IRIE
International Review of Information Ethics Vol. 8 (12/2007)

Jessica Heesen and Oliver Siemoneit:

Opportunities for privacy and trust in the development of ubiquitous computing

Abstract:

This article deals with the technical genesis of ubiquitous computing and the opportunities for social participation in the development of technology. In this context, the ability of the system to protect the private sphere is identified as one of the most important criteria for a socially acceptable constitution. On the basis of the relationship between privacy and freedom, it is shown that the trust necessary for the social establishment of global IT networks is only developed through the preservation of the freedoms of choice and action.

Agenda

Authors:

Dr. Jessica Heesen

Institut für Philosophie, Universität Stuttgart, Seidenstrasse 36, D-70174 Stuttgart
☎ +49- 711 - 6858 2491; Fax: +49 - 711 - 6858 2492; ✉ jessica.heesen@philo.uni-stuttgart.de .

Dipl.-Kfm. techn. Oliver Siemoneit

Institut für Philosophie, Universität Stuttgart, Seidenstrasse 36, D-70174 Stuttgart
☎ +49- 711 - 6858 2491; Fax: +49 - 711 - 6858 2492; ✉ oliver.siemoneit@philo.uni-stuttgart.de

Introduction

The topic of ubiquitous computing is a matter that, nowadays, is foremost in people's minds and enjoys a great deal of attention from research and professional practices. Above all, the media and consumer protection agencies have urged the risks and problems of the so-called RFID chips (Radio Frequency Identification) to the foreground of the discussion by treating them as forerunners to the technological vision. Many promoters and developers of this new technology are, therefore, complaining that social discussions exhibit a tendency to overemphasize the negative aspects and to extensively suppress the utility values. For many technical developers, it is, therefore, quite clear that a relationship of trust with selected user groups needs to be consciously developed so that the perception of this problem can be influenced and changed. The goal of the article at hand is to exhaustively discuss the desirability, possibilities, and limitations of this concept of trust management.

Technology development and social participation

Disputes about technology development are common practice in our modern society. This usually results in big, public debates about the manifested i.e. anticipated possible resulting consequences of technical artefacts and systems. From these debates, it is clear that not only the assessment of the consequences of mechanization but also the evaluation of its concrete technical advantages and induced social and socially structured effects diverge widely from one another. What counts as a contribution to the modernization of society for the one, is seen for the other as a step towards cultural decadence, massive unemployment, social coldness, and ecological catastrophe. Most of the controversies about technology are primarily not only about the technology itself but, above all, about the question of the development perspectives of the society in which we live: What kind of world do we want? What are our values, goals, and ideals? Which developments are extracted from these, and which are acceptable?

Toward the end of the 1980s and the beginning of the 1990s, the sociological research of technological genesis contributed significantly to destroying the idea of a traditional, uninfluenceable, quasi-self-propagating technological development and to replacing it with the model of „technology as social process“. Technological genesis is conceived of as a process that takes place in several different phases which, at each stage, is carried out by a different constellation of agents. In accordance with a theory of a self-organized social network, strategic, social agents associate their plans of action with one another so that stable, cooperative relationships that facilitate the production of socio-technological innovations are produced. With statements like, „In the future, our world will be equipped with a multitude of the smallest sensors and wireless communicating ICT-Systems„, and „the introduction of RFID has reached a point of no return“, the promoters of a technology create, similar to a self-fulfilling prophecy, a guideline for an individual action to which the aura of a certain inevitability attaches and which pushes towards its own realization and, in a structure building and altering manner, acts on social relationships.

Technological development as a social negotiating process is, according to Johannes Weyer, characterized by varying agent constellations and lines of confrontation, specific challenges and difficulties:

- Genesis phase: A group of loose, combined individuals create a technological vision through the free play of imagination and without consideration of the structures in demand. Concrete users are not yet in sight here.

- Stabilization phase: The transition from the building stage to systematic technological exploration is reached through the addition of strategic, social agents who, despite their different orientations, have a common interest in carrying through the advised technological project. Through the coupling of diverse, heterogeneous plans of action, a stable, social network is created which makes the development of prototypes and further research possible.

- The implementation phase: In the delicate phase of the implementation of a technology, the functioning applications under laboratory conditions need to show that the technology also functions outside of the support networks. Through extensively applied pilot attempts and demonstration projects, the new technology should prove its effectiveness and concern itself for the credibility and acceptance by its users. Thus, the implementation phase proves itself to be especially delicate because a variety of conflicting interests need to be integrated through the expansion of the relevant agents with potential users and concerned parties. The neuralgic point here is to identify a specific number of useful implementation classes for technology users which lift the project above a critical threshold beyond which a technological development with its own momentum is possible and it is possible to speak of a success or breakthrough or perhaps an effective, technological innovation.

