The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects

Marc Langheinrich

Institute for Pervasive Computing
Swiss Federal Institute of Technology (ETH)
Zurich, Switzerland
langhein@inf.ethz.ch

Even though few projects in ubiquitous computing explicitly address privacy in their research agenda, many designers of such system openly acknowledge the fact and reiterate their concern for privacy. With the help of a DC privacy troubadour action, the author envisioned harnessing such implicit concerns and unspoken ideas to create an explicit account of the "state of privacy" on the cumulative minds of ubiquitous computing researchers. However, after visiting four DC projects at five different locations, it became clear that even though general concerns for privacy remain high, few researchers have actually thought about such problems enough to be providing additional insights. This paper tries to formulate an initial set of hypotheses that explain this discrepancy between privacy concern and design effort, based on interviews with DC-researchers.

1 Introduction

At the first Disappearing Computer (DC) Jamboree in Zurich in October 2001, a group of researchers within the Ambient Agoras project organized a privacy workshop as part of the meeting program. Apart from members of the Ambient Agoras project itself, researchers from three other projects were present (Gloss, Grocer, and Smart-Its). After a half-day brainstorming session about the nature and attributes of privacy, a follow-up meeting at one of the Ambient Agoras partner sites, Electricité de France (EDF) in Paris, was scheduled for further investigating the actual privacy implications of the individual DC projects.

However, during the next meeting in January 2002, it turned out that an individual project assessment was nearly impossible without knowing the exact details and provisions of its systems and prototypes. Thus, the idea of a privacy troubadour was born: having a dedicated researcher visit individual DC-projects, it should be possible to answer in detail questions like "Where is data stored?" "Who has access to this data?" or "How long is data retained?", which all seemed

October 2002	Ambient Agoras, Paris, France (internal meeting)
November 2002	Smart-Its, Lancaster, UK
December 2002	Oresteia, London, UK
January 2003	Smart-Its, Gothenburg, Sweden
February 2003	E-Gadgets, Patras, Greece
May 2003	Ambient Agoras, Paris, France (internal meeting)
May 2003	Interliving, Paris, France

Table 1: Privacy Troubadour Visiting Schedule

to be required to judge a projects privacy implications. Beyond such factual project data, the group moreover hoped to be able to harness specific design experiences with respect to privacy: whenever a decision to process or store personal information or sensory data was made as part of the system design, the people involved would probably have made some technical or moral judgement as to its effect on user privacy. The group members envisioned soliciting such implicit concerns and unspoken ideas to arrive at privacy guidelines that would have been created from practical experience instead of theoretical analyses.

The Privacy Troubadour Action (TA6) within the Disappearing Computer Initiative was granted in September 2002. The initial application document proposed that

> "...by visiting selected projects within the DC-community, the troubadour should be able to examine each project's individual goals and concepts in detail in order to establish its inherent privacy threats and suggest improvements. Visits would include demonstrations of existing prototypes and various discussions with developers and researchers concerning their project goals and implementation methods."

Its initial funding included visits to five different DC projects in a first round effort, with an optional extension of visiting another five projects after a mid-term report had been prepared. Initial contacts were made during the second DC jamboree, held in October 2002 as part of the Ubicomp 2002 conference in Gothenburg. The interest in such an activity was actually quite high, and many projects welcomed a visit from the troubadour as they all were concerned about privacy implications and were eager to learn more about the issue, as well as share their design experiences.

2 Visits

Table 1 gives a timeline of the first seven visits, including two preparatory meetings at EDF in Paris. Even though the author is affiliated with the Smart-Its project itself, visiting two other Smart-Its project sites (Lancaster and Gothenburg) was thought to offer an interesting opportunity to observe how the same project could lead to very different levels of privacy awareness among participating researchers.

