Smart Technologies and Privacy: Running a close race?

Ulrike Hug

University of Innsbruck, University Innsbruck Business School, Universitätsstraße 15, 6020 Innsbruck, Austria
ulrike.hugl@uibk.ac.at
http://www2.uibk.ac.at/ibf/man_acc/master.html?http://www2.uibk.ac.at/ibf/man_acc/uhugl.html

Abstract. Ubiquitous Computing (UbiComp) and smart technologies as next evolutionary stages are already on the way and are changing the game in a fundamental way: The ubiquity of processing and communicating power brings various advantages but also a great deal of risk. On the one hand "calm" computers and smart applications "understand" our operations and aims, and are used to facilitate and advance processes in business, at work, and in our everyday lives - on the other hand (perhaps) they allow third parties to monitor and search such data records concerning these matter. This article focuses in a first step on a range of specific of UbiComp-applications and connected technologies and based on this possible scenarios will be elaborated. In a second stage different facets of Privacy issues will be figured out. Concluding, in a third stage the results of a qualitative study with scientists and managers working in ICT-related fields will be presented. The results of this study are especially aiming on behavioural aspects such as (1) estimations of Privacy in connection with upcoming technologies such as UbiComp, (2) individual definitions of Privacy and important issues from a individual point of view, and last but not least (3) aspects of individual resistance to technological change. - "The most profound revolutions are not the ones trumpeted by pundits, but those that sneak in when we are not looking" said Mark Weiser in 1993. Therefore, especially due to increasing UbiComp-implementations individual resistance in connection with Privacy has to be seen as an important factor and should be monitored in the long run.

1 Introduction

In commerce, a trend towards mass communication can be identified which leads to "[…] flexible systems that ultimately can deliver individualised products and services […] The growth of the Web and e-commerce and a drive towards one-to-one market-

ing strongly favours and reinforces the possibilities of individuals to choose and even build their own preferred arrangements".[1] [1]

Focusing on the actual EITO (European Information Technology Observatory) Report [1] some results can be identified: A worldwide ICT market value in 2005 of 2,044 billion Euros and an increasing ICT market annual growth (2004 - 2006). The worldwide ICT market by region shows 2005 about 32,1% for Europe, 29,3% for USA, 14,5% for Japan and 24,1% for the rest of the world (see figure 1).

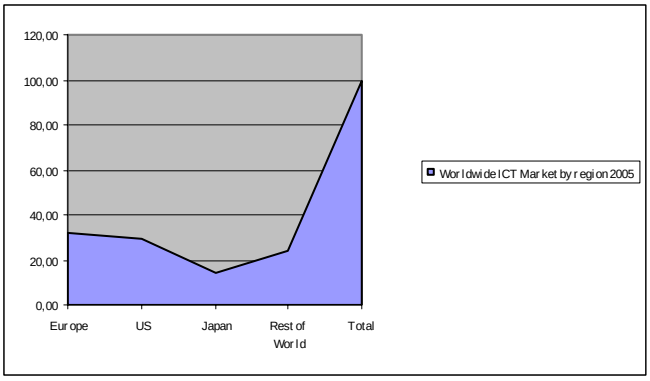

Fig. 1. Worldwide ICT Market by region 2005

Based on the mentioned EITO Report further prognoses can be identified: [1]

- The Web extends in the mobility area, to allow real-time access and responses to market needs.
- The Internet is more and more becoming the computing environment in the enterprise, and helping companies to achieve business processes integration – in this context Web services adoption is expected to become more ubiquitous/pervasive.
- The technology evolution in the enterprise is driven by speed (responding faster to changing business needs), performance, cost, capacity and mobility (improving servicing of employees/customers on the road).
- Mobile phones are the vast majority of access devices, with penetration of PDAs and smart phones still small. The latter are forecast to penetrate quite rapidly over the coming years, when many new handsets are set to appear that may not strictly quality as smart phones but offer the user much expanded scope in accessing content.
- In the PC domain a majority of business content is already distributed and accessed online and in the mobile world online content growth is supported by devices such as smart phones that allow web access and are gradually beginning to provide ac-

1 Different levels: hardware and software used, the personalized configurations within the platforms, selectivity within certain application areas (e.g. use of agents), and usage (e.g. belonging to a virtual community).

ceptable user experiences. In fact, much improved mobile access to business online content is a major growth driver in this area.
- To summarise, one key driver of increased business use of online content is to enable ubiquitous access to online content, “anytime, anywhere”.

2 Ubiquitous Computing Applications and Scenarios

The basic concept of Ubiquitous Computing (UbiComp) leads back to Mark Weiser (1988), who demanded, that the human environment should not be mapped in a computer (Virtual Reality), but the computer should be hidden in the habitual environment (Calm Technology): Technology, as a means to an end, has to take a back seat. In the vision of UbiComp, people are surrounded by a multiplicity of microprocessors, sensors, “memories” and necessary energy sources. All equipment with enclosed microprocessors and sensors is ubiquitous/pervasive and “intelligent/smart”.

