Privacy and Trust Issues with Invisible Computers

Saadi Lahlou, Marc Langheinrich, Carsten Roecker[1].

Appeared in: Communications of the ACM, Volume 48, number 3 (March 2005) pp. 59–60

When 59 years old Robert Rivera slipped on a spilled yogurt and hurt his kneecap in a Los Angeles supermarket, he sued its management for recovering hospitalization cost and lost wages. While the case was ultimately dismissed for lack of evidence, Rivera claims a mediator contacted him before the verdict and encouraged him to settle, as otherwise the store would reveal records of his (substantial) alcohol purchases [Vogel 1998]. Rivera was a card-club member, authorizing the store to track his shopping habits in exchange for a (small) discount. While Rivera's version might ultimately be impossible to verify, the story nevertheless shows how the recording of seemingly innocuous data about daily activities can have significant consequences for our lives.

A Crowd of Little Brothers

In the era of disappearing computers it would not just be our shopping habits that would be collected in an unnoticeable fashion. Smart objects and environments that support us unobtrusively and intelligently will gather large amounts of information about every aspect of our lives – our past preferences, current activities, and future plans – in order to help us best. Five characteristics make such systems very different from today's data collections [Langheinrich 2001]: Firstly, the unprecedented coverage of smart environments and objects present in homes, offices, cars, kindergartens, schools, and elderly care facilities. Secondly, their data collection will be practically invisible: no more card swiping or form signing, as sensors in walls, doors, and shirts silently collect their information. Thirdly, data will be more intimate than ever before: not only what we do, where we do it, and when we do it, but also how we *feel* while doing so (as expressed by our heart rate, perspiration, or walking pattern). A fourth difference concerns the underlying motivation for the data collection – after all, smart objects are dependent on as much information as they can possibly collect, in order to serve us best.Lastly, the increasing interconnectivity that will allow smart devices to *cooperatively* help us means an unprecedented level of data sharing; making unwanted information flows much more likely. Taken together, these characteristics mean that data collections in the age of ubiquitous computing would not just be quantitative change from today, but a *qualitative* change: Never before has so much information about us been instantly available to so many others in such a detailed and intimate fashion.

Fear of Filing

Surveys since the 1970s show that loss of privacy is associated with the quantity of personal information collected, and that fear of privacy infringements constantly increases with the integration of computers in everyday life [Robbin 2001]. When boundaries between public and private spaces blur, users feel uneasy because they do not know what information they actually share with whom, often triggering substantial privacy and security concerns about the technology. Making technology invisible means that sensory borders disappear and common principles like "if I can see you, you can see me" no longer hold. As collecting and processing

[1] - Saadi Lahlou (saadi.lahlou@edf.fr): Laboratory of Design for Cognition, EDF R&D, 92241 Clamart, France.
- Marc Langheinrich (langhein@inf.ethz.ch): Institute for Pervasive Computing, ETH Zurich, Clausiusstr. 59, 8092 Zurich, Switzerland
- Carsten Roecker (roecker@ipsi.fraunhofer.de): AMBIENTE Division, Fraunhofer IPSI, Dolivostraße 15, 64293 Darmstadt, Germany.

of personal information is a core function of smart environments; privacy and ubiquity seem to be in constant conflict

Designers: "Not my Problem"

But what keeps the public stirring has hardly reached the laboratories yet. A 2002 survey found a disturbing lack of concern among disappearing computer project designers [Langheinrich & Lahlou 2003]. Privacy was either an abstract problem, not a problem yet (as it were "only prototypes"), not a problem at all (firewalls and cryptography would take care of it), not *their* problem (but one for politicians, lawmakers, or, more vaguely, society), or simply not part of the project deliverables. While many companies might have an explicit company privacy policy, few do so at design level. This is a significant issue as, especially in the early stages of technological development, design decisions have far-reaching consequences for the future costs of privacy protection within the system. Hence, the design of adequate solutions will only succeed if privacy-related problems are methodically approached right from the beginning.

Privacy Enhancing Guidelines

The European Union Information Society Technologies Programme funded a collective initiative that, in response to the findings above, produced European Privacy Design Guidelines for Disappearing Computer [Lahlou & Jegou 2003]. These are meant to help system designers implement privacy within the core of ubiquitous computing systems. Designing for privacy is tricky because privacy is often a trade-off with usability. The guidelines state nine rules that not only reinterpret some of the well known fair information practices [OECD 1980], such as *openness* and *collection limitation*, in the light of disappearing computers, but also add new rules that specifically deal with the privacy challenges introduced by such an invisible and comprehensive data collection. For example, rule number two, "Re-visit classic solutions," challenges designers to incorporate existing socially constructed solutions whenever possible in order to be more compatible with real-world collection practices that users are already familiar with. Similarly, applying the "Privacy razor" (rule number four) during system design asks developers to revisit the amount of data that is to be collected, and to cut out all that is not *absolutely* necessary for providing the service (which can often be provided anonymously). Other rules are more fundamental in scope, such as rule number one, "Think before doing," which encourages designers to carefully consider the very philosophy of a system's functionality and its implication for the privacy of its users – a thought experiment that is often ignored when designers build applications around newly available technology. The full text of the guidelines can be downloaded from www.rufae.net/privacy.html.

While these rules still need more feedback from real-world deployments, they nevertheless present an important first step for building privacy-aware ubiquitous computing systems that European citizens can trust in. It is imperative that designers of such systems take these guidelines as a starting point when creating disappearing computer applications, evaluate their usefulness for their design process, and fold back their experiences into the guidelines, allowing them to evolve together with the applications that define the field of ubiquitous and pervasive computing. After a number of iterations, such guidelines could form the basis for a social dialogue that brings together developers, service providers, legal experts, and social scientists in order to update existing privacy legislation; and construct together with users a sustainable future with invisible computers.

Bibliography

Lahlou, Saadi & Jegou, François (2003). *European Disappearing Computer Privacy Design Guidelines V1.0* [EDC-PG 2003]. Ambient Agoras [IST-2000-25134] report D15.4. Disappearing Computer Initiative. Oct. 2003.

Langheinrich, Marc (2001): Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, In: *Proceedings of Ubicomp 2001*, October 2, 2001, Atlanta, GA.

Langheinrich, Marc & Lahlou, Saadi (2003). *A Troubadour approach to Privacy*. Ambient Agoras [IST-2000-25134] report 15.3.1. Disappearing Computer Initiative. Nov. 2003, 27p.

Organization for Economic Co-operation and Development (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* An excerpt is available from www.junkbusters.com/fip.html

Robbin, Alice (2001): The Loss of Personal Privacy and its Consequences for Social Research. In: *Journal of Government Information*, Iss.28, 2001, pp. 493 – 527.

Vogel, Jennifer (1998): When cards come collecting – How Safeway's new discount cards can be used against you. *Seattle Weekly*, September 24-30, 1998