Online Version. This article was originally published in “Poiesis and Praxis”
(URL: www.springerlink.com/link.asp?id=109376)

The original publication is available at http://www.springerlink.com

Technology Paternalism – Wider Implications of Ubiquitous Computing

SARAH SPIEKERMANN

FRANK PALLAS

Ubiquitous Computing technologies will have a wide impact on our daily lives in the future. Currently, most debates about social implications of these technologies concentrate on different aspects of privacy and data security. However, the authors of this paper argue that there is more to consider from a social perspective: In particular, the question is raised how people can maintain control in environments that are supposed to be totally automated. Hinting at the possibility that people may be subdued to machines' autonomous actions we introduce the term “Technology Paternalism”. We elaborate a working definition and illustrate the concept by looking at different examples based on current and future technology. We also dwell on the impacts of ubiquity and control of technology and suggest some approaches to assure a reasonable balance of interests such as a general “right for the last word”.

Ubiquitous Computing

„Ubiquitous Computing enhances computer use by making computers available throughout the physical environment, while making them effectively invisible to the user” (Weiser, 1991). With this definition Mark Weiser became a founding father of a new wave of research and development, namely in the area of Ubiquitous Computing (hereafter: Ubicomp). Some scholars also refer to this domain as Ambient Intelligence or Pervasive Computing.

According to Lyytinen and Yoo (2002), Ubiquitous Computing combines two major trends of computer science: First, the embeddedness of computing systems and second, their mobility.

Embeddedness means that every-day objects will integrate sensors and auto-id technology, such as RFID, which are used to enhance the functionality of objects. This embedded ‘intelligence’ gives objects the capability to obtain information from the environment and utilize it to dynamically respond to detected outside conditions. An example for such responsive behaviour are sensor enhanced cars which register driving speed and match this information with roadside speed limit signs. Based on this matching operation the car then deducts (computes) autonomous actions (output). For example, it

adjusts speed to traffic regulations. Such actions may be performed silently in the background and without any user interference (the driver of the car) or explicit user attention. The principle of silence and autonomy is often referred to as the principle of "calmness" (Weiser and Brown, 1996).

Mobility, in contrast, implies that computing services are able to physically move with us. Thus, personal data, preferences and services do not exist redundantly any more on multiple devices and with different settings, but are available seamlessly to us, anywhere and any time. For example: accessing one's e-mail can be done in the car in the same way as on one's home PC. Settings and data are available in the same way. Merely the interface is a different one.

The present article mostly resides on Ubicomp's first characteristic, the embeddedness. Embeddedness is realized with the help of two major technologies: radio frequency identification (RFID) systems and sensor networks. These two technologies give objects their ability to sense and respond to their environment, notably also to sense and respond to people.

Privacy is impacted if objects and sensors monitor our every-day actions. As a result of this ability, sensor networks and especially RFID have stirred a strong debate recently on privacy and security implications (Pohl, 2004). Yet, pervasive monitoring and the loss of information's natural ephemeral nature (Palen and Dourish, 2003; Bohn, Coroama et al., 2004) are not the only social threats inherent in Ubicomp environments. As Mark Weiser pointed out in his famous article on the computer of the 21st century: "The [social] problem [associated with Ubicomp], while often couched in terms of privacy, is really one of control" (Weiser, 1991).

Control is a construct that is tightly intertwined with privacy. Typically, scholars tend to view privacy as a means to 'control access' to the self (Altman, 1975; Margulis, 2003). With a view to Ubiquitous Computing, privacy related access control has been defined as "... the belief of a person in the electronic environment acting only in such ways as explicitly allowed for by the individual" (Spiekermann, 2005). Yet, in this article we want to focus on another aspect of control in Ubiquitous Computing. Specifically, we want to expand on the question ***who controls who*** in intelligent environments and ***how*** intelligent objects should actually be allowed to respond to people and situations (and thus ***exercise control***).

