Inherent Tradeoffs in Ubiquitous Computing Services

Stefan G. Weber, Sebastian Ries, Andreas Heinemann

Telecooperation Group
Department of Computer Science, Darmstadt University of Technology
Hochschulstraße 10, 64289 Darmstadt
sweber@tk.informatik.tu-darmstadt.de
ries@tk.informatik.tu-darmstadt.de
aheine@gkec.informatik.tu-darmstadt.de

Abstract: Assisting everyday life is one major intent of ubiquitous computing (UbiComp). In addition, a given UbiComp infrastructure can be harnessed beyond assisting and helping people in their daily life. Exploiting its sensing capabilities, the higher level services *tracing*, *attestation*, and *confirmation* are possible. This paper discusses the inherent tradeoffs and conflicts between the individual and the society as a whole arising from the employment and usage of these services.

1 Introduction and Motivation

Ubiquitous computing's initial vision was defined more than 15 years ago, with the implicit goal of "assisting everyday life and not overwhelming it" [AM00]. As technological progress has made parts of this vision (and synonymous concepts like ambient intelligence and pervasive computing) technically feasible, it's social and societal perception and implications are still questionable. Ubiquitous computing relies on large amounts of data, collected by widespread sensors, mostly unnoticed by those being sensed. Arising privacy issues have been perceived from the beginning [We93], the sheer scale of these data collection facilities raises individual fears. Researchers actively discuss this matter. Langheinrich proclaims that "by virtue of its very definitions, ubiquitous computing has (..) the potential to create an even more invisible and comprehensive surveillance network covering an unprecedented share of our public and private life." [La02a]. In an even more pessimistic view, Cas argues that ubiquitous computing environments "resemble quasi per definition perfect surveillance infrastructures" [Ca05]. In a not too far future virtually any (non-)action in daily life can potentially imply juridical or financial consequences, and even the most banal activities may cause privacy concerns when observed by ubiquitous computing infrastructures. Will these privacy concerns become "the Achilles heel" of the ubiquitous computing vision [Sa03]? Shaping the things to come by now is of high importance.

This paper aims to contribute to this matter by discussing *tracing*, *attestation*, and *confirmation* services. We focus on their positive and negative impacts on the individual and the society as a whole by clearly stating their inherent tradeoffs.

2 Beyond Sensing

In order to react to and adapt to people and situations ubiquitous computing environments collect data via multiple sensors. Building on this sensing infrastructure we notice the following services built on the use of collected data.

- **Tracing:** With an unrestricted access to the collected data, individuals become traceable in their daily life. This traceability relies on the possibility that data from multiple sources is accessed, aggregated and interpreted. Assuming that the ubiquitous computing infrastructure will be regulated (in democratic nations) through laws, such access will be restricted in some ways. Nevertheless, from a governmental point of view, one of the primary purposes is establishing a nearly global traceability for the penal system. For example, identifying and locating criminals will become easier for the police as well as the lines of argumenting for judges. Also detection of refraining from certain actions in punitive situations becomes possible and thus traceable. Beyond individual traceability, areas as a whole can be surveilled by searching for unusual patterns in the collected data, e.g., to implement and support early warning and emergency response systems.

- **Attestation:** Civilians can profit directly from the same data as well. With appropriate access to the data collected about oneself, it becomes possible to attest certain situations for personal purposes: “Sure, I was in time at the station. The train left to early!” or “I delivered my work in time and according to what we agreed on in our meeting!” illustrate situations of use and possible individual benefits.

- **Confirmation:** Financial, accounting and warranty issues can be managed more fine-grained as well. Charges can be based on individual attestable work loads, e.g., in the case of traffic cost; individual risk assessment in case of insurances becomes possible, e.g., to set up more personalized health care services or car insurances.

3 Conflicts and Tradeoffs

Having illustrated the services we now discuss the inherent tensions and conflicts that arise from these services between the interests of individuals, organizations and (democratic) governments.

