

Living in a goldfish bowl: lessons learned about privacy issues in a privacy-challenged environment.

Saadi Lahlou, Laboratory of Design for Cognition, EDF R&D, France.
saadi.lahlou@edf.fr

Abstract:

We discuss the findings of a live experiment in a real-life setting, where a group of people worked on a day-to day basis in a highly digitized environment, while their activity was continuously recorded for several years. In many ways this environment has properties close to the future of the normal world where activities will be followed by sensors and video. Findings, some of which grounded the “European Disappearing Computer Privacy design Guidelines”, show us how this world is liveable, and consequences of the design of Privacy Enhancing Technology are discussed.

Disappearing Computer, Ubiquitous, Pervasive, Attentive etc. Computing, Augmented Environments, Ambient Intelligence, are specific in the *continuous attention of computer systems to human activity*, and *because such systems may take initiatives in data collection*. Therefore such settings are potentially collecting data beyond individuals' awareness. How can we live in a world where we are continuously observed ? How should we design ubiquitous computing systems in order to make this life sustainable?

A vast body of literature tries to redefine the privacy concept in the ubiquitous computing context [Bellotti & Selen, 1993; Langheinrich, 2001; Ackerman, 2004]. There have been many discussions on its nature, some bringing views which could ground design. For example, [Dourish & Palen 2003], in a paper grounded in a larger diversity of cases, propose a promising vision of privacy as “negotiating boundaries”.

Privacy is a vast and complex, context dependant issue [Ackerman, 2000] which cannot probably be captured by one single definition. Privacy is indeed difficult to translate, for instance, in different languages. Privacy may be connected with other issues, which make it difficult to know how far generic approaches can be applied on the field. This paper approaches the problem from the field, where we looked at privacy issues emerging in a “privacy-challenged” environment. The idea is to see what “issues” actually emerge, in the long run, in a ubiquitous computing environment where everything is continuously observed and traced, because only in a real setting we thought we could observe the co-evolution of social rules and technology (Orlikowski, 1992).

The K1 living laboratory experiment observed for three years a population of about 20 real users (mostly engineers working on a project) who accepted doing their daily work in a 400m² digitally augmented environment, futuristic and designed as an observation laboratory (including 30 video cameras etc.). This “experimental reality” setting, installed in a large industry R&D facility, more fully described in [Lahlou et al., 2002] provided rich data for the design of augmented environments. It also enabled us to understand better what privacy issues emerge in daily life. In a way, this advanced setting where all activity leaves digital traces is a prefiguration of our future “normal” digitized world.

A first surprising result is that users can cope pretty well with such a situation. In fact, after a while, a series of subtle, and mostly implicit, changes, take place to adapt. When one thinks of

it, this is not so surprising since in our everyday “normal” environment, every social interaction is by definition observed (by the other participants), and to a certain point recorded in their memories. So human beings are in fact experts at managing such issues of what should be shown or not.

But some specific issues with digitized recording is the capacity to be transferred to non participants. Interestingly, the participants in the experiments created a situation where this was not socially possible; and in fact no-one broke that implicit “non disclosure” rule. Although this social contract took specific forms in the context of this experiment, we believe this tendency is more general. For example, there are implicit rules of “decency” at work in our daily etiquette: we seldom transmit an e-mail which would be embarrassing for the sender to a third party, although a simple click would be sufficient. The inhabitants of the K1 followed such implicit rules. This means that the users would naturally follow such tendency, and may easily follow relevant affordances provided by ubicomp systems. Of course malevolent users may exist in large populations, and –unlike in the K1 experiment- social pressure may not be strong enough to enforce rules, but they are exceptions.

Focus of systems may then be more on avoiding user’s blunders and on controlling the few users who don’t behave according to the rules. This is important because privacy is always a trade-off with verbosity and bothering the user, so if we can spare some privacy enforcing technologies the system may be easier to design and use..

This also suggests that the solution may be more at social level in creating and enforcing legal rules than putting a severe emphasis on technical safeguards. As a matter of fact, our social solution to limit violence was not to suppress weapons, but to make (some forms of) violence illegal. Of course this does not solve all problems. But that such social standards may be much more efficient than technical development is food for thought for our community.

A specific attention was given to privacy issues by exploring in detail a series of incidents occurring in the K1 building [Cicourel & Lahlou, 2002]. A typical example for privacy is when a subject is led to answer, in an open space environment, a phone call which has nothing to do with her present work in the local project (family, friends, doctor, or a colleague with whom she work on a *another* project). Another is when the search engine’s memory reveals someone’s browsing habits on a computer which is used by several users. In such cases, the privacy problem occurs from the fact that a person is caught, or forced to, perform an activity in the wrong context, or exhibits a face which is wrong in a specific setting.

In the real world, unlike in design specifications, normal subjects pursue different lines of action simultaneously. These activities draw on the same attention resources, and often take place in the same physical space and time-span. But in these different activities, the subject does not necessarily put on the same face. And she is supposed to put on the right face for the right place. When the subject cannot do so, this raises a problem.

This research found, strangely, that *Cognitive Overflow* and *privacy* were two aspects of the same problem for subjects. They provoked similar stress reactions, uneasiness, the feeling of loss of control, being forced into something, and sometimes anger. This captures something of the feeling of denial of the classic “right to be left alone”.