On the background of this research question we identify a potentially devastating effect of Ubicomp which we call 'Technology Paternalism'. On a high abstraction level Technology Paternalism has been defined as the fear of uncontrolled autonomous action of machines that cannot be overruled by object owners (Spiekermann and Ziekow, 2004). The concept was identified in a number of focus groups conducted at Humboldt University Berlin where persons with different backgrounds discussed RFID-based technologies and their future uses (Berthold, Günther and Spiekermann, 2005).

The goal of this article is to deduct and establish the term 'Technology Paternalism'. For this purpose, we first take a look at the concept of 'paternalism' and its existing definitions. Thereupon we deduct the concept of *Technology* Paternalism and apply it to Ubiquitous Computing scenarios. Finally, we discuss requirements and technical guidelines for Ubiquitous Computing systems in the face of Technology Paternalism.

An Introduction to Paternalism

Based on the Latin word for "father" – pater – paternalism originates from a hierarchical model of family-life, where the father cares for his children and advices them what to do and what not to do. In this original model of paternalism the father commands, because he assumes that his children are not capable enough of making decisions for themselves. Yet, paternalism does not only refer to the role and actions of fathers in a family context. Instead, scholars view paternalism as an application of a dominant and hierarchic paradigm to everyday life and as a general "**way of controlling** people…" (The Longmans Dictionary of Contemporary English, 1987). Established examples of paternalistic behaviour therefore include a husband that takes away sleeping pills from his depressive wife, a government that prohibits the sale of ineffective drugs or doctors that do not tell the truth about a patient's real condition[1].

This control can be exercised by an individual as well as a 'system' or 'institution': "[Paternalism is] **a system** under which an authority undertakes to supply needs or regulate conduct of those under its control in matters affecting them as individuals as well as in their relations to authority and to each other" (Merriam-Webster's Collegiate Dictionary, 2003). And this system can be considered – at least by the liberal mind – as **repressive**: "protecting people and satisfying their needs, but without allowing them any freedom or responsibility" (The Longmans Dictionary of Contemporary English, 1987).

Couto (2005) comments on the latter in particular when he writes: "Liberals often assume that the state should never act in a paternalistic way towards its citizens, an assumption justified by the liberal concern for freedom and autonomy." Yet, still, paternalism is accepted in many contexts and societies. This is, because paternalism also implies the aspect of "protecting people and satisfying their needs". Paternalistic behaviour is always **claimed to be mainly in the interest** of the one affected by it. Here, scholars tend to distinguish between soft and hard paternalism. Soft paternalism stands for situations in which limited rationality and competence leads to domination (so paternalism is claimed rightfully in ones interest). In contrast, hard paternalism "argues that paternalistic action is justified even in cases in which the choice is voluntary" (Couto, 2005).

[1] All these examples taken from Dworkin (2002)

What we feel is still missing from these definitions of paternalism is the aspect of 'perception'. As we know from social theory, actions do not only lead to measurable outcomes, but also to perceptions. And perception is what finally leads to acceptance, refusal or other types of responses. Since we want to analyse response behaviour in later sections of this paper, we feel the need to introduce the notion of 'perceived paternalism'. In this sense paternalism is not only about whether an action really is paternalistic, but also whether it is perceived as such by the affected individual.

Summing up these arguments we want to define paternalism as follows:

Given an instance *A* (father, government, etc., in the following: patron) that makes a decision or performs an action *X* which is affecting instance *B* (child, citizen etc., in the following: subject) directly, X is paternalistic if and only if:

- *X* is perceived by subject *B* as limiting, punishing or in any other way cutting down on freedom
- *X* is perceived by subject *B* as one that should not be overruled or in any other way disregarded
- *X* is claimed by patron A to be mainly in B's own interest

Technology Paternalism

With a view to the general concept of paternalism we have so far talked about social institutions as patrons, operating through human interface: parents, doctors or government representatives being paternalistic with their children, patients or citizens. Yet, with Ubicomp a new type of potentially paternalistic interface comes into being: the objects people use or are surrounded with.