With a future “ubiquitous e-world”, the accessibility of persons will obtain higher significance. [2, 3] Computing is no longer a discrete activity bound to a desktop: network computing, mobile computing together with the Internet is rapidly becoming a part of everyday life. Rather than being an infrastructure for computers and their users alone, it is now an infrastructure for everyone.

The aim of Ubiquitous Computing, is computing availability wherever required, which in other terms means, a spread of “intelligence” and connectivity to more or less everything. In a “ubiquitous world” objects like books, tickets, ships, aircrafts, cars, bridges, door handles, tunnels, machines, refrigerators, lighting fixtures, shoes, hats, packaging clothing, appliances, tools, homes, offices and even things like coffee mugs, “learning environments” and the human body (“wearable computing”) will be embedded with chips, to link together an infinite network of other devices and to create an environment, where the connectivity of devices is integrated in a way that is unobtrusive and always available.[2]

Therefore, UbiComp refers to the emerging trend towards numerous, easily accessible computing devices that are connected to an increasingly ubiquitous network infrastructure. "Tools" are a new class of intelligent, portable devices that allow the user to plug into powerful networks and gain direct and simple access to both, relevant information and services. Though, UbiComp devices are not personal computers as we tend to think of them, but very tiny - even invisible - devices, either mobile or integrated in almost any type of object imaginable; all communicating through increasingly interconnected networks.

A smart environment is one that enables the acquisition and application of information and knowledge about persons and their surroundings, and also adapts to improve their experience. Based on an UbiComp-vision this means saturation with

---

2 Presently, numerous forms of UbiComp-applications (for example in the supply chain, production processes, health care, clothing, homes etc.) are implemented in various business processes. In addition, companies like IBM, Siemens, HP, Rank Xerox, SAP, Microsoft, Metro, Infenion et al. are working on sequences of a “ubiquitous world” in the future.

computing and communication capabilities to make intelligent decisions in an automated, pro-active and context-aware manner. [4]

In the vision of Wearable Computing, computers are not only a machine to carry with us, instead, they will be an integral part of our every day outfit, and any-time operational and equipped in order to assist us in dealing with a wide range of possible situations. Each component of the system is miniaturized and worn as close as possible to the part of the body using it. So, the wearable perspective suggests that instead of putting sensors and cameras in the room put them on the person.

This year, several conferences are dealing with special fields and respectively with the connection of "Wearables" and Ubiquitous Computing (UbiComp).[3]

An example of "Wearables" is shown in figure 2 [5]: The maintenance wearable includes a vest housing the computer and accessories and in addition a data glove with sensors for interaction. "The vest was designed to house all components of the wearable expect the data glove, which is worn separately." The wearable system consists of the following components: MicroOptical HMD (Head Mounted Device) with controller box and battery, a Personal Computer (OQO, smallest tablet PC) with built-in touch screen with pen input, and a Bluetooth keyboard. The PC and the HMD are connected by a wire, the keyboard connects wirelessly. The PC is worn on the body and its internal display is not visible. A part of the vest is partially detachable.

Fig. 2. Vest with PC (OQO), Head Mounted Device (HMD) and Keyboard

Based on a case study with a major aircraft manufacturer Nicolai et al. identified a (future) application for a maintenance worker (see figure 3) [6]: The worker is equipped with a PDA and a HMD. The PDA is worn on the belt connected with the HMD. A special input device is worn around the wrist and enables interaction with the PDA and is also used for the localization of the worker. There exists a possible

[3] See for example "Intelligent Environments", Artificial Intelligence Grooup, Saarland University (May 2006); "MobiQuitous 2006" (The Third Annual International Conference on Mobile and Ubiquitous Systems – Computing, Networking and Services), San Jose, California (July 2006), etc.

switch from wearable mode to handheld mode in case of detachment of the PDA by its holder. The toolbox of the worker is enhanced by a notebook computer to store experience data. Wireless connections are used where possible. For localization there are fixed FRID tags in the cabin, a wearable RFID reader on the wrist of the worker and a mapping table between tag identifiers and corresponding aircraft parts.