In recent years, a certain technology in its implementation stage is especially making headlines: the so-called 'Radio Frequency Identification' technology, in short: RFID technology, whose history began in the industry under the banner of Transponder Technology toward the end of the 1980s but whose origins can actually be traced back to the 1940s in the military realm. But only the rapid progress in material-, nano-, and microsystem technology in the past years made Transponder dwindle to a manageable magnitude and to approach an affordable mass-application. Especially in the course of discussions on the so-called ubiquitous and pervasive computing and also the ambient intelligence which propagates a dramatic integration of information and communications appliances, in short ICT-Systems, in our world, RFID technology enjoys high attention as an important enabler and forerunner of this vision.

The implementation phase of RFID technology proves itself, above all, to be difficult in the final consumer stage and is met with considerable controversy by users, data security engineers, and citizen organizations. Thus, the implementation phase, as the critical phase in the life cycle of a new technology, determines its future success: pilot projects should immediately put the performance of a new technology to the test, push through an integration of this new technology in the existing market and create new infrastructures of demand. The large-scale pilot projects and demonstrations have, however, not carried this out but, rather, have let loose an enormous shared refrain and fomented massive concern regarding its social desirability given the damage to jobs or the threat to data security and consumer sovereignty in the form of the creation of consumer and movement profiles, individual pricing and intensive advertisement, and one-to-one marketing. The social negotiation process of the technological configuration that has gotten underway threatens to tip over, from the perspective of the promoters of the RFID technology, so that the critical threshold which makes a self-perpetuating market possible is not longer reached. This in turn threatens a restriction in the area of commodities-logistics because the especially lucrative market of the final consumer realm cannot be made available due to these objections against the technology.

As already discussed, technical controversies during the introduction of a new technology are unavoidable because, exactly at the implementation phase of a technology, varying interests of social groups conflict with one another and need to be reconciled in a social negotiation process. The current discussions on the social tolerance of RFIDs and of ubiquitous computing are, from this perspective, typical of the phase and are to be deemed welcome because, alongside the uncontroversially present utility potentials, the important side-effects and negative consequences are now also coming to light. The safeguarding of personal freedom rights but also the protection of other so-called option- and liability values create, through this, the main focal point of contention. In this context, a key position accepts the protection of the private sphere, which is valued differently in the realm of this discussion: statements like „Forget privacy“ or that privacy constitutes a repetitive, content-less concept in the western societies of the 21st century – are definitely extreme positions but they are, nevertheless, positions which, in the course of uncertainties due to international terrorism in recent times, are nurtured and are considered absorbing to discuss.

The changing and safeguarding of the private

The determinings of the private realm are results of the social development process which are fundamentally open to the practice of social discourses and of a general decision-making. The use of the applications of Context-Aware and ubiquitous computing demands the preparation of personal data and many applications aim at the protection of everyday activities and, through this, of the information-technological permeation of the private sphere. A social acceptance of these technologies is, due to their utility value, thus pitted against the problem of acceptability based on higher ranking ideals such as personal autonomy and the ability to take action. Liberal social orders ascribe a high significance to the protection of the private sphere, especially because the safeguarding of a private sphere is a necessary precondition for the protection of a freedom to take action. The private sphere offers, furthermore, the possibilities for personal retreat, rebound, for leisure as well as for the experience of individual unreachability. Only in a realm that is extensively protected from heteronomous conditions can that spontaneity and unbiasedness of behavior be cultivated which is tied to the concept of freedom of action.

Three different forms of privacy are commonly distinguished. a) Decisional privacy which refers to the level of freedom of decision. b) Local privacy which has to do with the protection of living quarters and of residence information but also with the safeguarding of corporal integrity. c) Informational privacy which describes the protection and control of person-related information. Consequently, the effects of ubiquitous computing on the understanding and protection of the private are structured into these three parts.

Decisional privacy: ubiquitous assistance or control through ubiquitous computing?

The integration of sensors, PDA's (Personal Digital Assistants) and internet connections in our everyday life provides our surroundings, at least in our psychological perception, with the character of a social counterpart. The context appears as the generalized Other which confronts us as partner, assistant but also as spy. In the further development of network communications as „Internet of Things“ , this effect of ubiquitous observability is turned into something positive and is considered acceptable as a ubiquitous assistance. Out of the connection between control and assistance in an intelligent environment, parasocial interaction-forms of media users are to be expected which not only induce discipline-effects but also bring about behavioral changes in a „positive“ way, through free choice. This means that technologically anthropomorphic behavioral patterns increase and that a medialized, intelligent environment appears as a virtual reference group according to which the individual models his or her behavior. For the level of the freedom of decision (decisional privacy), this means that decisions are increasingly made as a reflection of the reaction to a technological system.