Everyday examples that we already observe today are loudly beeping cars that – based on sensor information – annoy us if we want to drive without fasting our seatbelt. Another example is Saab's proposal to introduce car keys "keeping the engine immobilised if a breath sample from the driver is found to contain alcohol above the permitted level" (Saab, 2005). Another example is a drilling machine that cannot be operated without wearing protective glasses.[2] The list of potential examples is growing at a rapid pace. And it shows that sensor and auto-id technologies are going to be used for more than just enhanced information provision or decision support. If objects sense what is rightful and what isn't and based on this information limit or punish peoples' actions, they effectively become paternalistic. Every definition criterion identified above for paternalism is met: If someone wants to back his car out of the garage and for this short driving instance does not want to fasten a seatbelt, a loudly beeping car is easily

[2] "Elektrisierende Idee", Technology Review – Das M.I.T Magazin für Innovation, No. 5, May 2005, p.30

perceived as a *punishing* nuisance. Typically, people cannot neglect or disregard the noise *nor can they easily switch it off*. Also. the nuisance is *claimed to be in the very own interest of the driver*, because it reminds her to wear a seatbelt for her own safety.

What distinguishes the technology example from the human examples above are two further aspects: First, machines react **automatically** and autonomously which leaves recipients little room for anticipation or reaction. Second, machines are absolute. With alcohol in one's breath, for example, one would not be able to start a car any more at all, even in cases of emergency. Consequently, Technology Paternalism is not a matter of obedience as is the case with human interfaces. Instead it is a matter of **total compliance**. The risk exists that humans may have to subdue to the machine. They may not be able to overrule their intelligent objects any more in many instances. If engineers take the decision that "IF detectedLevelOfAlcohol > allowedLevelOfAlcohol THEN startingAllowed = FALSE" then, "code is law"[3].

Hence, the definition of Technology Paternalism extends the general notion of paternalism with respect to two aspects: one is that actions are being taken autonomously by machines. The other one is that by their coded rules, machines can become 'absolute' forces and therefore may not be overrulable any more (in contrast to "*should* not be overruled" in the definition above):

We therefore define Technology Paternalism as follows:

Given a technology *T* controlled by a patron *A* that performs an action *X* which is affecting a subject *B* directly, *X* is paternalistic if and only if:

- *X* is perceived by subject *B* as limiting, punishing or in any other way cutting down on freedom
- *X cannot be* overruled or in any other way disregarded without sacrificing functionality
- *X* is claimed by patron *A* to be mainly in *B*'s own interest
- *X* is performed autonomously

Finally, it should be noticed that Technology Paternalism thus defined may exist in different intensities. The example of the alcohol-testing key impeding a driver to use his car may be perceived by customers as a nuisance. In such cases, self-regulating market forces promise to impede the wide-spread diffusion of such paternalistic technical solutions. Yet, another scenario may be more feasible: When a driver is detected to be drunken, a warning lamp, labelled "You are drunk driving!", could switch on in his cockpit. This would remind the driver of his "false" behaviour but still allow him to drive anyway. This is a less intrusive way to influence user behaviour. But, is it a better one? How will drivers with low levels of alcohol feel about such constant admonishment? And

[3] This term was shaped by Lawrence Lessig in his famous book "Code is Law" (Lessig, 1999).

how will drivers that never consume alcohol feel about blowing into alcohol testing tubes every time they want to drive? The questions demonstrate that even smoother forms of Technology Paternalism may be intrusive. And it could be argued that hence objects and environments integrating this type of restrictive technology will never be marketable. Yet, as the chapter below on 'the real patrons' of Ubicomp will show, this type of apparently unmarketable technology design may not be too far fetched when other economic and governmental interests dictate its introduction. Before we delve into these issues though one more conceptual aspect of Technology Paternalism must be discussed: the inherent contradiction of Technology Paternalism with Ubicomp's vision of calmness.