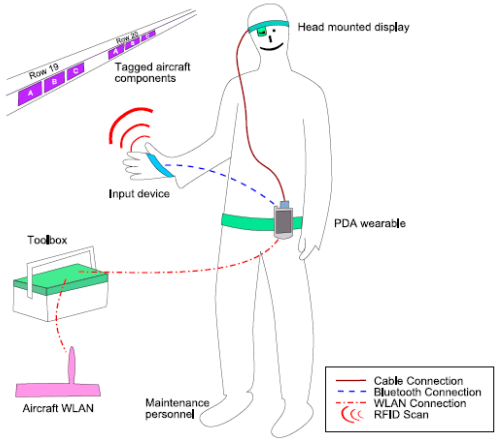

Fig. 3. Maintenance Worker with "Wearables" [6]

Beside "Wearables" another scenario for (future) RFID-driven applications in supermarkets can be mentioned: The example of "The Metro Future Store" (Rheinberg, Germany; www.future-store.org, see figure 4). At the CeBit 2006 the Metro Group presented together with several business partners applications of RFID-technology in retail and logistic processes (since 2004). According to this first presence at the CeBit the Metro Group wanted to test acceptance and usability issues of (potential) customers. All companies working in cooperation with Metro share a common vision: setting new technological standards in retailing and supporting the modernization process of the industry on a sustainable basis. In the meantime, numerous partners in the consumer goods industry equip their pallets intended for the Metro Group with RFID transponders (Procter & Gamble, Henkel, Johnson & Johnson and Esprit). Worldwide several other major international retail companies including Wal-Mart, Texco and Albertsons are investing in RFID. EPCglobal4, an international organization dedicated to coordinating RFID deployment in the consumer goods and trade sectors, is in charge of defining standards. In Germany, EPCglobal is represented by GS1 Germany. In cooperation with trade and industry companies, the Metro Group is working to establish the EPCgloabl Electronic Product Code as the binding worldwide standard.

[4] EPC = Electronic Product Code

Fig. 4. Future Store of the Metro Group in Rheinberg (www.future-store.org)

At present, there exist several other examples of RFID-applications:

- Libraries, e.g. www.buecherein.wien.at, Vienna (all lending media are equipped with RFID transponders)
- Football World Cup 2006 (FIFA World Cup), Germany (to apply for a ticket someone has to give his name, address, nationality, which team he wants to support and bank details – in addition ID or passport number and birth date; This enables authorities to check the ticket against someone's passport.)
- Museums, e.g. www.naturhistorikmuseum.dk, Denmark (By means of a PDA, visitors can access the museum's database, and call up background information on the exhibits etc.)
- Applications for an efficient collection of toll fees (e.g. in Austria), in Healthcare (patients receive RFID bracelets with integrated transponders in which their patient numbers are stored), in air traffic (baggage handling etc.), in genetic research (RFID transponders and readers monitor the growth of genetically modified trees) etc.

3 Study Results concerning Privacy Issues

Many UbiComp-applications raise questions in terms of security, privacy, maintenance, etc. Ambient, intelligent and smart environments are creating a new "quality of privacy". Consequently, existing and upcoming technologies are rapidly changing our life, but also provide a dramatic challenge to traditional ethical postulates.

Westin [7] defined Privacy as "the claim of individuals […] to determine for themselves when, how and to what extent information about them is communicated to others." Langheinrich argues: "...In an environment containing countless, invisible sensors that constantly monitor their surroundings and communicate their findings to each of their peers, both, real-world and virtual transactions are certain to find their

way into sheer limitless data storage systems, to be saved forever and recalled at a moment's notice." [8]

In 1980 the OECD published "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" [9]. These principles (e.g. collection limitation principle, use limitation principle, individual participation principles etc.) have also been the basis for the EU Directive 95/46/EC [10]. For example, article 6 of the Directive requires data collectors to collect only as much information as necessary (also called the proportionality principle or the principle of data minimization) while article 7 requires them to obtain the unambiguous consent of the data subject before the collection." [11]

In general, there can be identified some specific aspects and questions for further research of "e-privacy": [12]

- Anonymity: How to protect personalised data (if necessary)?
- Confidentiality: How to assure that unauthorised third parties have no access to data (during and after contextual data transfer)?
- Transparency*:* How to be sure what aspects of personal data (e.g. of learners, managers, employees etc.) are monitored and analysed at what time and under what circumstances (reason of monitoring, duration of data storage, audience of data, etc.?)
- Trust and coverage: Can learners have trust in conditions and pacts (reason and coverage of data connection and receivers of data)? Is there help in case of conflicts (in organisations, in the public sector)?

A research study concerning "New Technologies and Privacy" with the following target groups - (IT-) Managers and professors of universities and Fraunhofer Institutes - was conducted by the author. First results of 10 qualitative interviews show that privacy is an important issue of middle-aged and older people.

What estimations do interviewees have in connection with upcoming technologies such as Ubiquitous Computing (UbiComp)?