Local privacy: the severance of the local

Drawing borders between public and private residence areas is becoming increasingly difficult. Locator services (such as „Friend Finder“) allow the discovery of individuals in the most diverse situations. Residence areas do not proffer a clear separation between private and public spheres anymore.

Ubiquitous computing scenarios make plain that, in this context, the trend is towards the further penetration of a more public private and professional world. The awareness of geographical independence in the undertaking of a job and of the never-actually-effected, temporal ending to a work-day can call the perception of the private sphere as an autonomous and unreachable component of human life into question. At the same time, strategies to pull oneself out of the immediate communication-context while simultaneously satisfying one's need for availability/communicability are already familiar. The new communication (online) relationships make possible a proxy representation of the individual (the digital Me, the avatar), which helps to manage a part of the communication problem. The ideal of constant reachability is modified into a realization of a spatial and temporal internet presence. „The telematic networks release us from the pressure of existence by their existence alone“ claims Stefan Münker.

The residence also changes its persona as the embodiment of the local private sphere in the age of everyday information technology. The intelligent house technology connects the home with the World Wide Web and also with the supermarket around the corner. Smart-Home scenarios conceive of the private residence area as a place of integration in the extra-domestic realm (the home as the center of integration) . Thus, the scenarios outline a concept for living, that distinguishes itself from several conceptions that have been passed down, about the role of the house for the psycho-social experience. Until the middle of the 20th century, the house was perceived as a decidely not-public and as a familiar realm. The maintenance of local privacy corresponded with the image of the individual as someone who was divided into a public and a private person. But these role definitions are becoming increasingly invalidated. Even the concept of one's body as the most intimate locale of private availability can, in ubiquitous computing, become a component of data transfer. Health information and so-called vital statistics are becoming controlled and institutionally utilized to a large extent, in accordance with scenarios for the information-technological future optimization of public health. Thus, the domestic environment offers innumerable possibilities for automatic health tests and recommendations (measurements through the lavatory and the mirror, control of the purchase of food products, etc.).

Informational privacy: own data protection as a report

From the acceptance and dissemination of private homepages, cell phones, and other utility options from the Web 2.0 as well as from the widespread lack of concern in the realm of data security, it can be understood that the traditional protection of the personal private sphere has, in general, lost all meaning. As has already become clear with respect to local privacy, the separating line between public and private depends increasingly on the responsibility of the concerned persons (own data protection).

The free and individualized relationships with informational and media technologies frequently stand in contradiction to the right of the individual to privacy and informational self-determination. The realization of a right to informational self-determination seems hardly possible given the flood of personal data whose collection and transmission are indisposable for the functionality of applications. Precisely because, within the perspective of the guiding idea of ubiquitous computing, the individual is supposed to be the focal point, personal data are of high relevance in several applications. The maintenance of social relationship networks stands at the center of many considerations for a networked world. But exactly this connection between interactive user possibilities and the organization of relationship networks and self data protection produces new problems with respect to informational privacy.

Community platforms and information systems facilitate the uncomplicated and constant absorption of contacts for people from specific social relationship networks or also for strangers who learn about one another only through their shared interests. In this context, the locator service is of prominent importance. It gives information about the residence areas and, thus, about very sensitive data over which the concerned individuals, in claim of their right to informational self-determination, want to have autonomous control. A necessary precondition to this self-determination is, however, the assessment, classification, and indirect, external evaluation of the relationship qualities within the respective information systems. For individuals from familiar, friendly or professional relationship networks, the glimpse into their residence areas is protected in accordance with personal system pre-settings or is denied and is restricted to specific areas (for instance, the location within the office sphere could be allowed but queries beyond that be rejected). Through the protection or restriction of location queries, the concerned individuals in a personal relationship network indirectly leave behind a representation of their personal network relationships – the social subtext of their user settings – which itself has a reciprocal effect on the formation or establishment of relationships.

Also generally acknowledged in information technology imbued worlds: even technologies for the „anonymisation“ or „pseudonymisation“ of identities don't prevent strategies of personal data administration from becoming an essential component of external or individual safeguarding. Self/Own data protection is already a problem in anonymous communications networks in view of the competence of the individual to protect herself and also with regard to the technical and legal implementations of such strategies. In social networks, however, the own data protection can become problematic insofar as it reports ex-negativo on the behavior and preferences of the respective user.

