it is important to introduce virtues such as prudence, justice, moderation, who have to bring order and harmony. Without these virtues, reason, in other words, is not capable to keep thymos and epithymos in balance. In the myth of Orpheus, the firmness of Orpheus' thymos accessing the underworld is not feasible without the help of the virtue of hope. When as seen above, technology constantly develops on the basis of ever new needs created and stimulated by business, in the long term the biggest danger is that society is no longer able to rely on technology as a solution to problems. This because society appears to succumb for the permanent overwhelming of her desires. If one really wants to understand the impact of this power, a truly balance must be rediscovered between thymos and epithymos. For this, reintegrating virtues in the ICT context is essential.

European Research Area & ESLA of science

Information session

Efforts of the European Commission to monitor the ESLA aspects of the research funded by its framework programmes

Maurizio Salvi
Head of the EGE Secretariat, Member of the Bureau of European Policy Advisors (BEPA)
European Commission, Brussels

[**Missing**: abstract or summary]

Concluding session

Breakout groups: Drawing conclusions for the implementation of Science and Science analysis

1. ICT research
2. ESLA research
3. Science education

Plenary session: Recommendations to the European Commission, linked to its further Framework Programmes

[**Missing**: abstract or summary]

Open discussion session: Posters and research materials on display

Theme 1: Uses of Ambient Intelligence

Ambient Intelligence approaches water management

Peter Mikulecky[1]
[1] University of Kradec Kralove (Czech Republic)

Ambient intelligence environments may be considered as strongly related with multi-agent systems in that they can be adequately modelled using multi-agent systems of various types. One of the most interesting approaches is based on the idea of so-called ad hoc agent environments.
An ad hoc agent environment (Misker et al., 2004) is a way for users to interact with an ambient intelligent environment. Agents are associated with every device, service or content. The user interacts with his environment as a whole, instead of interacting with individual applications on individual devices. Devices and services in the environment have to be more or less independent, which fits well with the notion that agents are autonomous. The research was oriented on how the user is able to interact with the environment in such a way that he/she would have the control over collaborating agents. Some experiments showed certain tension between the user being in control and the autonomy of agents. Therefore the notion of cooperating groups was introduced as a way for users to gain control over which agents collaborate. Users can then establish connections between devices and content that are meaningful to them, in the context of their task.
The organizational model Aalaadin (Ferber and Gutknecht, 1998) has been quite often used when speaking about participative water management support. The core concepts of the Aalaadin are agent, group and role (Abrami et al., 2002):

- An agent is defined as an active communicating entity, no constraints other than those triggered by the ability to play a role or not.
- A group is defined as a set of agents.
- A role is defined as an abstract representation of an agent function, service or identification within a group. The role encapsulates the way an agent should act within a group. Roles are local to groups.

According to (Abrami et al., 2002) an agent can simultaneously play different roles in different groups, i.e. groups can freely overlap. An agent can enter or leave groups by acquiring or resigning a role, that is, groups are dynamic structures. Groups represent organizational levels, and roles represent functions within these levels; through the roles it is handling, an entity gathers information from the different processes it is involved in without concern about eventual scale or time heterogeneity of these processes.
If we adopt this approach further on, we can combine it with the ad hoc agent environment concept by (Misker et al., 2004) described above. This idea gives us a potential of using ambient intelligence concepts based on multi-agent models, usable for enhancing the watershed by various AmI artifacts capable of ubiquitous communication and helping intelligently to manage the watershed. This concept could be also combined with the largescale ambient intelligence concept described, e.g. by (Iqbal et al, 2008) and others. In the paper we wish to present some possibilities for large-cale ambient intelligence oriented on solving problems appearing in water management, very often having inevitable importance for nature as well as for thousands of inhabitants of certain area with frequently occurring floods.

References

Abrami, G., Barreteau, O., Cernesson, F. (2002). An Agent-Group-Role based modelling framework for participative water management support. In: Proc. of the iEMSs 2002, Vol. 3, Lugano, pp. 497-502.

Ferber, J. and O. Gutknecht (1998). A meta-model for the analysis and design of organizations in multiagents systems. In Demazeau, Y., editor, ICMAS'98, pp. 128–135, Paris.

Iqbal, M. et al (2008). A Sensor Grid Infrastructure for Large-Scale Ambient Intelligence. In: 2008 IEEE Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, 468-473.

Misker, J.M.V., Veenman, C.J., Rothkrantz, L.J.M. (2004) Groups of collaborating users and agents in ambient intelligent environments. In: Proc. ACM AAMAS 2004, ACM, New York, 2004, 1318-1319.

Theme 1: Uses of Ambient Intelligence

A "human-or-bot" authentication means for VoIP systems in the AmI context

Dimitris Gritzalis[1], Nikos Virvilis[1], Alexios Mylonas[1], Yannis Soupionis[1]
[1] Athens University of Economics & Business (Greece)

Athens University of Economics & Business

Dept. of Informatics

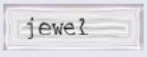
A "human-or-bot" authentication means for VoIP systems in the AmI context

Nikos Virvilis, Alexios Mylonas, Yannis Soupionis, Dimitris Gritzalis
{nvir, amylonas, jsoup, dgrit}@aueb.gr
Information Security and Critical Infrastructure Protection Research Group
Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece

CAPTCHA

CAPTCHA is a contrived acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart". A CAPTCHA is a challenge-response test, or else a "human-or-bot" authentication means, based on open A.I. problems that most humans should be able to pass easily but current computer programs should be very hard to solve. Thus, any correct solution to a CAPTCHA challenge is presumed to be from a human. There are three main CAPTCHA categories: (a) Visual, (b) Logical, and c) Audio CAPTCHA.

Visual CAPTCHA (Text or image based)



Logical CAPTCHA (Simple questions)

Which day, from Thursday, Wednesday, Sunday, or Tuesday, is part of the weekend?

Audio CAPTCHA (Spoken character based)

Regardless of the CAPTCHA category, each one of them must be: (a) Easy for humans to pass, (b) Easy for a tester machine to generate and grad, and (c) Hard for a software bot to solve.

VoIP popularity and the SPIT issue

VoIP is an emerging technology which utilizes traditional data networks to provide inexpensive voice communications worldwide as a promising alternative to the traditional PSTN telephony. Due to this fact, VoIP solutions have gained wide-spread popularity from home users to enterprises. Unfortunately, its popularity makes VoIP particularly interesting to attackers, which can target and exploit its features for their benefit.

One potential source of user annoyance in VoIP environments is the problem of SPam over Internet Telephony (SPIT).

VoIP Spammers, namely "spitters", are be able to exploit VoIP to call individuals and produce audio advertisements through the use of bots.

USA VoIP statistics	
Residential Subscribers, 2006	9.5 Million Dollars
Residential Subscribers, 2010	44.0 Million Dollars
Vonage Subscribers, Q2'06	1.8 Million Dollars
Revenues, 2005	$1.1 Billion Dollars
Mobile VoIP Revenues, 2012	$18.6 Billion Dollars
Fixed VoIP Revenues, 2012	$11.9 Billion Dollars
SMB Spend, 2005	$2.1 Billion Dollars
SMB Spend, 2010	$8.9 Billion Dollars
Spend on Equipment, 2008	$5.8 Billion Dollars
Subs Growth per Month	100.000 Dollars

Source: http://www.metrics2.com/blog/2006/09/25/voip_by_the_numbers_subscribers_revenues_top_servi.html

Audio CAPTCHA as an effective defense against SPIT attacks

Audio CAPTCHAs were initially created to satisfy visual impaired users which wanted to register or make use of a service which demanded the answer of a visual CAPTCHA. However, audio CAPTCHAs can be a very effective defense against the SPIT problem in a VoIP infrastructure.

Design methodology

In order to develop an effective audio CAPTCHA that will achieve the optimal performance (high human success rate and very low bot success rate), we decided upon a number of audio CAPTCHA attributes/characteristics, which were selected via an incremental testing procedure consisting of five stages. In each stage of this procedure we measured the CAPTCHA efficiency, namely the success rate of the bot and the success rate of humans.

Figure 1: Audio CAPTCHA attributes/characteristics

Selected attributes

The attributes that were chosen for the production of our CAPTCHA are the following:

1. Vocabulary: 1) A data field (pool of characters) consisting of ten one-digit numbers (0-9) is used, allowing the users to respond to the CAPTCHA using the DTMF method. 2) A variable number of characters is also used in order to harden automated analysis, and 3) Since the mother tongue of the users is playing a major role in achieving high human success rate, our CAPTCHA can be easily adjusted to the mother tongue of the users.

resulting the bots being unable to segment the audio file correctly. 2) Use of sound distortion techniques is also implemented, preventing bots from isolating the spoken characters from the voice message correctly.

3. Duration: The proposed CAPTCHA avoids using fixed time intervals in order to harden the automated analysis.

4. Audio production: 1) The generation of the audio CAPTCHA files is done periodically to avoid real-time overhead as the production is a resource intensive process and 2) Avoid producing the generation of identical snapshots for extended periods of time. Moreover, different announcers are used, having the announcer of each and every digit selected randomly.