A typical example for cognitive overflow is when the subject is sidetracked to another line of activity, either by external interruption, or because he is prompted into it by the casual encounter of an opportunity to solve an urgent and pending issue.

It became clear that *many privacy issues emerged from role conflicts between activities. Managing faces and resources with competing activities is what should be considered the basic framework for systems design, since most privacy issues –as well as cognitive overflow issues*

– emerge from the difficulty of following simultaneously several cognitive attractors with divergent demands.

This issue is well highlighted by [Philipps, 2002]. By the way, these activities were not necessarily physically located (especially distant collaboration), and therefore our initial approach based on space and borders revealed not adequate for all cases. Using a “face” approached seemed to be more appropriate, at least in our context. Privacy was, to put it short, “loosing face”.

We take here “face” as including more than mere presentation of self, as considered in western psychology, following Goffman [1959]. In the East Asian sense, according to [Choi et al, 1997], “face” (*chemion* in Korean, *mientze* in Chinese, *taimien* in Japanese) is literally “the appearance of one’s self”, and includes five facets : (i) moral integrity or virtue, (ii) true intention, (iii) position and role, (iv) propriety and (v) outward behavior. We consider that this elaborate East Asian social construct, polished through millennia of culture, can serve as a basis for privacy guidelines worldwide. The Asian construct of chemyon has moral aspects based on Confucian philosophy which may go beyond our purposes (although this may be discussed), and highlights the status aspects ; still (ii) to (v) are relevant for our topic here. Maintenance of face is perceived as less important in intimate or informal settings, which is coherent with classic definitions of privacy.

In this perspective, one does not “play” a face, one “lives” a face, and as a face, has emotional involvement and can be hurt.

The notion of “persona” has been used in the IT design literature, especially for interaction in mediaspaces. Persona is a partial individual construct, some subself or alias, whether it is created as an agent or proxy by the subject, or as [Clarke, 1994].notes, a passive identity created by an external party by gathering activity traces of a subject. Although this notion is close to the notion of face, it differs since face is a social construct. Any member of a culture knows how a face should behave in a given situation, while a persona is specific and lacks this predictability.

Based on this comes the idea that designing for privacy would be designing to allow people keeping face, and prevent them from loosing face. For this, the systems, or entities peeping though it, should only see the person as the local face its wishes to hold vis-à-vis the system, and behave towards this face according the social rules locally valid.

The 9 European Disappearing Computer Privacy design Guidelines [Lahlou & Jegou, 2004: www.rufae.net/privacy] include a translation of this principle into design principles. The way this philosophy is applied is by tailoring the system as close as possible to fit the “face” which the user expects to exhibit in her interaction here and now with the ubicomp system. Rule 4, the “privacy razor”, states:

“Human user characteristics seen by the system should contain ONLY elements which are necessary for the explicit goal of the activity performed with the system. No data should be copied without necessity. In case of doubt, remember further information may be added in context.”

We will discuss these points based on empirical observations, and what problems we encountered in applying these guidelines to our own systems, for office work and home services.

Bibliography

- Ackerman, M. S. (2000). The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human Computer Interaction*, 15, pp.179-203.
- Ackerman, M. S. (2004). *Privacy in pervasive environments: next generation labeling protocols*. *Personal Ubiquitous Computing* (2004) 8: 430–439
- Bellotti, V. & Sellen, A. 1993. *Design for Privacy in Ubiquitous Computing Environments*. Proc. Third European Conf. Computer-Supported Cooperative Work ECSCW'93 (Milano, Italy), 77--92. Dordrecht: Kluwer.
- Choin Sang-Chin, Kim, Uichol, Kim, Dae-Ik D.(1997). Multifaceted Analyses of Chemyon (“social face”): an Indigenous Korean Perspective. In Kwok Leung, Uichol Kim, Susumu Yamaguchi & Yoshihisaz Kashima, (eds.): *Progress in Asian Social Psychology*, vol.1. Singapore : John Wiley & Sons Inc., 1997. pp. 3-22.
- Dourish, P, Palen, L.(2003). *Unpacking "privacy" for a networked world*. *Conference on Human Factors and Computing Systems archive*. Proceedings of the conference on Human factors in computing systems. Ft. Lauderdale, Florida, USA. 2003, pp. 129-136
- Lahlou, S. (2003). *Constructing European Design Guidelines for Privacy in Ubiquitous Computing*. Workshop on Privacy In Ubicomp'2003. Ubicomp communities: privacy as boundary negotiation. October 12, 2003
- Lahlou, S., Jegou, F. *European Disappearing Computer Privacy Design Guidelines VI [EDC-PG 2003] Ambient Agoras IST-DC report D15.4. LDC, EDF, R&D, Oct. 2003*
- Langheinrich, M. (2001). *Privacy by Design - Principles of Privacy Aware Ubiquitous Systems*. Ubicomp 2001, September 30-October 2, 2001, Atlanta, GA.
- Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, 3(3), 398-427.
- Phillips, D. J. (2002). *Context, Identity, and Privacy in Ubiquitous Computing Environments*. Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, UBICOMP 2002. Göteborg, Sweden. September