- **Tracing** potentially exposes citizens to an enormous pressure not to violate widely accepted norms of social behaviour [Ca05], thus acting as a preventive measure against crimes as well. While the individual perception of public and personal security can increase, personal fears of misuse and feelings of loss of personal privacy and freedom, which are fundamental social values, are likely to increase as well. Individual political decision-making processes can be sup-

pressed, as these require anonymity. Of importance is also the need to provide an equal and dependable traceability, causing high infrastructure costs.

- **Attestation** allows to prove actions, presence and absence in cases of damage, loss or dispute. Thus, it supports individuals in attending to their legal interests. As in the case of traceability, the possibility of actively attesting about oneself can lead to social pressure. For example, suspiciousness may arise if a wife forces her husband to reveal where he spent the last night and he does not want to. The possibility to refuse attestation must be given. If attestation techniques are used too often they may lead to tendencies of overdrawn rigorousness and further undesirable changes of user behaviour. Moreover, attestation needs to be person specific; the generated and presented report data may not contain evidences of actions of further people.

- **Confirmation** allows for individual charging, which can help to reduce costs and to receive personalized services with high quality and flexibility. This leads to stress to bring the quality-of-service, and as well the privacy of the workers is intruded. In the area of medial care/insurances, solidarity principles can be worn out, threatening social values. Especially in the case of health insurances the question arises: to which degree are individual risk based models appropriate for societies that fundamentally rely on solidarity?

The individual and public benefits and burdens are summarized in Table 1. Concerning tracing, attestation and confirmation, specific tradeoffs to privacy needs are noticeable. Tracing conflicts with privacy on a level different from the tensions between *attestation and privacy* and *confirmation and privacy*. While the first tradeoff concerns interests of individuals and governments, the second occurs between individuals and the last one matters between individuals, companies, and society.

	Individual benefits	Individual burdens	Public benefits	Public burdens
Tracing	Personal security	Loss of privacy & freedom; fear of misuse	Improved penal system & public security	Infrastructure costs; social values worn out; political decision-making suppressed
Attestation	Attesting presence / absence / (non-) actions	Private surveillance; suspiciousness	Legal certainty; justice	Undesirable changes of user behaviour; rigorousness
Confirmation	Individual charging; improved services	Pressure to perform	Cost reduction	Solidarity threatened; pressure to perform

Table 1: Individual and public benefits and burdens

4 Shaping Things to Come

Developing a deeper understanding of the aforementioned conflicts of interests can shape the way for building socially accepted ubiquitous computing infrastructures. An obvious solution is to address the arising tradeoffs from technological, social, legal and economic perspectives [ITU05]. Customizable technological solutions reflecting these tradeoffs (illustrated in Figure 1) need to be developed; social, legal and political discussions have to determine the actual mode ubiquitous computing environments will op-

erate in, adjusted to technical possibilities and peoples' needs. We assume that the actual configuration of the tradeoffs will actually decide how ubiquitous computing will be individually perceived.