The digits of the CAPTCHA are distributed randomly in the available space.

VoIP Integration

In order to test the bots in a VoIP environment we decided that the implementation procedure should consist of three stages:

Stage 0: When the callee's domain receives a SIP INVITE message, there are three possible distinct outcomes: (a) forward the message to the caller, (b) reject the message, and (c) send a CAPTCHA to the caller.

Stage 1: An audio CAPTCHA is sent (in the form of an 182 message) to the caller. In the proposed implementation, the caller is replaced by a bot. The bot must record the audio CAPTCHA, reform it to an appropriate audio format, and identify the announced digits.

Stage 2: When the bot has generated an answer, it forms a SIP message that includes the DTMF answer. The answer is sent, as a reply to the CAPTCHA puzzle. If the caller does not receive a 200 OK message, then a new CAPTCHA is sent and the bot starts recording again.

The above procedure should be completed in a specific time frame. This time frame begins when the whole audio file (CAPTCHA) has been received by the caller, and expires when the allowed timeout for user input (the answer) is exceeded. The duration of the CAPTCHA playback does not affect the time frame because the waiting time for an answer starts when the playback is complete. If there is no answer before the timeout, then the bot is allowed for another try.

We propose an indicative timeout of six (6) seconds for the answer and a total number of three (3) attempts. This will give adequate time to humans to answer the CAPTCHA, as well as limit the effectiveness of a potential automated brute-force attack against the CAPTCHA.

Figure 2: SIP message exchange for CAPTCHA

Automated bot and audio analysis – Frequency and energy detection

One of the bots that was used to test the proposed CAPTCHA efficiency is developed by J. van der Vorm. It employs frequency and energy peak detection methods.

The selection of this bot was due to its high success rate against known audio CAPTCHA (Google >30%), as well as to the limited time it requires to generate the result.

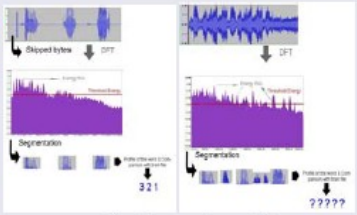


Figure 3: Frequency and energy analysis

User and bot success – Frequency and energy detection

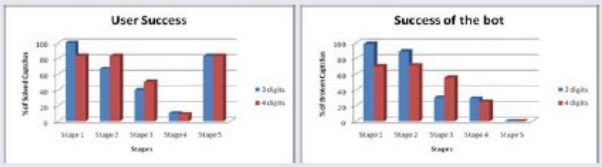


Figure 4: User and bot success rates

Automated bot and audio analysis – Speech recognition

The second bot, which was used against the proposed CAPTCHA was a widely used, state-of-the-art and open-source speech recognition system, namely SPHINX.

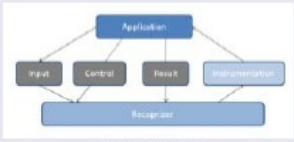


Figure 5: Sphinx-4 Architecture

Bot success – Speech recognition

SPHINX performance was really poor against the proposed CAPTCHA, achieving a low 27% success rate only in stage 1. In stages 2 and 4 the success rate was 0.7-0.8%, whereas in

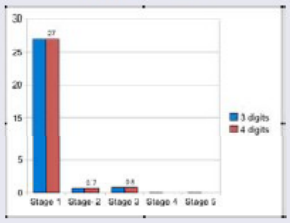


Figure 6: SPHINX success rate vs. proposed CAPTCHA

The main issue for the above results is that such speech recognition tools are effective only in "controlled" conditions, such as with only one speaker, without any noise. Moreover, these methods are demanding in hardware and time resources, because they use combinations of speech recognition methods. Additionally, they do not focus on how quick they reach a result, but rather on how correct the result is.

Conclusions

The proposed CAPTCHA, which aimed to address the SPIT problem in VoIP environments, has achieved a considerable human success rate, as well as a low success rate against two widely known bots. For future research, we envisage to compare the proposed CAPTCHA with additional audio CAPTCHA implementations and aim at optimizing further its success rate, mainly against frequency and energy detection bots.

References

1. von Ahn L., Blum M., Langford J., "Telling Humans & Computer Apart Automatically", Com. of the ACM, Vol. 47, No. 2, pp. 57-60, 2004.
2. von Ahn L., Blum M, Hopper N., Langford J, "CAPTCHA: Using hard AI problems for security", in *Proc. of the International Conference on Theory and Applications of Cryptographic Techniques* (EUROCRYPT 03), E. Biham (Ed.), pp. 294-311, Springer (LNCS 2656), Poland, 2003.
3. Soupionis Y., Tountas G., Gritzalis D., "Audio CAPTCHA for SIP-based VoIP", in *Proc. of the 24th International Information Security Conference* (SEC-2009), pp. 25-38, Gritzalis D., Lopez J. (Eds.), Springer (IFIP AICT 297), Cyprus, 2009.
4. SPHINX: The CMU Sphinx Group Open Source Speech Recognition Engines (http://cmusphinx.sourceforge.net/html/cmusphinx.php) (retrieved August 2009).
5. Tam J., Simsa J., Huggins-Daines D., von Ahn L., Blum M., "Improving Audio CAPTCHAs", in *Proc. of the Symposium on Usable Privacy and Security* (SOUPS 2008), USA, 2008.
6. van der Vorm J., *Defeating Audio (Voice) CAPTCHA* (http://vorm.net/captchas/) (retrieved August 2009).

The idea of the poster is based on Y. Soupionis on-going Ph.D. research at AUEB, being performed under the supervision of Prof. D. Gritzalis.

Context grouping and distribution in the MUSIC middleware

Yves Vanrompay[1], Yolande Berbers[1]
[1] K.U.Leuven (Belgium)

ABSTRACT
Context distribution is a key aspect in mobile and ubiquitous computing environments. The successful adaptation of applications depends on the availability of context information, which is disseminated over the network. Only a fraction of all available context information is required by the adaptation mechanisms. Moreover, for privacy reasons, it is important to limit the scope of context dissemination. We propose a context grouping mechanism which allows the definition of groups based on context information and which provides a low-level privacy mechanism.

1. INTRODUCTION

Context distribution is a key aspect within mobile and ubiquitous computing environments. Context information is acquired by a set of context sensors distributed in the environment. Applications use the collected data to adapt themselves to the current context and optimize QoS for the user. In general, context is any information about the circumstances, objects, and conditions by which the user is surrounded that is considered relevant to the interaction between the user and the ubiquitous computing environment [0]. The success of the adaptation mechanism depends on the availability of context information, which is disseminated over the network. However, in practice, only a fraction of all available context information is required by the adaptation mechanisms. Moreover, for privacy reasons, it is important to limit the scope of context dissemination. We propose a context grouping mechanism which allows the definition of groups based on context information [1]. Each group defines a given context information set that can be distributed among group members. This approach acts as a two-fold mechanism. Firstly, it controls and organizes context distribution over a peer-to-peer network. Each context-aware application running in such an environment will use only a subset of the current context information. Secondly, it provides a low-level privacy mechanism for context distribution, which is an important aspect influencing context distribution. Context information can be sensitive information, whose unlimited distribution is inappropriate. Private context information can be exploited by context-ware applications, but its distribution should thus be limited to the allowed entities. The proposed grouping mechanism belongs to a larger initiative, the MUSIC Project, which provides an open platform, including a middleware, tools and a methodology for developing mobile self-adaptive applications. Applications run on top of the MUSIC middleware and are able to execute and adapt themselves in ubiquitous and dynamic environments.

2. A PEER-TO-PEER CONTEXT DISTRIBUTION ARCHITECTURE

In previous research [3], MUSIC proposed a hybrid peer-to-peer architecture for context distribution, which specified 3 kinds of peers according to device capabilities and associated roles for context distribution purposes: (i) *sensor peers*, which correspond to devices providing only context raw data (context sensors); (ii) *consumer peers*, resource-onstrained devices that need synthesized higher-level context information; (iii) *disseminator peers*, which represent peers providing context distribution services and performing the context reasoning.

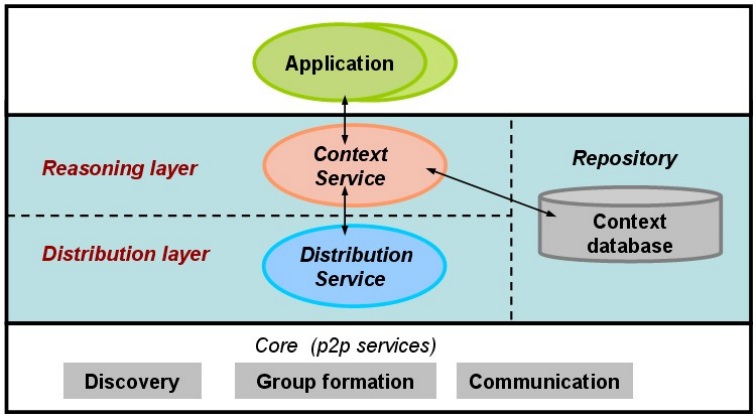


Figure 1: Disseminator peers architecture

In this work, the disseminator peers are responsible for context distribution. As illustrated in figure 1, each of these peers offers a "*Context Service*", which provides context clients with a way to query context or to subscribe to context updates, and a "*Distribution Service*", which disseminates context information in a certain scope. Here we go further by improving these services proposing a more advanced context grouping mechanism. This grouping mechanism makes use of context information as the criteria for group formation and explicitly attributes an allowed context-related content to each group. We consider these services as forming two independent layers: a "reasoning" layer, which manages the context grouping, and a "distribution" layer, which handles the context dissemination according to the grouping definitions. In this way, the grouping mechanism can be defined independently of the actually used distribution technologies. This allows the use of different group formation mechanisms that are adapted to the actual applications running in the middleware.