Technology Paternalism and the Calmness Concept in Ubiquitous Computing

Mark Weiser pointed out that: "The most potentially interesting, challenging, and profound change implied by the ubiquitous computing era is a focus on *calm*. If computers are everywhere they better stay out of the way, and that means designing them so that the people being shared by the computers remain serene and in control" (Weiser and Brown, 1996).

Weiser's call for staying in control over calm computing is addressed by Ubicomp scholars today with technical models that allow systems to grasp and adapt to context. With RFID, for example, context knowledge can be extended to include information about things and persons. With sensor-networks context knowledge may even include the state and condition of these things and persons. By combining the information to form entities with roles and relationships, situations are reconstructed and are then being combined to define context (Coutaz, Crowley et al., 2005). The hope of scholars proposing this type of context sensitivity in systems is that they will be able to seamlessly integrate technology into decision and support functions for our every-day lives. However, as other scholars point out "Context is such an all-embracing term that it is easy to underestimate the problem of designing a computational device that could be 'aware' of it" (Agre, 2001). The question has therefore been raised whether Ubicomp technology will ever be capable enough to fully grasp context and then apply the appropriate functionality. If functionality does *not* match the context appropriately, then technology may quickly become more of a patronizing nuisance than an aid. It will then be diametrically opposed to the vision of scholars predicting "calmness".

Yet, even if functionality was to map fine onto context and also stay calm in the literal sense, the question is whether functionality could still be paternalistic. An example may illustrate this point: Think about cars that recognise traffic signs on the roadside, compare these with the current manner of driving and – against the driver's will – slow

down if he is too fast (see: Petersson et al., 2004[4]; Hooper, 2004). Applying our definition of Technology Paternalism to such a system is not complicated: There is a punishing action (slowing down the car) that is performed by technology automatically which affects a person (the driver). The action is potentially not overrulable. And the action of slowing down the car is claimed to be in the very own interest of the driver. Thus, obviously, well matching and calm systems could indeed be paternalistic as well. Hence, the dilemma with Ubicomp becomes evident: If machines are controlled, then they are not calm any more. There is a clear disaccord between the concept of disappearing technologies and the attempt to remain in control. Control premises attention and visibility whilst Ubiquitous Computing environments are designed to be invisible and seamlessly adaptive. Can this dissonance really ever be resolved?
An important factor in this will certainly be the motivation for system introduction.

The Real Patrons

Having seen the potential for paternalistic technology design associated with Ubiquitous Computing, a tempting level of power over people's behaviour is on the horizon. Of course, this power does not lie in the hands of technology itself. Technology only follows rules implemented into it. Therefore, the question arises on who are the real patrons behind Technology Paternalism if it were to become a reality? Who decides about the rules, the 'rights' and 'wrongs' of every-day actions? And what are the real interests behind a paternalistic technology? We want to discuss three groups as the potential patrons behind technology paternalism: engineers and marketers of Ubicomp technologies as well as regulators influencing application design.
First, the engineers: They could be considered the real patrons behind Technology Paternalism, because it is they who build technology. Julia M. Williams (2004) points to engineering arrogance in a flaming online article criticizing the "engineer knows best' perspective that puts the engineer at odds with society". Yet, often, it may not even be the engineers' arrogance that leads to socially suboptimal technical designs. In an interview study in the context of privacy, Langheinrich und Lahlou, for example, found that many engineers simply don't care or don't want to care about the consequences of what they create. They found that engineers systematically viewed privacy not to be a problem yet („only prototypes"), not *their* problem, not a problem at all (since firewalls and cryptography would take care of the problem) or finally saw privacy not as part of

[4] In their paper, Petersson et al. demand a system that is explicitly designed to be overrulable. On the other hand, the proposed system is demanded to "be able to perform any semi- or fully autonomous manoeuvres" (Petersson et al., 2004, p. 2476).

their project deliverables (Lahlou and Langheinrich et al. 2005). So, what if we ran into the same 'mindless' problem with the design of Ubicomp-based applications?