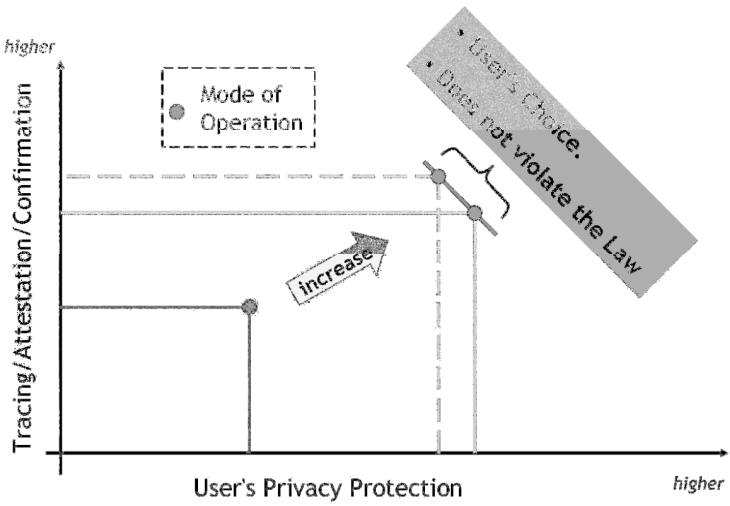

Figure 1: Tradeoffs and mode of operation of infrastructures

Current approaches to implement privacy-friendly ubiquitous computing, e.g., [La02b, BS03], give insights into further aspects that need to be addressed. Langheinrich's [La02b] intention is to equip each person with a privacy assistant, establishing a limited user control over the sensor configuration of one's current environment and some degree of transparency on being sensed. Alternatively, Beresford and Stajano [BS03] propose to establish so called mix zones, i.e., areas where users do not use ubiquitous applications and services, allowing for some degree of anonymity, as sensed data is not required in these zones and user can change their pseudonyms (for a more detailed discussion on this issue see [GHT05]). Moreover, models of privacy-friendly surveillance are being developed. In Sweeney's approach called selective revelation [Sw05], the surveillance system can grant itself a kind of search warrant on detecting anomalies in anonymized data, that allows for further and more detailed searches. However, the following questions still lack adequate answers:

- What are appropriate transparency models for ubiquitous computing? Who watches the watchers? As Weber [We06] mentions, “we do not need a totalitarian state to fear that civil rights will fade away.”

- Is there no escape possible from being watched? Is being a user ubiquitous as well? What defines being a user in ubiquitous computing environments?

- Can systems be established that automate legal decisions, to overcome limitations due to working hours of a few officials? What is the normal mode of operation of these systems?

5 Conclusions

In this paper, we discussed conflicting interests in tracing, attestation, and confirmation services, with respect to individuals, organizations, governments, and the society. We pictured that these conflicting interests and arising tradeoffs are inherent in ubiquitous computing. In order to cope with this situation and establish a positive social and societal perception of ubiquitous computing, we advocate fine-grained customizable security and privacy mechanisms to support individuals as well as governments and organizations. Beyond these technical challenges, finding and establishing accepted modes of operation of ubiquitous computing infrastructures and identifying ethical borders to their employment and usage are central tasks to maximize benefits and minimize burdens of the concerned parties (i.e., all of us). From our perspective, fine-grained customizable security and privacy mechanisms for services like tracing, attestation, and confirmation paves the way for new forms of UbiComp applications in which the positive aspects will outweigh arising fears and burdens, if technologically addressed in an appropriate manner. Herein lies the challenge for the next steps in ubiquitous computing research.

References

[AM00] Abowd, G. D.; Mynatt, E. D.: Charting Past, Present, and Future Research in Ubiquitous Computing. ACM Trans. Comput.-Hum. Interact., 7(1):29–58, 2000.

[BS03] Beresford, A. R.; Stajano, F.: Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 02(1):46–55, 2003.

[Ca05] Cas, J.: Privacy in Pervasive Computing Environments - A Contradiction in Terms? IEEE Technology and Society Magazine, 24(1):24– 33, 2005.

[GHT05] Görlach, A.; Heinemann, A.; Terpstra, W. W.: Survey on Location Privacy in Pervasive Computing. In: Privacy, Security and Trust within the Context of Pervasive Computing, 2005.

[ITU05] ITU: The Internet of Things. ITU Internet Reports, 2005.

[La02a] Langheinrich, M.: Privacy Invasions in Ubiquitous Computing. In: Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, 2002.

[La02b] Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. In: UbiComp, 2002.

[Sa03] Satyanarayanan, M.: Privacy: The Achilles Heel of Pervasive Computing? IEEE Pervasive Computing, 2(1):2–3, 2003.

[Sw05] Sweeney, L.: Privacy-Preserving Surveillance using Databases from Daily Life. IEEE Intelligent Systems, 20(5), September-October 2005.

[We06] Weber, K.: The Next Step: Privacy Invasions by Biometrics and ICT Implants. Ubiquity. An ACM IT Magazine and Forum, 7(45), 2006.

[We93] Weiser, M.: Some Computer Science Issues in Ubiquitous Computing. Communications of the ACM, 36(7):75–84, 1993.