3. PRIVACY-ENSURING CONTEXTAWARE GROUPING

The main principle of the context-aware grouping mechanism consists in forming groups with peers that share common observable context items (for example the same location or the same network connection). In this sense, grouping can be seen as the peer neighborhood. The notion of neighborhood not only includes the notion of network neighborhood (peers in the same network), but also geographical neighborhood (peers in the same location) or other application-pecific criteria (peers executing over similar devices, peers acting on the behalf of users playing a given role in an organization, etc.). Thus, in the "reasoning" layer, applications can determine the criteria for the group formation. These criteria for forming context groups depend on the context characteristics, which can be described by a context model, in our case the MUSIC Context Model [4]. Figure 2 shows a set of peers forming two groups: a first group is formed based on the peer location (group formation criterion) and disseminating information about device available memory, screen size and battery; and a second group is defined based on the user role and disseminating location information. The criteria defining the groups are translated to real values of peer observable context (location = room x, user role = expert…), which are used by the distribution layer to disseminate the allowed context information.

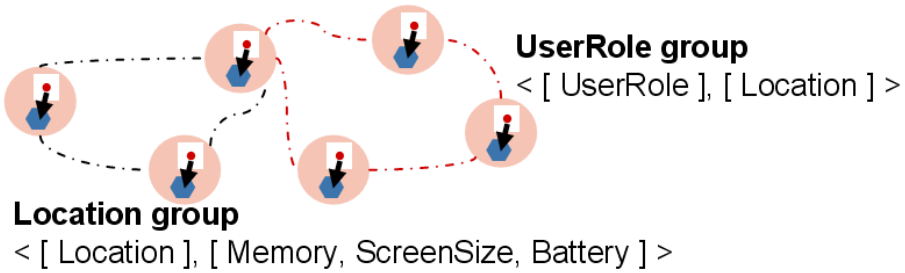


Figure 2: Context groups definition by criteria and allowed content

Context groups are formally defined as follows:

$G_D = < C_D, I_D >$, *where*

- C_D is the *criteria set*, *i.e.* the set of context elements that determine the context group;
- ID is the dissemination set. It is the context information that can be disseminated in this group, i.e. the context elements that are allowed to be disseminated (by push requests) or requested (by pull requests) in this group.

Context information is often considered sensitive and should be disseminated with caution. Organizing context distribution in order to prevent a massive distribution of such information is the first step for building privacy mechanisms proper to the context information. The grouping mechanism we propose in this paper represents a low-evel mechanism that can be used for privacy issues. The main idea, in this case, is to limit the dissemination of certain context information to specific context groups which are allowed to receive this information.

4. CURRENT WORK

We are currently working on automatic formation of groups to implicitly adapt to changing program behavior and network traffic, and optimize group efficiency without program intervention. Automatic formation of groups is done on two levels. On the level of the program, context element requests are monitored and clustered to match possible group formation. Additionally, on the network level, traffic is monitored to avoid redundant formation of groups. Group formation will play a major role in a more general context addressing scheme [5] that improves the addressing of objects in mobile context-aware environments.

5. CONCLUSIONS

Context distribution is a key part of the MUSIC middleware and is improved by the context grouping approach. Network traffic is reduced because context information is only distributed to relevant nodes. Additionally, context grouping enables low-level privacy management which is a first step towards security for MUSIC applications in ubiquitous computing environments.

REFERENCES

[0] Dey, A., Abowd, G., Towards a better understanding of context and context-awareness. Technical Report, 1999

[1] Kirsch-Pinheiro, M., Vanrompay, Y., Victor, K., Berbers, Y., Valla, M., FrÃ , C., Mamelli, A., Barone, P., Hu, X., Devlic, A., Panagiotou, G., Context Grouping Mechanism for Context Distribution in Ubiquitous Environments, DOA08, 2008

[2] MUSIC Consortium, Self-Adapting Applications for Mobile Users in Ubiquitous Computing Environments (MUSIC), Website: http://www.ist-music.eu/

[3] Hu, X., Ding, Y., Paspallis, N., Bratskas, P., Papadopoulos, G.A., Barone, P., Mamelli, A.: A Peer-to-Peer based infrastructure for Context Distribution in Mobile and Ubiquitous Environments. In: R. Meersman, Z. Tari, P. Herrero, (Eds.), 3rd Int. Workshop on Context-Aware Mobile Systems (CAMS'07), OTM Workshops, LNCS 4805, pp. 236-239 (2007)

[4] Reichle, R., Wagner, M., Khan, M.U., Geihs, K., Lorenzo, L., Valla, M., Fra, C., Paspallis, N., Papadopoulos G.A.: A Comprehensive Context Modeling Framework for Pervasive Computing Systems, 8th IFIP Int. Conf. on Distributed Applications and Interoperable Systems (DAIS), 4-6 June, 2008, Oslo, Norway

[5] Davy Preuveneers, Koen Victor, Yves Vanrompay, Peter Rigole, Manuele Kirsch Pinheiro and Yolande Berbers Context-Aware adaptation in an ecology of applications, to appear: Context-Aware Mobile and Ubiquitous Computing for Enhanced Usability: Adaptive Technologies and Applications, (ed Dragan Stojanovic), 2008

Theme 1: Uses of Ambient Intelligence

Discovery and interaction in smart environments

René Reiners[1], Marc Jentsch[1]
[1] Fraunhofer FIT (Germany)

Fraunhofer FIT

Discovery and Interaction in Smart Environments

René Reiners and Marc Jentsch
Fraunhofer Institute for Applied Information Technology
-Mobile Knowledge –

Interaction in UbiComp Environments:

- Discovery of Smart Objects
- Usage of offered functionalities
- Combination of services

Problem Domain

- Virtual functionalities merge with real world objects
- Users' problem: Discovery of smart objects in unfamiliar environments
- Usage and combination of available functionalities

Technical Challenges

- Discovery metaphors for finding smart objects
- Illustration of smart objects' capabilities
- Context – adaptive behavior
- Visualization of possible actions and combinations

Target Scenario

- User enters a new environment
- Tries to discover smart objects
- "Scans" the environment with mobile mediating device
- Functionalities are projected
- Functionalities are shown on augmented camera picture
- User consumes offered functionality:
  - Retrieve media
  - Use media on devices
  - Consume any other kind of service

Expected Results

- Exploration of new interaction metaphors for ubicomp environments
- Introduction of a familiar mediator device
- Easy identification of smart objects for users
- Smooth integration of object tagging and recognition technologies
- Needed technologies also remain invisible
- Augmentation of arbitrary objects

Collaboration and Knowledge Exchanges

FIT: Exploration of interaction metaphors
OFFIS: Approaches for image recognition
ULANC: Experience in mobile computing

UbiTorch

Interaction via Projector Phone

- User points his mobile phone through the environment
- When there is a smart object in the line of sight, it is highlighted by the integrated projector
- The information how well a feature is supported is indicated by the color of highlighting

Projector Setup

- Sophisticated projector phones are currently not available
- A small LED projector is connected to a mobile phone
- Connecting the projector to a battery makes this construction portable.

UbiLens

Visualization on Camera Screen

- User points his mobile phone through the environment
- When there is a smart object in the line of sight, it is highlighted on the camera screen
- Short information about the current object and its functionalities is displayed as an overlay

Concepts & Goals

- Visualization of found objects
- Resolution of Ambiguity
- Selection of functionality
- Adaptation of 2D desktop metaphors like:
  - Hover
  - Click
  - Double Click
  - Drag & Drop

Object Identification

- Infrared light is invisible for the human eye but visible for a mobile phone's camera
- Infrared LEDs are put to every corner of a device to determine its location
- Additional infrared LEDs at the top border are used to determine a device ID
- Other components used for object recognition are:
  - Client – server – based camera image recognition
  - RFID tagging
  - Barcode tagging
  - Semacode tagging

http://www.fit.fraunhofer.de/projects/mobiles-wissen_en.html

Emulating the internet for QoE testing

Sam Lefebvre[1], Brecht Vermeulen[1]
[1] Ghent University, Intec ibcn – IBBT (Belgium)

For many audio and video applications, it is essential to integrate an accurate synchronization system. Video walls, which are composed of tiles, produce video streams that have to be aligned on each other. Video conference systems need synchronization between audio and video to meet the lip-sync requirements, and stereo speaker systems require time synchronization between left and right. The earlier approach was to send such traffic through a dedicated set of wires which also carry the synchronization signals. Unfortunately, this is limited to point to point connections. A further step was the use of circuit switched networks. However, the limitation in distance, higher costs and the growing cloud of inconsistent standards have stimulated the use of “off-the-shelf” packet switched network devices. An extra advantage is that different kinds of traffic can be sent over the same medium.