On the other hand, engineers seldom act independently. In most cases they simply implement what their employers ask them to. Thus, corporate financial benefits could be a key driver of Technology Paternalism. A realistic example in this context would certainly be to force people to buy product bundles, because one product component (e.g. a drilling machine) is not working without another complementary component (e.g. protection glasses). Or, it may be the enforcement to buy only from original equipment manufacturers. For example, cars could be built in such a way that they can only be repaired with spare parts of the original manufacturer (and not with cheaper ones). RFID technology generally allows the testing of matching of components. First steps towards such scenarios are mentioned by Strassner and Fleisch (2003, p. 9): They motivate suppliers to "tag their products with at least a serial number" to "[ensure] that only parts from licensed production are sold."

But the economics behind paternalistic designs could be even more subtle: Take the drilling machine that forces the user to wear protection glasses. In this case, there could be, of course, a purely altruistic interest of the manufacturer to enforce eye-protection in order to protect people from harm. Yet, it must be noted that this type of protection would also reduce the manufacturer's insurance liabilities arising from potential indemnifications to victims of accidents with drilling machines. By forcing customers to wear protection glasses accidents may become less frequent or cause weaker injuries, leading to lower compensation payments and thus lower insurance fees for the manufacturer. The case illuminates a difficult trade-off to be made when deciding on potentially paternalistic technology design: How can paternalism be avoided while still achieving 'the best' for the individual? And who is actually entitled to claim what's best for the individual? The same question may have crossed the readers' mind when reflecting on automated speed reduction in cars.

Potentially, we could see governments and other regulatory bodies like the EU in this role. But where is the borderline between Technology Paternalism and simple regulation? If there was a law that stated the obligation to wear protection glasses with drilling machines would technical enforcement then be Technology Paternalism or simply an enforcement of the law? Or both? The answer to this question could be extensive and fill volumes of debates on the role of the state in every-day life. We want to take a liberal perspective on this issue that would state that in principle "states should never act in a paternalistic way towards its citizens" (Couto 2005). Only if there were negative externalities created through a specific behaviour that lead to a general forfeit of public welfare we would consider the use of technology justified to exercise social control. Negative externalities are defined in economics. They occur if a decision (for example, to pollute the atmosphere) causes costs to stakeholders other than the person or institution

making the decision. Potentially, Ubicomp technology could be used to impede people from making this type of negative decisions. Any other use of the technology though should – in our personal opinion – be considered as paternalistic and avoided wherever possible. This would imply that if people take the risk and harm themselves through drilling without glasses, then that's their choice and they have to carry the consequences. Equally so with wearing seat belts. No more deaths than my own are caused if I decided to drive without it. Insurance experts, of course, would argue that greater harm through peoples' thoughtless choice to drive without seatbelt drives up insurance fees for everybody. Thus, negative externalities are indeed created through this adverse selection of happy risky liberals. But, then again, that's what insurance is there for, to enure the risk, isn't it?

Recommendations for Ubicomp Design

With the widespread adoption and use of RFID and sensors in every-day objects, engineers will be confronted with the question of how to best avoid Technology Paternalism.

In order to give some advice on how to design Ubicomp technology properly we wanted to go beyond our own thoughts and conducted two focus groups at Humboldt University Berlin (Baran and Krasnova, 2005). 13 people volunteered to participate in the study, most of them students at the end of their studies. The average age of participants ranged from 22 to 35**.** The first group consisted of seven students from Azerbaijan, Kyrgyzstan, Germany, China, Thailand and USA. The second focus group consisted of students and employees from Germany, India and the Dominican Republic. A moderator led the meeting and controlled the course of discussion and one assistant took notes.