The maintenance of optionality as a precondition for trust

From the preceding remarks, it is clear that: only the formation of utility options which allow the individual to freely decide about the form and extent of the private sphere can build a proportion of trust which is the precondition for the acceptable and enduring social use of ubiquitous computing applications. Such utility options expand into three preconditions: 1. The preparation of mature systems for the guarantee of data protection and security, 2. the increasing of user-autonomy through the enhancement of user-competence (transparency on demand, parallel communication), 3. the option to not participate in the use of comprehensive IT systems but, nevertheless, to not be closed off from relevant service facilities and information.

The idea of a directed trust management is to be rejected from a technological-ethical perspective. In any case, trust is hardly intentionally producible: trust is not implementable, and cannot be bought, ordered, learned or taught – but, rather, can only be supported as the characteristic of an attitude. Trust is not something that can be produced monocausally („Trust!“), cannot easily be summoned but is, instead, much like happiness, potentially „only“ the valuable side-effect of actions which are undertaken for a different purpose. This does not mean that trust is not amenable to certain implementation technologies. Yet, the transition from „formally trustworthy“ to „factual trust“ is always a gift and, due to its complex pre-conditions and conditions, is, in any case, hardly organizable.

References

Bohn, Jürgen, Coroama, Vlad, Langheinrich, Marc, Mattern, Friedemann, Rohs, Michael (2003): Allgegenwart und Verschwinden des Computers - Leben in einer Welt smarter Alltagsgegenstände, in: Grötker, Ralf (2003, Pub.), Privat!, Hannover, pp. 195-245

Feltes, Karin (2006): RFID-Chips: Geniale Erfindung oder Big Brother?, http://www.ard.de/ratgeber/special/rfid-chips/-/id=322978/nid=322978/did=320270/152dt16/

Fleisch, Elgar und Mattern, Friedemann (2005, Pub.): Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Berlin/Heidelberg 2005.

FoeBuD (2003): Positionspapier über den Gebrauch von RFID, http://www.foebud.org/rfid/positionspapier

Gesellschaft für Informatik (2005): Sachverständige der Gesellschaft für Informatik warnen vor möglicher Überwachung der Bevölkerung durch RFID-Chips, http://www.gi-ev.de/presse/pressearchiv/sachverstaendige-der-gesellschaft-fuer-informatik-warnen-vor-moeglicher-ueberwachung-der-bevoelkerung-durch-rfid-chips/

Heesen, Jessica (2007): Strategien für einen selbst bestimmten und freiheitlichen Umgang mit allgegenwärtigen Kommunikationsdiensten, in: GI (2007, Pub.): Informatik trifft Logistik. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e. V. – Proceedings 110 (2007), Band 1.

Hubig, Christoph (1995): Technik- und Wissenschaftsethik. Ein Leitfaden, Berlin/Heidelberg/New York 1993, 2. Version. Aufl. 1995.

Hubig, Christoph und Siemoneit, Oliver (2007): Vertrauen und Glaubwürdigkeit in der Unternehmenskommunikation, in: Piwinger, Manfred / Zerfaß, Ansgar (2007, Hrsg.), Handbuch Unternehmenskommunikation. Wiesbaden 2007.

Mead, George Herbert (1934): Mind, self and society. Chicago/London 1934.

Münker, Stefan (1997): Was heißt eigentlich: "Virtuelle Realität?", in: Münker, Stefan/Roesler, Alexander (1997, Pub.): Mythos Internet. Frankfurt a. M. 1997, 108 – 131.

Rössler, Beate (2001): Der Wert des Privaten. Frankfurt a. M. 2001.

Siemoneit, Oliver (2007): Context-Awareness und rationale Risikowahrnehmnung, in: GI (2007, Pub.): Informatik trifft Logistik. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e. V. – Proceedings 110 (2007), Band 1.

Spiegel (2005): Unweltschäden durch Funkchips?, in: Der Spiegel 50/2005, p. 150

Thiesse, Frederic (2005): Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung, in: Fleisch, Elgar / Mattern, Friedemann (2005, Pub.): Das Internet der Dinge: Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Berlin/Heidelberg 2005, 363 - 378

Weyer, Johannes (1997): Konturen einer netzwerktheoretischen Techniksoziologie, in: Weyer, Johannes (1997, Pub.), Technik, die Gesellschaft schafft: Soziale Netzwerke als Ort der Technikgenese, pp. 23 - 52

Wiegerling, Klaus (2007): Das Stuttgarter Konzept der Parallelkommunikation, in: GI (2007, Hrsg.): Informatik trifft Logistik. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e. V. – Proceedings 110 (2007), Band 1.