All these new applications have stringent network requirements such as low delay, wander and jitter. Unfortunately, the current Ethernet standard is not very well suited for this kind of traffic because it was originally developed for ‘best effort’ communication. Current devices have buffers and adaptive clock recovery systems to limit the consequences of these shortcomings. However, it is opportune to specify the mechanisms in order to isolate time sensitive layer-2 packet-flows and provide network resources in terms of buffering and scheduling schemes. Devices of a bridged network have to be synchronized in order to reconstruct the original packet precedence and align the traffic flows.

The IEEE 802.1 AVB (Audio/Video Bridging) tasking group is developing a comprehensive set of standards to address these issues. The original motivation for the AVB project was to enable the use of Ethernet in home and enterprise networks for conventional data as well as audio/video applications.

Three subcategories are specified:
IEEE 802.1Qat Stream Reservation Protocol (SRP) for reservation and admission control
IEEE 802.1AS Precise Timing Protocol (PTP) for providing time synchronization
IEEE 802.1Qav Forwarding and Queuing Enhancements for time-sensitive streams for scheduling and shaping

1) IEEE 802.1Qat: Stream Reservation Protocol (SRP)
Based on IEEE 802.1Q (VLAN tagging protocol), the IEEE 802.1ak MRP (Multiple Registration Protocol) defines a suite of registration protocols for the MAC layer, depending on the item that will be registered. One of them is MSRP (Multiple Stream Reservation Protocol), which is capable of reserving streams and forming the base for SRP. The stream will be identified by the streamID-field (64 bits) in the RTP header, and is passed down to layer-2 in the network stack. The RTP header structure is not changed for AVB, which improves the interoperability. The system defines a request/acknowledgement structure in order to indicate a failed or successful registration process. Hardware buffers are reserved through the entire transmission path. Designated MSRP node (DMN) defines the mapping between MSRP and SRP shared media QoS protocols. The total AVB bandwidth on any link may not exceed 75% of the complete utilization.

2) IEEE 802.1AS: Precise Timing Protocol (PTP)
The Precise Timing Protocol provides a 125µs synchronized clock by sending dedicated RTCP (Real Time Control Protocol, RFC 3550) packets on a regular base. This meets the jitter, wander and time synchronization requirements and eliminates the use of GPS-receivers. RTCP defines the relationship between the AS-clock and the RTP media clock and is customized to fulfill the AVB standard. The grand master, which is the reference clock, is elected using the Best Master Clock Algorithm (BMCA).

3) IEEE 802.1Qav: Forwarding and Queuing Enhancements
IEEE 802.1p defines 8 different QoS field classes. AVB specifies that class 5 is to be used for the lowest latency streaming (250/125µs/hop for 100/1000) and class 4 is reserved for moderate latency streaming (1ms). It remaps the flows when entering an AVB traffic cloud and performs the scheduling and queuing on a per-stream base. The protocol defines bandwidth intervals to avoid bursting (Pacing and Metering).

Challenges:
Currently, the three AVB standards are still in a draft stage and need to be further refined and optimized. The network

management, meaning the way AVB compliant devices will be detected in a network, needs to be further investigated. Like many new technologies, the security management surely is an important issue in order to handle confidential data and prevent malicious hackers. Furthermore, some optimalizations could be defined for the SRP message exchange algorithms. This research will be performed in collaboration with IBBT and Barco NV and will be started in the summer of 2009.

References:
[1] Stream reservation protocol for bridged networks, http://www.freepatentsonline.com/y2009/0049175.html
[2] Virtual Bridged Local Area Networks – Amendment XX: Stream Reservation Protocol (SRP), AVB tasking group of IEEE 802.1, August 1, 2009
[3] Multicast handling in 802.1 AVB Infrastructure, 20 November 2007
[4] Audio Video Bridging, Stream reservation, forwarding and queuing, Sam Lefebvre, Intec IBBT, June 2009
[5] IEEE P1733TM/D2.2 Draft Standard for Layer 3 Transport Protocol for Time Sensitive Applications in Local Area Networks, IEEE 2009
[6] AV Bridging and Ethernet AV, Michael Johas Teener, Broadcom
[7] Marvell FAE Training, Switching 101 to AVB, Don Pannell, Marvell June 2007
[8] IEEE 802.1 AVB and its Application in Carrier-Grade Ethernet, GM. Garnet et Al., SAIT 2007
[9] What is Qat?, Craig Gunter, IEEE 802.1 Plenary Dallas, November 2008
[10] Frame Forwarding Rules for Link Utilization in IEEE 802.1 AVB Networks, MJ Kim et Al., 2008

Managing uncertainty in business and industrial environments

Daniella De Vos[1], Koen Vanhoof[1], Hendrik Van Landeghem[2]
[1] Hasselt University (Belgium)
[2] Ghent University (Belgium)

This paper exposes research on theoretical aspects in continuation of former research on concurrent engineering benchmarking. In this research we relate logistical performances to the financial state of the company. On the one hand we are working with small sample sets per sector, rich in data per sample, on the other hand we resembled financial figures available in the annual statement of accounts published to the Belgian National Bank. Statistical methods cannot be applied. The model works with probability functions and has to combine two different types of data, i.e. qualitative data coming from the surveys and quantitative data from the annual accounts. Both data are related to the decisions made by management in a business and industrial environment.

We looked up theoretical matters to broaden our insights on probability issues and the learning facilities of human mind. Handling uncertainty seems to be a common and captivating actor for both aspects. Experience then narrows uncertainty and is encoded within our memories in patterns. Therefore reminding plays a large part in expert reasoning and entrepreneurs doing business very well have become experts in their branch.

We searched for knowledge on the quantification of information and its measuring. A binary decision between two things is made answering ‘yes’ and ‘no’ questions, called a ‘bit’. Then information becomes a measurable entity. The big start on this subject started with Shannon. In the data analysis field Shannon was the base for the Information Theory which in turn is the base of our research. The concept entropy is the measure of the amount of information one is missing, expressed in terms of probabilities. The ever growing mass of information is a growing disordering process. Next, human mind is confronted with uncertainty, i.e. the amount of information missing in order to get a 100% certainty.

We opted for a quantitative modelling approach. The model aims to extract new information to be added to the existing data. We identified objective criteria to decide whether one state of the model is better or more desirable then the other. A common denominator serves the classification of the training cases : a financial criterion. Another criterion is the size of the company. The ‘best’ course is then identified within the classification of the training cases. The model transforms the quantitative and qualitative data of the examples into quantitative measures. This new concept is an aggregation and ordering process of information and becomes the memories of the model looked up passing a new test case.

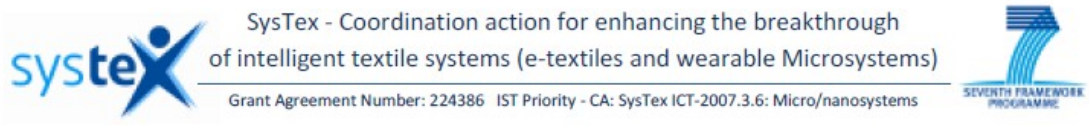
The model experiments with uncertainty and classifies the different cases searching for patterns. This then is the analyzing part on the new concepts or symbolic data.

Visualization techniques are used. Latter have been recognized as an effective way to communicate both abstract and concrete ideas. In this phase we are also looking for rules, i.e. we attempt to formulate the patterns of data in words as rules express predictions based on the information available i.e. are giving responses on future events based on elliptical data.

Theme 1: Uses of Ambient Intelligence

SysTex - For the future of smart fabrics and interactive textiles in Europe

Lina Rambausek[1], Lieva Van Langenhove[1]
[1] Ghent University (Belgium)



The European textile and clothing industry still significantly contributes to the wealth in Europe. Nevertheless it faces huge challenges today. Fierce worldwide competition is at present putting a lot of pressure on our textile industry. E-textiles, also called intelligent, interactive or smart textiles or textile systems are expected to be a new generation of textile products that can help the textile industry in its transformation into a competitive knowledge driven industry. They are electronic systems based on or embedded in textile substrates, adding wearability and comfort to devices and systems made for signal acquisition, transmission and processing. An example could be wearable health monitoring systems. Basically these systems include sensing and actuation, data processing, communication and energy supply. E-extiles and wearable electronics are expected to be one of the answers to these threats and hence will play a significant role in the future European textile and clothing sector. But also on societal level they will contribute significantly. In particular application areas like health, sports and protection their benefits are enormous, leading to improved health care and safety, combining increased performance and cost savings. Several projects in smart textiles and wearable electronics have been carried out or are under execution within national as well as European programmes. Also in the US and Asian countries small and large projects are being undertaken. **Co-ordination** is limited and only takes place on an international level.