Some of the comments given by the focus group members are mentioned below to illustrate our suggestions from a lay perspective[5]. They stem from the two tape-recorded discussions.

One of our main findings was that there should be a general possibility to overrule 'decisions' made by technology and any exceptions from this should be considered very carefully. **People should always have the last word!** This was also claimed by the members of the focus groups:

"In extreme situations, a person must always be able to overrule the machine"

[5] A comparable approach was also mentioned by Clausen and Hansen (2002), decribing 'Consensus conferences' held in Denmark, where "[t]he idea has been to qualify lay people to participate in debates with experts, to get this debate diffused to a broader public, and to get the debate boiled down to a 'consensus' document […]".

"You want to be in charge. Maybe the car will signal that the driver is drunk but the person should have a choice."

Yet, as we have pointed out in our section on calmness this "right for the last word" can get complicated in a world of Ubiquitous Computing as most decisions are performed in the background and are often neither noticed nor can they be reviewed or overruled constantly. In many instances, a driver would not even know that his car has just "made the decision" to slow down. Needless to say, a "notice of action" should be a required precondition for reviewing and eventually overriding the action. **Users of Ubicomp technology should be offered choices before letting technology retreat to the calm!** The possible future users confirm this recommendation, too:

"Compromise solution should always be implemented!"

But how could choice be implemented? One alternative could be to bring all computing activities to the foreground to assess them individually. Such a proceeding would give back control but would lead to an *obligation to decide* or, as Sunstein and Thaler (2003, p. 14) call it, a "coerced choosing": Every action would require attention. As the number of actions and "decisions" performed by technology will increase and as "each piece is such a small part of the whole that nobody can reasonably lay hands on all of them." (Estrin et al., 2002, p. 60), this solution is therefore impractical.

The alternative of an obligation to decide might be an *option to decide.* Here, the person mostly affected by an action would *always be informed of her choices*. A good example for this type of technical design is modern privacy management in some Internet browsers: Initially, when an Internet site with no assigned user-defined rule tries to set a cookie, a small window with four options appears: 1) allow cookie, 2) do not allow cookie, 3) allow all cookies from this site, 4) never allow cookies from this site. This window has two effects: First, the user is aware of the things going on and has to decide at least once (obligation to decide) and second, he can decide whether he wants to stay with the setting and delegate further actions to the technology for future occasions. These delegations should be revisable though. And they should allow users to take an informed decision that should, according to group discussions, lay open who is behind the technology design and for what reason. Thus, **technology should create transparency and explain who is behind the design and what motivates it!** This transparency was also claimed by the members of the focus groups:

"Once you know who is behind it you feel more safe!"
"By and large people feel comfortable if they know who is making it beep!"

And finally, people seem to be afraid of potentially being embarrassed by technology, showing them their errors or mirroring them their own defaults. We would therefore suggest encouraging **good behaviour instead of humiliating bad behaviour!** One final statement shall underpin this:

"I don't want the technical system to detect my errors when I want to do them!"

Conclusion

The key questions that arise from Technology Paternalism seem to be always the same: *When do we want to have things under control and when do we want things to act silently and autonomously? When should things be intrusive and when not? When is Paternalism in general right and when wrong? And, of course, who controls who in a specific context?*

The first two questions have to be answered individually by everyone. Some people might prefer total personal control and would also pay the price of lower comfort and more attention. Others would eventually prefer the feeling of things that work automatically and would be willing to pay the price of a restrained freedom of choice. There is no single answer and there will be no silver bullet except building flexibility into systems to allow everyone to answer these questions for themselves.

