BY **Saadi Lahlou, Marc Langheinrich,** AND **Carsten Röcker**

Privacy and Trust Issues *with Invisible Computers*

A set of designer guidelines from the European Union offers the first step in building privacy-aware systems.

When 59-year-old Robert Rivera slipped on spilled yogurt and injured his kneecap in a Los Angeles supermarket, he sued the store's management to recover hospitalization costs 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; if he didn't the store would reveal records of his (substantial) alcohol purchases [6]. Rivera was a card-club member of that supermarket, as such authorizing the tracking of his shopping habits in exchange for a small discount. While Rivera's version might ultimately be impossible to verify, the story nevertheless shows how recording seemingly innocuous data about daily activities can have significant consequences on our lives.

In the era of disappearing computers, shopping habits would not be the only data 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 better serve us.

Five characteristics make such systems very different from today's data collections [2]: First, the unprecedented coverage of smart environments and objects present in homes, offices, cars, schools, and elderly care facilities. Second, the data collection will be practically invisible: no more card swiping or form signing, as sensors in walls, doors, and shirts silently collect information. Third, 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 best serve us. Lastly, the increasing interconnectivity allowing smart devices to *cooperatively* help us means an unprecedented level of data sharing; making unwanted information flows much more likely. Together, these characteristics indicate that data collections in the age of ubiquitous computing would not only be a 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 [5]. 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. Because collecting and processing of personal information is a core function of smart environments, privacy and ubiquity seem to be in constant conflict

But what keeps the public stirring has hardly penetrated the laboratories. A 2002 survey found a disturbing lack of concern among the Disappearing Computer Project designers [3]. Privacy was either an abstract problem; not a problem yet (they are "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 the design level. This is a significant issue, especially in the early stages of technological development, as 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 from the initial stages of development.

Privacy Enhancing Guidelines

The European Union Information Society Technologies Programme funded a collective initiative that, in response to the findings noted here, produced the European Privacy Design Guidelines for the Disappearing Computer [1]. These guidelines are meant to help system designers implement privacy within the core of ubiquitous computing systems. Designing for privacy is difficult 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 [4] in light of disappearing computers, such as openness and collection limitation, but also add new rules that specifically deal with the privacy challenges introduced by such invisible and comprehensive data collection. For example, rule Number Two, "Revisit classic solutions," challenges designers to incorporate existing socially constructed solutions whenever possible, to be more compatible with real-world collection practices with which users are already familiar. Applying the "Privacy razor" (rule Number Four) in design means listing everything the system knows about the human user, and cutting out what is not "absolutely necessary" to provide the service; for example, personal identification.

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 often ignored when designers build applications around newly available technology. The guidelines are available at www.rufae.net/privacy.html.

While these rules still require 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. It is imperative that designers of such systems use 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. C

References

1. Lahlou, S. and Jegou, F. *European Disappearing Computer Privacy Design Guidelines V1.0.* Ambient Agoras Report D15.4. Disappearing Computer Initiative (Oct. 2003).
2. Langheinrich, M. Privacy by design—Principles of privacy-aware ubiquitous systems In *Proceedings of Ubicomp 2001* (Atlanta, GA, Oct. 2, 2001).
3. Langheinrich, M. and Lahlou, S.A *Troubadour Approach to Privacy.* Ambient Agoras report 15.3.1. Disappearing Computer Initiative (Nov. 2003).
4. Organization for Economic Co-operation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (1980); www.junkbusters.com/fip.html for excerpt.
5. Robbin, A. The loss of personal privacy and its consequences for social research. *J. Government Information 28* (2001), 493–527.
6. Vogel, J. When cards come collecting—How Safeway's new discount cards can be used against you. *Seattle Weekly* (Sept. 24–30, 1998).

Saadi Lahlou (saadi.lahlou@edf.fr) heads the Laboratory of Design for Cognition at Electricité de France (EDF) R&D, Clamart, France.
Marc Langheinrich (langhein@inf.ethz.ch) is a research assistant in the Distributed Systems Group at the Institute for Pervasive Computing, ETH Zurich, Switzerland.
Carsten Röcker (roecker@ipsi.fraunhofer.de) is a scientific staff member of the research division AMBIENTE at the Fraunhofer Institute IPSI in Darmstadt, Germany.