E-textiles and wearable electronics are complex systems that combine knowledge from many disciplines with the specific requirements of textile and clothes and this is a huge challenge. Intelligent stand alone suits must be considered as systems consisting of a set of components and this system approach is rather new to textiles. However without a **system approach** successful developments cannot be achieved. In addition individual components/devices are often available but when they are brought together in one system for one particular application often the overall result does not meet the requirements. Similarly, solutions found for one particular application may not fully meet the requirements for other applications.

Another challenge is the **gap** between Microsystems (often large to very large companies) and textiles (consisting of more than 90% of SME's). Many materials and systems are available as well as devices for sensing and actuation, but they are not compatible with a textile nor with the textile production process. They could be transformed into a textile compatible structure or even in a full textile structure, but for this understanding on how the devices work must be combined with knowledge on textile materials, structures and processes and this turns out to be the obstacle. Organic electronics is an emerging field that merges electronics and polymeric materials, but textiles are still hardly involved in this.

Several efforts are made to make **surveys** or **roadmaps** in areas related to e-textiles.

SYSTEX wants to coordinate the activities of these actions and offer complementary actions to reinforce their overall result.

All partners will collect information within their own range of activities on technological as well as non technological aspects of smart textile systems.

This information will be stored in a user friendly data base. This data base will be accessible through the project website. Access rights will vary according to the status of a person requesting access to the database e.g. project partner, member of the user group who have signed an agreement or other person.

The information will be analysed in order to identify actions needed to meet the prime objective of SYSTEX. Actions that will be taken include preparation of an agenda for research and development, dissemination of available and missing knowledge and experience, communication with all stakeholders ranging from policy makers to the end users (wide public).

Apart from information, special efforts will be made to exchange materials as well. This includes collecting demonstrators but also prototypes for inter project exchange.

The information will be spread actively through training as well as through dissemination. Target groups are industry, researchers, students and potential end users. The intention is to combine activities with ongoing events and networks and to create as many synergy effects as possible.

A task will be dedicated to agreements that must enable optimal inter project exchanges as well as access to confidential information wherever appropriate.

SYSTEX aims at developing a framework for current and future actions in research, education and technology transfer in the field of e-textiles and wearable micro systems / electronics in Europe to support the textile industry in the most efficient and effective way to transform into a dynamic, innovative, knowledge-driven competitive and sustainable sector.

uWear - Wearable technology for you

Alexandru Stan[1], Michael Weber[1], George Ioannidis[1], Roselyne van der Keul[1], Hugo Verweij[2], Richard van Tol[2]
[1] IN2 Search Interfaces Development ltd. (Germany)
[2] Utrecht School of the Arts (The Netherlands)

1. Introduction

The wearIT@work project was set up by the European Commission as an Integrated Project to investigate “Wearable Computing” as a technology dealing with computer systems integrated in clothing. WearIT@work sets the stage for the applicability of wearable computer technology in various industrial environments, by using novel computer systems to support their users in an unobtrusive way. This allows them to perform their primary task without distracting their attention and thus enabling computer applications in novel fields. One of the major goals is to investigate the user acceptance of wearables and the project established three take-up actions, one of which was the uWEAR project. This poster describes the system developed by uWEAR and the results of the user tests.

uWEAR addresses users on a more personal level and investigated how new technologies could enrich their everyday life. By adapting and extending existing WearIT@Work wearable components, uWEAR developed navigational services for visually impaired users. The interfaces designed in uWEAR allow the user to efficiently get the required information whenever necessary, while minimizing interference with current actions. uWEAR is not meant to replace current tools such as white canes, but rather augment them in order to empower the users and give them more independence. uWEAR makes it possible to, for example, get route guidance to a place that was never visited before, or always find out the current position - two not so trivial tasks for the blind.

2. System Overview

The approach followed by uWEAR is adapted from User Sensitive Inclusive Design that bases its methodology on the Design for All / Universal Design movement. An iterative development cycle was chosen to ensure that a maximum of user requirements were incorporated and validated in the technical solution, thus improving acceptance of the developed technologies.

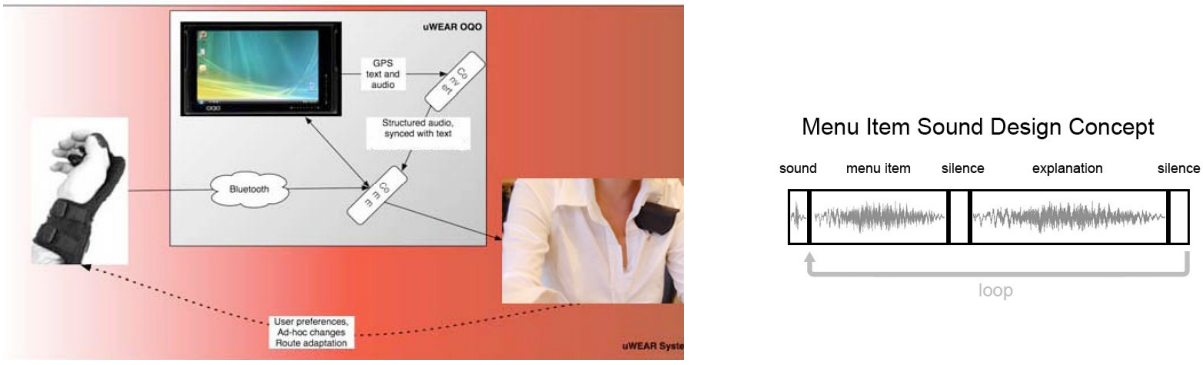


Figure 1 The uWear system and Audio menu design

The system was built in a modular fashion such that various components can be replaced easily as upgrades become available. Figure1 gives a representation of the high-level system architecture. Below we give a brief description of the system components.

The TZI SCIPIO Winspect Glove [1] is a general purpose wearable input device that was developed by the WearLab at TZI Bremen. The physical appearance is of a lightweight fingerless glove with two buttons that are fitted around the finger. The glove was designed in such a way that it does not interfere with the way a user performs regular tasks. Through custom micro-gestures and the finger buttons, the glove can be used to browse menus and make selections. As an alternative input interface, the user can make use of speech by issuing simple commands such as "previous", "next"

and "select" or make selections according to the menu item names. Those are available within a grammar, which is automatically created and updated for the current menu screen.

The uWEAR team developed a wearable speaker. We tested different speaker designs and decided to use a small and cheap off the shelf available speaker that can be connected trough a mini-jack connection and that works on its own AAA-batteries. We integrated this speaker into a small reflective, waterproof and magnetic cover that can be easily and flexibly attached to different pieces of clothing.

A major part of the output interface of the system is the audio menu, which provides sound-only feedback of the system and which is controlled by the data glove. The looping menu is designed so that it supports not only novice users, but also more experienced users and even expert ones. For this, each menu item consists of three parts. The first part, a generic beep which pitch and timbre is based on the number of items and depth in the menu, allows expert users who are already familiar with the menus to browse solely on pitch. The second part consists of a short line of speech, announcing the menu title. The third part consists of a more lengthy description of the menu item, describing what the menu item is used for. This allows novice users to learn the function of each menu item. Each part is followed by a small silence.

The WUI-Toolkit [2] is a framework to support and ease the development of wearable user interfaces. The toolkit features the ability to use available context sources and can automatically adapt generated interfaces to maintain their usability. The computing horsepower is provided by the OQO e2 wearable computer. For the outdoor scenario the current coordinates can be provided to the system using any common GPS receiver, using Bluetooth for connectivity. For the outdoor route calculation an off-the-shelf solution was used, while in the indoor scenario a custom algorithm was developed.

3. Test results and Evaluation

A total of three tests were carried out with 3 to 6 users each. The users were both male and female, between 18 and 48 years old, having different experience level with computers. The actual tests consisted of a number of tasks that the user had to fulfill, varying from simply setting a route to a specific location, to actual way-finding outdoors and indoors on the basis of instruction provided by the uWEAR system.

The shoulder speaker user tests revealed that flexibility and fashion are of prime importance. This resulted in the selection of the magnetic speaker which can be place anywhere and is also very discrete. As a further improvement the speaker should be wirelessly connected.

Testing of the outdoor scenario showed the need of using navigational software that is designed for pedestrian use. Nevertheless, the test also revealed that the system does indeed blend very well with the existing navigational tools of the visually impaired people: the system gives the instruction 'first street on the right', the user gives this instruction to the dog and the dog selects the first street on the right. Another participant that was using a white cane noted that while the instructions from the system sometimes came quite early or too late ('turn left') the participant could decide for herself whether or not it was really the right position to turn right by combining the audio instruction with echo-location techniques.

Testing of the indoor scenario was based on a mock-up of an actual RFID tile room. The test was concerned with the way to provide instructions to the users and the type of instructions that would be optimal for them. The user feedback was very positive regarding such a system. The users enjoyed the extra information that they received apart from the strictly navigational instructions ("kitchen on the right").