The question whether paternalism is good for people is one of the oldest philosophic questions around and still discussed widely. Sunstein and Thaler (2003, p. 4f) claim a model of "Libertarian Paternalism" because "it is testable and false" to assume that "almost all people […] make choices that are in their best interest or at the very least better, by their own lights, than the choices that would be made by third parties", whereas Mitchell (2005, p. 29) answers this by mentioning that "it is impossible by definition for a third party to make judgements about another individual's utility, because the ranking of preferences is purely subjective". There will be no single answer and we did not really expect to find one here, either.

But we introduced the paternalistic principle to serve as a basis for reflection about Ubicomp technology. We showed the need for debating about paternalism in the context of this new computing era and elaborated a working definition that accounts for the special conditions of paternalism enforceable through technological means.

We also identified some main issues that arise from Technology Paternalism and the ongoing trend towards it in an era of Ubiquitous Computing. And last but not least we made some design suggestions that could embrace the potentially negative effects arising from Technology Paternalism.

As the current discussions about privacy in the field of Ubiquitous Computing show, in the majority of cases there is no way of resolving a problem only by regulating it or only by employing technological means. A well-adjusted mix of methods, consisting of mechanisms of norms, law, market and technology seems to be the most promising approach. In the context of Technology Paternalism this could, for instance, include a legal obligation for manufacturers to design technology in an overrulable way to allow individual diversifying according to different wishes and needs of people.

In any case, a public process of discussion on the shaping of Ubiquitous Computing technologies is needed. Even if the question of 'the right degree of paternalism' is an extremely subjective and political one, we need obligatory and socially accepted guidelines for designing calm technologies. There is no determinism regarding to the impacts of Ubiquitous Computing for society leading to a pre-defined outcome. As Williams and Edge (1996, p. 857) mention, "[e]very stage in the generation and implementation of new technologies involves a set of choices between technical options." These choices have to be considered and discussed publicly – especially with deeper involvement of those people affected.

We hope we have given some food for thought with respect to the level of desirable automation.

References

Agre, P. E. (2001): "Changing Places: Contexts of Awareness in Computing", Human-Computer Interaction 16(2): 177-192.

Altman, I. (1975): "The environment and social behaviour: Privacy, personal space, territory, crowding", Monterey, California, Brooks/Cole.

Baran, E. and Krasnova, H. (2005): "Technology Paternalism", Seminar paper, Institut für Wirtschaftsinformatik - Humboldt Universität zu Berlin.

Berthold, O., Günther, O., Spiekermann, S., „RFID: Verbraucherängste und Verbraucherschutz", IWI Working Paper, Humboldt University Berlin, July 2005

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. and Rohs, M. (2004): "Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications", Journal of Human and Ecological Risk Assessment, 10(5), pp. 763-786. Online: http://www.vs.inf.ethz.ch/publ/papers/hera.pdf [2005-04-22]

Clausen, C. and Hansen, A. (2002): "The Role of TA in the Social Shaping of Technology", In: Banse, Grunwald, Rader (eds.): "Technology Assessment in the IT Society", Campus Verlag, Berlin

Coutaz, J., Crowley, J. L. et al. (2005): "Context is Key", Communications of the ACM 48(3): 49-53.

Couto, A. (2005): "The Social Legitimacy of Paternalism", Social Justice, Bremen.

Dworkin, Gerald (2002): "Paternalism", The Stanford Encyclopedia of Philosophy (Winter 2002 Edition), Edward N. Zalta (ed.). Online: http://plato.stanford.edu/archives/win2002/entries/paternalism [2005-04-26]

Estrin, D., Culler, D., Pister, K., and Sukhatme, G. (2002): "Connecting the Physical World with Pervasive Networks", IEEE Pervasive Computing, 1/2002, pp. 59-69. Online: http://www.cs.utah.edu/classes/cs6935/papers/sensNet2.pdf [2005-04-25]

Hooper, S. (2004): "The car that can read road signs", In: CNN.com, Oct. 7, 2004. Online: http://www.cnn.com/2004/TECH/10/06/roadsign.recognition/

Lahlou, S., Langheinrich, M. et al. (2005): "Privacy and trust issues with invisible computers.", Communications of the ACM 48(3): 59-60.