Interviewees see some of the largest risks in a (unnoticed) connection of (personal) data, the authority about their data and partially fear of questions like "Who is holder of my data – in what quality (data quality and quality of security) and in what range and profoundness?" (transparency and trust). Further critical questions are: "What influence does exist due to another usage and a (possible) cancellation of my data?" (highness of data). "Who could help in case of a necessity of a cancellation of wrong or old data and what (possible) resentments could occur of (public) authorities etc.?" ("ombudsman" in case of need).

A special data protection is demanded by interviewees due to individual financial and health data. Concerns are seen especially in case of data combinations/consolidations (unseen profiling/monitoring and utilization). Last but not least interview partners see a dangerous development towards "big business of personal data" (e.g. in marketing-related business) and "overruled ethical issues".

Some statements: "Privacy protection is a question of trust. Trust is a very important issue. For example banking houses are conservative and more confidentially than

for example service providers in telecommunication […] But: Trust can be gambled away with only one privacy occurrence – especially, if there has been an occurrence, an organisation is not allowed to brush it under the carpet – the organisation would have to communicate it: There was that occurrence, and we will do our best to avoid it in the future." And: "In the future – in about 10, 20 or 30 years - we will have two categories of persons. Firstly, persons who are prepared to loose their privacy – that will be mainstream trend and they will live without any privacy. The second group will go down and exist on an after market – they have to organize themselves, whatever way they are going do it. That means, they will have to struggle for survival. […] In the future, people could be in an extortion situation: 'If you do want to have privacy, you won't get an employment.' Further technical developments also will have serious consequences for insurance companies, for computer business (ICT) etc."

How do interviewees define their (individual) privacy? And: What about (further) individual resistance of interviewees?

Some statements:

- "Privacy means for me to be 'owner' of my data."
- "Privacy means for me the protection of my data against unauthorized access and storage."
- "Privacy means for me a sensible information-handling – I have to make sure an avoidance that data can appear in several and other context […] I should have the possibility to control my data." And: "In the meantime, I am very careful with my data. I always ask myself: Why do they need my data, for what purpose? If someone is not able to say me intelligent reasons for that, I do not give my data away."
- "I want to know what happens with my data and – if I have influence on it – to know who gets my data. I would like to have the possibility to cancel my acceptance of my data storage."
- "Data like my name, my residence, and data of my business card are public. But there are also things such as depts – this data have to be secure. My neighbor has not to know something about my financial situation. There is a clear individual border."

Adam Sarner, analyst of Garnter, spoke in an interview of "Privacy as 'creepiness factor'". For best practice implementations of ubiquitous computing-applications in the future responsible technicians and specialists are rely on feedback of (potential) users of applications. It is necessary to create a balance between a technically- and financially-oriented approach and also an approach which makes sure that data protection and acceptance is considered.

References

1. EITO 2004: European Information Technology Observatory Report 2004 (2004)

2. Pfaff, D., Skiera, B.: Ubiquitous Computing – Abgrenzung, Merkmale und Auswirkungen aus betriebswirtschaftlicher Sicht. In: Britzelmaier, B., Geberl, St., Weinmann, S. (eds.): Wirtschaftsinformatik: Der Mensch im Netz – Ubiquitous Computing. Teubner, Wiesbaden Stuttgart Leipzig (2002)
3. Fleisch, E.: Von der Vernetzung von Unternehmen zur Vernetzung von Dingen. In: Buhl, H.U., Huther, A., Reitwiesner, B. (eds.): Information Age Economy. Physica-Verlag, Heidelberg (2001)
4. Cook, D., Das, S.K.: Smart Environments: Technology, Protocols and Applications. John Wiley, New York (2004)
5. Nicolai, T., Sindt, Th., Witt, H., Reimerdes, J., Kenn, H.: Wearable Computing for Aircraft Maintenance: Simplifying the User Interface. 2nd International Forum on Applied Wearable Computing, ETH Zurich (17 – 18 March, 2005).
6. Nicolai, T., Sindt, Th., Kenn, H., Witt, H.: Case Study of Wearable Computing for Aircraft Maintenance. 2nd International Forum on Applied Wearable Computing, ETH Zurich (17 – 18 March, 2005).
7. Westin, A.: Privacy and Freedom. Atheneum, New York (1967)
8. Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. Paper presented at Ubicomp 2002, Göteborg, Sweden (October 2002, 1)
9. OECD: Fair Information Practices (FIP). Recommendation of the Council concerning Guidelines govering the Protection of Privacy and Transborder Flows of Personal Data (23rd September, 1980)
10. European Union: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)
11. Floerkemeier, Chr., Schneider, R., Langheinrich, M.: Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. Paper presented at the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan (November 2004), used version: 2005, 2
12. Mattern, F., Langheinrich, M.: Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller, G., Reichenbach, M. (eds.): Sicherheitskonzepte für das Internet. Springer, Heidelberg (2001) 8-10