Overall the prototype was well received in terms of usability and functionality. This proves that by careful design and with strong user centered development, wearable computing is a technology that can be assimilated easily. The different stages in the development and user test cycles allowed us to include many valuable recommendations and requirements from the user-perspective. Our initial assumption on the importance of a good audio-based menu for the success of a uWEAR type of technology, was confirmed in the tests. The importance of paying sufficient attention to the audio-design applies especially to this specific user group of Visually Impaired People, but it is likely to also apply to a wide range of other technologies that include sound as an important component of their interfaces. The system will be enhanced and customized for other target groups, for example sport enthusiasts like cyclists or snowboarders, who require the same level of unobtrusiveness when it comes to navigation.

Acknowledgment: This work has been funded by the European Commission through IST Project wearIT@work: Empowering the Mobile Worker with Wearable Computing (No. IP 004216-2004).

References

[1] Michael Lawo, Hendrik Witt, Holger Kenn, Tom Nicolai, Rü diger Leibrand, (2006), *A Glove for Seamless Computer Interaction - Understand the WINSPECT*. In Proceedings of the The Smart Glove Workshop, pp. 3-8
[2] Hendrik Witt, Tom Nicolai, Holger Kenn, (29th June, 2007), *The WUIToolkit: A Modeldriven UI Development Framework for Wearable User Interfaces*. 7th IEEE International Workshop on Smart Appliances and Wearable Computing (IWSAWC), Toronto, Canada.

Theme 2: Security

Physical and digital security: getting the best of both worlds

Roel Wieringa[1], Wolter Pieters[1], André van Cleeff[1]
[1] University of Twente (The Netherlands)

[**Missing**: abstract or summary]

Developing a novel service concept for wellbeing management: methodological perspective to the concept definition

Veikko Ikonen[1]
[1] VTT (Finland)

We developed a novel service concept for wellbeing management of a working age population. The focus of this so-called “P4Well” (Personal and PsychoPhysiological WELLness and recovery management based on stress, sleep, and exercise). concept is on managing stress, overload, and recovery from load caused by daily life. Our driving principle in designing the concept has been the fact that an individual is the best master of his/her own wellness. In the concept, the main tools for the wellbeing management are composed of (1) stress management and methods for recovery, (2) exercise, (3) sleep, and (4) psychological intervention methods The building blocks of the tools consisted of technologies such as mobile phones, pedometer, heart rate monitor, sleep time monitor, and different analysis software. These technologies are combined with psychological miniintervention methods and physiological theories forming a coherent and cost-efficient concept to support a life-style change; emphasizing self-management, with potential expert consultation.

In this paper we focus on a concept definition phase where the ICT solutions are specified for further development. In the design procedure of the P4Well concept, we used cross-disciplinary working methods to design the concept and its requirements, as well as to discuss the usage scenarios of the service. The participants of the expert group (EG) meetings consisted of experts from participating organisations with various backgrounds, for example, in engineering, physiology, psychology, business, and other fields.

The goal of the EG meetings was to develop the requirements and general description of the functions and elements of the concept (Error: Reference source not found). The approach for the concept creation was need-driven, since our assumption was that technologies are mainly available for their utilization, and that the immature applications and service designs would be the main hindrances for the wider spread of new potential wellness technologies.

We wanted to have efficient but yet inspiring working group meetings with the experts from the different fields. To do so, we emphasized the collaborative working group methods to collect opinions from all the stakeholders, and to create genuine cross disciplinary discussions. Each meeting lasted from half a day to one or two working days. Our plan for the six expert group meeting topics were following:

First EG meeting: brainstorming for new ideas, examining potential target groups, ethical issues, and identifying basic elements for the service concept. A dialogue workshop method was used [viite1]: punctilious manuscripted group discussions under predefined themes and groups. The goal was to get different perspectives from the various stakeholders for the concept development in a deliberative manner.

Second EG meeting: user stories, use cases, and their analyses, as well as pathways of usage (see Error: Reference source not found, viite 2). A preliminary task and scenario-pair-writing methods were performed. We organized one hour writing sessions as a pair work for P4Well user scenario creation.

Third EG meeting: Legal and ethical issues. In this meeting, we applied a conventional team work method. The aim of the meeting was to find out the most critical ethical as well as juridical issues related to the service concept.

Fourth EG meeting: an intermediate summary report of the concept work was launched, and we revised the results of our previous meetings. The goal was to investigate the material gathered for the concept and (re)direct the remaining concept development work according to the made conclusions.

Fifth EG meeting: technology concept, functions, and critical requirements. In this meeting, a so-called card-sorting game was “played” in pairs. The aim of the meeting was to prioritize and categorize most relevant features for the concept in different usage phases using the collaborative, as well as entertaining, approach.

Sixth EG meeting: business models, value chains, and concept review. This meeting consisted of pair and group works with the stakeholder cards from the previous meeting with the potential business platform. The goal was to identify potential business models for the P4Well service concept and also study potential opportunities and threats related to the

analyzed models.

Based on the results of the six expert group meetings, we defined the requirements for the concept as:

- The target group: citizen between the ages 30-64 years. Concept should be suitable especially for small company employees/employers (company size less than 10 employees) and for entrepreneurs due to general lack of cost-efficient service access by them currently.
- Most potential utilisation time of the concept: From primary prevention to early intervention, no diagnosis of illness required (but allowed). The emphasis must be on self management, with potential expert consultation and support.
- The content focus: stress, recovery, and mental wellbeing (including signs of mild to moderate depression).
- The methods: the intervention and management methods include stress management and recovery strategies, physical activity, exercising, sleep, and psychological methods.
- The driving principle: the concept was defined so that an individual is seen as the best master of his/her own wellness.

In this paper we will focus on the design process of early concept definition phase, and share our experiences based on that. We will also briefly describe later studies with potential users of the service and describe forthcoming next steps of the work. However, our main contribution in this paper will be the methodological and design process perspective while developing personal health and well-being management system.

Theme 3: ICT, health and care

Exploring the crossroad between ICT and life sciences through modelling of biochemical data

Wanda Guedens[1], Monique Reynders[1]
[1] Hasselt University (Belgium)

universiteit hasselt

Exploring the Crossroad between ICT and Life Sciences through modeling of Biochemical Data

Wanda Guedens and Monique Reynders

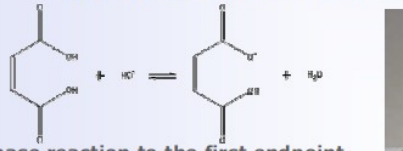
Hasselt University, Campus Diepenbeek, Agoralaan - Building D, BE-3590, Diepenbeek, Belgium
E-mail: wanda.guedens@uhasselt.be; monique.reynders@uhasselt.be

Introduction

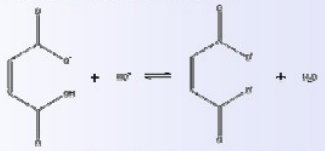
Data from a potentiometric acid-base titration digitally transferred to a graphing calculator during a biochemistry class are studied in a mathematics lesson. The graphing calculator provides the ability to modeling data by smart edits easy to implement. This is a most challenging way of bridging the mind gap between biochemistry and mathematics for youngsters exposed to a digital world.

A Biochemistry Class

An unknown solution of maleic acid or *cis*-butenedioic acid is titrated with a 0,1000 mol/L NaOH solution.
Two endpoints can be detected for it is a titration of a weak diprotic acid with a strong base.



Acid-base reaction to the first endpoint



Acid-base reaction to the second endpoint

Collecting Data from the acid-base Titration

The data collection is done with DataMate™, a program that transfers signals from the Vernier™ pH-sensor to the graphing calculator, Texas Instruments TI-84 Plus (TI-84+).

The collected data are stored into lists:

- VOL is the list of the volume of the added NaOH solution
- PH is the list of the corresponding pH-data

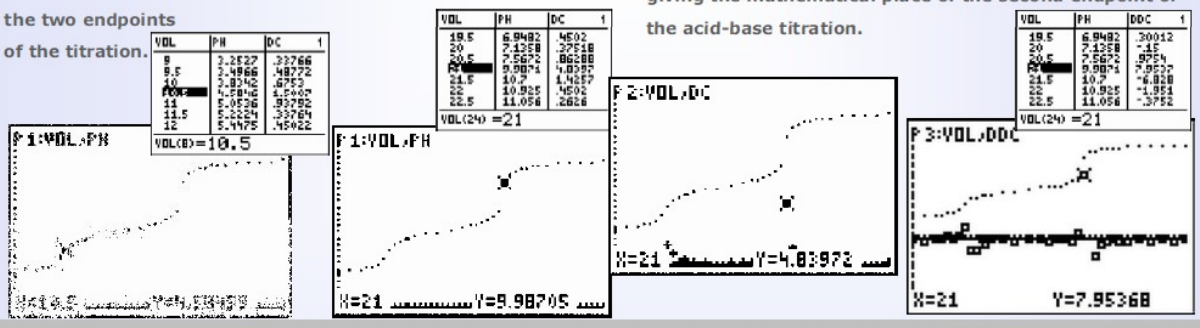
The calculator can also present the PH(VOL)-graphic showing the two endpoints of the titration.