Lessig, L. (1999): "Code and Other Laws of Cyberspace", Basic Books, New York

Longmans Dictionary of Contemporary English (1987): "Paternalism" and "paternal", Licensed edition published by Langenscheidt KG, Berlin

Lyytinen, K. and Yoo, Y. (2002): "Issues and Challenges in Ubiquitous Computing", Communications of the ACM 45(12): 63-65.

Margulis, S. (2003): "Privacy as a Social Issue and Behavioral Concept" Journal of Social Issues 59(2): 243-261.

Merriam-Webster (2003): "Paternalism", Merriam Webster's Collegiate Dictionary. In: Encyclopædia Britannica – Deluxe Edition 2003 for PC, Encyclopædia Britannica Inc., UK

Mitchell, G. (2005): "Libertarian Paternalism Is an Oxymoron", Northwestern University Law Review, Vol. 99, No. 3, 2005. Online: http://ssrn.com/abstract=615562 [2005-05-30]

Palen, L. and Dourish, P. (2003): "Unpacking 'Privacy' for a Networked World", CHI 2003, Ft. Lauderdale, Florida, USA, ACM Press.

Petersson, L., Fletcher, L., Barnes, N. and Zelinsky, A. (2004): "An interactive driver assistance system monitoring the scene in and out of the vehicle", Proceedings of the 2004 IEEE International Conference on Robotics and Automation, p. 3475-3481

Pohl, H. (2004): „Hintergrundinformationen der Gesellschaft für Informatik e.V. (GI) zu RFID - Radio Frequency Identification."

Saab (2005): "Saab unveils Alcohol Lock-Out Concept to discourage drinking and driving", Saab South Africa. Online: http://www.saab.com/main/ZA/en/alcokey.shtml [2005-04-27]

Spiekermann, S. and Ziekow, H. (2004): "Technische Analyse RFID-bezogener Angstszenarien", Berlin, Institut für Wirtschaftsinformatik - Humboldt Universität zu Berlin: 44.

Spiekermann, S. (2005): "Perceived Control: Scales for Privacy in Ubiquitous Computing Environments", 10th International Conference on User Modeling, Edinburgh, Scotland.

Spiekermann, S. and Ziekow, H. (2005): "RFID: a 7-point-plan to ensure privacy", 13th European conference on Information Systems, Regensburg, May 2005. Online: http://www.wiwi.hu-berlin.de/~sspiek/ECIS_final.pdf [2005-04-25]

Strassner, M. and Fleisch, E. (2003): „The Promise of Auto-ID in the Automotive Industry", Auto-ID Center, May 2003. Online: http://www.autoid.org/SC31/clr/200305_3826_Automotive%20Prpsl.pdf [2005-05-18]

Sunstein, C. R. and Thaler, R. H. (2003) "Libertarian Paternalism Is Not An Oxymoron", University of Chicago Law Review, Forthcoming. Online: http://ssrn.com/abstract=405940 [2005-05-28]

Walker, G. H., Stanton, N. A. and Young, M. S. (2001): “Where Is Computing Driving Cars?”, International Journal of Human-Computer Interaction, 13(2), pp. 203-229

Weiser, M. (1991): “The computer for the 21st century”, Scientific American 265, p. 94-104

Weiser, M. and Brown, J. S. (1996): “The Coming Age of Calm Technology”. Online: http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm [2005-05-04]

Williams, J. M. (2004): “Technological Paternalism”, Prism, December 2004, Vol. 14, No. 4, American Society for Engineering Education, Washington DC. Online: http://prism-magazine.org/dec04/last_word.cfm [2005-04-28]

Williams, R. and Edge, D. (1996): “The Social Shaping of Technology”, Research Policy, Vol. 20, pp. 856-899