Experimental Data-Analysis

Mathematical analyses of the second endpoint – the most explicit slope of the curve – show the first and second derivative using respectively the formulae:

- ΔList(PH)/ΔList(VOL) = List(DC)
- ΔList(DC)/ΔList(VOL) = List(DDC)

These analyses result in a DC(VOL)- and a DDC(VOL)-curve giving the mathematical place of the second endpoint of the acid-base titration.



Conclusion

Using the method of interdisciplinary teaching biochemistry and mathematics by means of the graphing calculator the gap between these two disciplines becomes smaller. This interactive manner of teaching also engages the interest of the general public, but above all by providing modern ICT tools and lessons in context science and technology become more accessible for the next generation.

Literature cited

–Guedens, W. & Reynders, M. (2003). *Geboeid door Wiskunde en Wetenschappen-Chemie, Meten met sensoren in vier leerlingenpractica: Temperatuur-pH-Geleidbaarheid-Extinctie*, D/2003/2451/33, LUC Diepenbeek, België
–Holmquist D.D., Volz.D. (2000). *Chemistry with computers – Using Logger Pro™*, Second ed. Beaverton: Vernier Software & Technology.
–www.education.ti.com
–www.rhombus.be
–www.vernier.com

The morality of software usage

Fabian Geier[1]
[1] University of Bamberg (Germany)

The question of which software we should use – which browser, which data format, which operating system – is one of the most fiercely discussed questions in ICT. In many quarters it is a sure kick-off for squabbles, prejudices and outright condemnation. Even where technical arguments are put forward, it often seems that people have only been looking for them in order to support an affection that is itself not founded on technical reasons. At the same time the discussion also makes heavy use of moral categories. One of the most central terms is the emphasis on freedom ("free as in free speech, not as in free beer"), i.e. as advocated by the Free Software Movement. But also negative moral judgements are put forward abundantly when it comes to why we should abstain from Apple, Microsoft or Skype. Given the fierceness of this discussion it seems a desideratum, to soberly and comprehensively analyse the possible moral qualities of software.

While problems like Privacy, Intellectual Property or the Digital Divides have attracted an enormous amount of research, the question of the Morality of Software Usage has rarely been addressed. Main contributions to the discussion have rather been made by engineers than by genuine scholars. It seems to be especially ICT-pioneers like Richard Stallman or Eric S. Raymond, who are most sensitive to the problem. Picking up their threads – without agreeing with them in every respect – I would like to outline questions and conceptual frameworks for further research: What are the criteria and the type of arguments relevant for the morality of software usage? I would frame this under the following topics:

1. The Question of Freedom
What does freedom mean with regard to software? On the one hand it is the freedom of choice: the opportunity to modify and use different devices to different aims. This is the idea of freedom put forward by advocates of Free Software. On the other hand, freedom means not giving anyone or any institution the power to arbitrarily limit or change the choices we have. Since in the realm of programming the borders between different systems are less stable than in primary reality, the question of power is of extraordinary importance. Control over a basic system can easily be used to extend control to another system. Thus it was possible to extend control from the market for operating systems to the browser-market and from there to modifying world wide web standards. Such a taking hold of standards decreases the number of choices for developers and subsequently for users: Both have to follow the standards the controller finds most suitable to establish for its own ends – as opposed to which standards would guarantee the best platform for generating new things and new choices.

2. Consequentialist Arguments
A second way to approach the morality of software usage is to judge them by their benefits and drawbacks for the user: What are the results of the use of certain software pieces for the life of the people who use it? No matter whether it is made according to an open source or closed source model, or whether it poses a de facto standard or an unknown product, software can have good and bad effects on its users in various ways.
a.) Does a program accomplish its task to the highest possible degree or reach only less than optimal results?
b.) Does it do so in the most efficient way or does it steal unnecessary resources (time and labour)?
c.) Does the program and the knowledge and habits of handling it open up new possibilities, or is the user stuck with what it does? Or does he even depend on further help or further products (lock-in effects)?
d.) In which way does software influence our thinking about us and the world?
e.) Does a program force us to trade the use of it for other unwelcome things, i.e. giving away parts of our privacy, or our control over our devices and their further development?

3. Structure: What software should be like
Another question is the inner structure of software. When economic and marketing interests determine the structure of a piece of software, it differs significantly from what it would be like if it had been developed independently from such influences. Certain functions will be hidden or artificially limited, and others more emphasized than they would be, if they were developed just for accomplishing the task they are supposed to fulfill. It might be interesting to ask whether such an influence should be considered wrong, even if it does not clearly lead to bad consequences in one of the above ways. Does it make sense to talk about a "nature of software" - meaning the way that a piece of software would and should be like, if no outer interests would guide its development? And is it in any way valuable to view this nature as being "corrupted" by such external influences?

4. Software as a Product

Why does it matter morally whether we use one software in favour of another? Software is a tool that can be used for both good and bad ends. So one might claim that it itself is morally neutral. But software is also a product in our economic system and therefore the question of good and bad starts already when we use it, and even more so if we spend money on it. Outside ICT the idea of ethical choices in consumption is well established: By spending money on a product we support a company and a policy along with it, and these might entail various acts of moral relevance. In software products, however, problems like child labour and industrial safety are of minor importance. Instead there is another aspect of specific relevance for them: Affirmation by participation. Information systems are not a solitary undertaking but highly standardized and cross-linked so that they essentially depend on compatibility with each other. The usage of a certain product, especially in conjunction with others, automatically means supporting specific data formats and protocols (many of them invisible to the ordinary user) and subsequently a.) approves of the acts by which a company has achieved the status its product has and b.) gives momentum to further establishing the respective standards as a means of power.

5. Radicalism vs. Pragmatism

What are the consequences of all this? Which software, if any, should we deny then? And should we even go so far as to compromise our own capacity to act within the world of ICT – and thus limit the very number of choices for which we wanted to be free? This is a question that individuals, companies and software-projects, too, have to answer (A good example are the incessant discussions about binary firmware blobs in the Debian-project).

There is certainly not one answer that fits all situations. Indeed it seems important that there are both crusaders for software entirely free of restraints, like Richard Stallman. And yet there may also be good reasons not to consider this the most pressing moral question in ICT nowadays. This is expressed in the more pragmatic approaches of people like Ted Ts'o or Linus Thorwalds. And especially when it comes to possible futures of ICT, it is vital to discuss whether pragmatic approaches have damaged the goal the radical approach is pursuing or whether they have helped to give it momentum in a society that has more questions to solve than the problem of software usage alone.

Theme 4: Ethical aspects

A new participatory conception of technology: when ICT meets ethics

Penny Duquenoy[1], Aygen Kurt[1], Norberto Patrignani[2], Federico Rajola[2], Alessia Santuccio[2]
[1] Middlesex University (United Kingdom)
[2] Università Cattolica del Sacro Cuore di Milano (Italy)

Nowadays it is impossible not to recognise the relevance and positive impact of ICTs in everyday life. ICTs present opportunities for social interaction and management of life activities in new ways, offering great potential for enhancing many aspects of living. In fact, since our environment will become aware, active and responsive, many applications will have the immense potential to bring benefit to our lives by improving our communication abilities, automating common tasks, assisting those with special needs to participate more actively in society and helping to keep vulnerable populations safe. Indeed, on one side, this evolution can be considered as an important goal reached by civil society, in particular if we think about how ICTs can help particular categories of users, for example the elderly and infirm.

On the other hand, the very characteristics of these technologies that lend themselves to inspiring visions of the future (such as the Ambient Intelligence environment) also hold the potential for negative ethical impact as those applications have the potential to lead us to an Orwellian society where every person's action could be monitored and recorded. When the application of these emerging technologies also include life-critical matters, then availability and reliability concerns (typical of very complex computing applications) become critically important. Important questions arise, which include but are not limited to the following: is equality of access to the ICTs guaranteed (digital divide)? Are there specific guidelines for user-centred design (at what stage, if any, will the end-user be involved in the design process?)? Is there a security control (who will have access to sensitive information, how, and for how long?)? Will the combined impact (of multiple applications) be robust, and manageable, by the end user?

These are issues that the society is already aware of but as technologies converge, interactions and possibilities for interactions change, and the use of intelligent systems and agents increases, other impacts as yet unknown are likely to emerge.

Put briefly, the questions above (and others we are not yet aware of) suggest a need for a coherent framework for an ethical governance of ICTs which today is missing, both at the EU and international level. The convergence of ICTs with ethics is relevant, as it helps to address the need for moral norms and ethical and social considerations and design in a technical environment. It is important to underline that the ethical management of technology in this new environment will require more than the current ad hoc arrangements (i.e. some ethical considerations arise just at the end of the project, other ones are not noticed at all, solutions might vary among projects and can be addressed in different ways and by different people who not necessarily have the appropriate background, a lack of mutual understanding between ethical experts and technologists leaves room for error, it is no longer sufficient to address the ethical problems from a theoretical perspective if such approaches have no practical impact and remain external to the development of the technical project itself).

The ethics of co-responsibility - as opposed to an ethics of the individual role responsibility - in the field of scientific and technical innovation has to be addressed. This implies that the "technical" community has to meet the "ethical" community, which is typically separated because of the specialisation of high-level studying (e.g. universities) and where the "technical" study plan of engineers is very different from the "humanities" subjects of other faculties. A more interdisciplinary approach is strongly required. Researchers, project leaders, policy makers, project reviewers and stakeholders in general need guidance towards a coherent and cohesive approach to the integration of ethical consideration within projects that begins with the proposal design and continues throughout the project. This coherency is particularly important in view of the multi-cultural spread within and across Europe. Where projects incorporate the views of a broader group of stakeholders the ethical commitment and awareness-raising becomes extended beyond the project team to a wider community, promoting a participatory design and democratic inclusion in the development of technologies that will ultimately impact all citizens.

The EGAIS project - The Ethical GovernAnce of emergIng technologies: New Governance Perspectives for Integrating Ethics into Technical Development Projects and Applications – is funded by the European Commission (VII FP) to go beyond the current ethical limitations of technology: ethical knowledge will not have to reside only in the territory of specialised scholars ("ethicists") but will be "embedded" in any large technical projects. EGAIS analyses and suggests new forms of scientific and technical European project governance capable to produce the creation of ethically acceptable project outcomes, following the analysis of the way actual European project structure governance seeks to recognize and address ethical issues. EGAIS investigates how ethical considerations of governance could be integrated into the research and technology development culture of EU research, so that these considerations become a natural part of the evaluation and technical development process. It aims to provide to the stakeholders in general guidance towards a coherent and cohesive approach to the integration of ethical consideration within projects that

begins with the proposal design and continues throughout the project. In order to overcome the existing limits of current approaches to ethics, EGAIS intends to define an ethical framework harmonizing the theoretical, practical and governance perspective based on empirical findings that will be useful for decision makers, computer professionals, application designers and the society in general for analyzing, assessing and providing some guidelines when new technologies are developed, designed and deployed. In addition, the framework and the ethical guidelines will be crucial for the EU not only to define a common set of assessment criteria to evaluate any technical project from an integrated perspective of ethical analysis, but especially to evaluate the project efforts in addressing those issues by adopting a standardized approach that could overcome the problem of the cultural heterogeneity that is characteristic of the European Union.

The core of the investigation is the specific field of AmI technologies, which is used as the starting point of the research, whereas the ending point is the set of guidelines for AmI and other fields of technology. EGAIS scrutinizes some technological projects in several fields in order to assess their options as well as their advancement in terms of public debate, constitutional change, and technology and knowledge assessment. Given the wide impact of the ethical implications that arise from new and emerging technologies, EGAIS will actively take into consideration the insights, suggestions, relevant problems and feedback gained directly from key stakeholders, who emphasize three levels of interest: (i) those who finance IT projects (political level, i.e. policy makers); (ii) those who develop the output of IT projects (technical level, i.e. IT industry); (iii) those who use the output of IT projects (society level). In detail, they will benefit from the project for the following reasons:

- Policy makers, within the EU in the first instance, with the potential of broadening the reach to national level (certainly within the projects undertaken). As the notion of embedded ethical governance in IT projects permeates the technical scientific community the benefits are likely to be extended beyond those projects funded by the EU.
- Project leaders of technical projects, developers and the IT industry. Ethical issues arising from the use of technology can be understood as risks for the developers and vendors of technology. Developing measures that allow researchers to become sensitised to ethical questions and to address them can thus be seen as a risk management strategy of the IT industry in Europe and is of fundamental importance for the addressing of the relation between society and science above all when emerging technologies are concerned.
- The civil society, through enhanced technical projects that have been ‘ethically assessed’ before implementation.
- The European Commission and, in particular, the reviewers of projects in ICT programs. Governance mechanisms will provide EU commissioners and technical projects’ reviewers with clear guidance for conducting ethical reviews of existing projects and future ones.
- Academics, the scientific community and researchers in ICT and converging technologies, who will be guided through governance methods to better develop and manage ethical issues in their projects. Our project will present initial empirical findings relating to ethics in completed EU technical projects to illustrate more clearly, and in a practical way understandable to all those working in projects, our vision.

Theme 5: Legal aspects and privacy

Embracing the 'sousveillance state'

Danny Weston[1], Penders Jacques[1]
[1] Sheffield Hallam University (United Kingdom)

Surveillance has long been an issue for civil liberties advocates and technologists. A related concept, sousveillance (also known as 'Inverse Surveillance', and meaning ‘watching from below’) has received comparatively less attention as an ethical concept. This paper argues that the direction of technological, social and even economic development makes dramatic increases in the extent of both surveillance and sousveillance technologies inevitable and as a result, that we should focus our efforts on better understanding the sousveillance aspects and begin to discard surveillance.

The pace and deployment of advances in both surveillance and sousveillance is so rapid that technologies are now regularly outstripping the ability of national governments to effectively legislate for them. It is proposed that the legislature, locally, nationally and internationally will become increasingly out of touch in respect of these developments and is increasing danger of applying harmful legislation.

Because of this ‘policy gap’, a vacuum is created into which technologically focused ethicists now have an obligation to step. The paper argues that norms are more powerful than laws and that where legislation is made with reference to these technologies, it should be considered as a framework to work within rather than a definitive statement of morally appropriate behaviour. The rise of personalised, mobile data recording and transmission technology empowers millions of citizens and creates new ethical dilemmas, many involving the collision of two freedoms - freedom of expression and the right to privacy. The rapid spread and ubiquity of new applications also means many new and unanticipated behaviours are made possible (from, for example, ‘flash mobs’ to ‘happy slapping’).

An additional argument presented is that the current plethora of technology has led us, or is about to lead us, across a rubicon where the effective power lies in the hands of individuals and small groups rather than state bureaucracies to determine how technologies could and should be used. One of the constants in debates over recent decades seems to be the idea that the technology should change (or be limited), or the law should change. Everything it seems, should change, except us.

On the contrary, following the position that norms are more effective than laws, it is argued that we must embrace new ways of thinking about ourselves , our roles, identities and relationships with one another and with institutions in a way that fundamentally breaks with the past. This includes an inevitable blurring of the meanings of 'public' and 'private'. The movement inspired by notions of 'sousveillance', the primary subject of this paper, points the way to such new conceptions. It also introduces novel means of giving and requesting consent not possible or practical with ‘surveillance’. An argument is also made against increasing the surveillance capabilities of the state and security apparatus, pointing out instead that proper harnessing of ‘sousveillance’ (for example, through ‘crowdsourcing’) may in fact provide more practical and ethically sound techniques.

The capacity of sousveillance technologies potentially far outstrips the surveillance capacities of the state. And security services will not be able to maintain a monopoly on any new technology for long. Using the example of the U.K. An argument is made for a return to the 'Peelian principles' that formed the original basis of policing in the U.K., however this position is argued on the basis of creeping ‘sousveillance’.

Notions of privacy, as linked to private property, are also considered. In particular, differences are considered between the implications and impact of ubiquitous computing and wearable computing, where ambient intelligence is concerned as well as the role of machines effectively ‘watching’ us through complex data mining and pattern matching.

ICT that makes the difference

The future of Ambient Intelligence and ICT for Security

International Conference

22 – 25 November 2009

1000 Brussels Belgium

Sunday

Opening

Ambassador Room

19.00 - 22.00 and later...

Walking Dinner

Registration

Documents

Monday

	Excelsior Room	Ambassador Room	Bourgmestres Room
09.00	Welcome. Overview of the structure of the Conference (15 ')		
100 '	ICT, Health & Care 1 – Medical access to the human brain	Security & Biometrics 1 – Security in Danger	
10.40			
40 '	Rubinstein Room	Networking break	
11.20	ICT, Health & Care 2 – Health care and mental care	Security & Biometrics 2 – Emotional Biometrics	Legal aspects 1 – RFID. Implants and the human body
100 '			
13.00		Lunch – Le Jardin Indien	
14.20	The future of the internet – The Internet of X		Legal aspects 2 – Privacy. Toward an electronic identity
100 '			
16.00			
40 '	Rubinstein Room	Networking break	
16.40	Golden keynote session Golden Eurydice Award		
100 '			
18.20			
	Rubinstein Room	Reception	

Tuesday

	Excelsior Room	Ambassador Room
	Real and virtual 1 – Robotics. Keynote session	
	Real and virtual 2 – Robotics in daily life	Learning from Nanotech & Biotech
	Rubinstein Room	Networking break
	Real and virtual 3 – Disappearing interfaces	Technology, users and society 1 – Identifying new social issues
		Lunch – Le Jardin Indien
	Developing new research – Work in Progress	Technology, users and society 2 – Inclusion and exclusion
	Rubinstein Room	Networking break
	Open discussion Session Posters & Research Material (soft drinks, water, wine and beer are served)	

Wednesday

Excelsior Room

European Research Area and ESLA 1 – Activities & plans
Networking break
European Research Area and ESLA 2 – Lessons learned & Recommendations
Lunch – Le Jardin Indien

The Budapest Meeting

WePuble – Going Public with Science

Venue: Conference Facilities of Hotel Métropole 31, Place de Brouckère tel +32 1 217 2300

20091112