After the initial contacts had been made during the Gothenburg Jamboree, agreeing on actual appointments often took considerable time. Also, preparing the individual visits turned out to be more time consuming than initially thought, as they required both reading up on existing project

reports, as well as preparing project-specific (informal) questionnairs that were send out ahead of the visit. Lastly, most sites welcomed brief presentation on privacy issues, which needed to be slightly adapted to fit the various audiences involved (e.g., classroom-style lectures, general research seminars, or closed presentations to project members only).

The format of the visits varied widely. At one site, a single researcher was available for most of the day to exclusively discuss the questionaire with the troubadour, while other sites had arranged for a large number of meetings with different researches, also from non-DC-projects. Some sites organized a separate public seminar for interested researchers and students, one even arranged for a lecture as part of a design class in order to facilitate discussions with graduate students. Another project co-located the visit with its regular project-meeting, which lasted for two full days and also involved researchers from other sites, offering two two-hour slots exclusively to the troubadour cause.

As part of each visit, interviews were recorded for later transcription, totaling about five hours of audio. While this worked well in office settings, many meetings took place in public spaces such as cafeterias or cafés, and footage from such sessions turned out to be very hard to understand. A digital camera was used to photograph or film prototypes or demonstrator that were shown during the visits, but future interviews might benefit from using the camera to also film the discussions itself, aiding transcription in noisy environments.

3 Findings

The initial aim of learning about the individual experiences of DC-researchers in order to arrive at privacy guidelines for future DC-projects soon proved futile. Most researchers that participated in the interviews and discussions did not (yet) think of privacy issues in their own work, or only on a very obvious level. Over the course of the various interviews and discussion, the following hypotheses emerged that would explain why researchers, even with a heightened awareness for privacy issues, would not actively pursue the privacy implications of their systems:

- **Not feeling morally responsible:** There were several reasons why researchers felt that it was not up to them to provide for privacy awareness in their designs: either lack of applicability to their specific field of expertise (“for [may colleague] it is more appropriate to think about privacy issues. it is not really the case in my case”) or because other social processes were felt to be more adequate to regulate such issues (“little by little – I expect that would be a process of 20 years – that you need a generation actually to sort out, where is the social value, [...] and then formalize the legislation”).

- **Not necessary anymore:** Some researchers thought existing security mechanisms to be adequate protection from privacy abuses: “i think all you need is really good firewalls. [...] if you know, or if you are aware of, that this might be a problem, then you are safe.” Similar ideas came up in other interviews: Question: “So you imagine that existing technology would be used?” Answer: “Yes, right."

- **Not yet necessary:** In many cases, researchers thought that only after initial prototypes had been built, a topic like privacy could properly be addressed. One of the many design

strategies heard were: “we first thought: let’s build this first...” and “my approach is more to really build these things now in order to see what issues arise there”.

- **No problem for prototypes:** Related to the above point, but with a slighlty more practical orientation, were remarks that privacy had not proved to be a problem in this early stage of prototype design. Far more often, designers would identify and tackle problems of energy usage, communication protocols, or data analysis, instead of spending creative energy on privacy issues.

- **Too abstract of a problem:** In some cases, researchers purposefully did not think about privacy: “I think you can’t think of privacy when you are trying out... it’s impossible, because if I do it, I have troubles with finding ubicomp future [laughs], when I think of the privacy issues. but i... and the more I think about it, the more I become sceptical. but... on the other hand, some.... I think it’s important that you think about it, but I think you can’t... you can’t... when you are building prototypes and you are trying making design examples you can’t have that...”

- **Not part of deliverables:** In one case, four hours had been reserved for privacy issues during a two-day meeting. However, the first day the session got cut down to half the time due to extended discussions on getting the final deliverable into shape. The second day saw the entire rest of the planned privacy session cancelled, due to ongoing deliberations about specific implementation details. In another case, interviews were cut short since the researchers had to furnish the newly aquired office space (e.g., unpacking boxes, rushing to IKEA to buy new furniture...).

The few cases that had researchers explicitly address privacy were few and often shallow. Some projects had privacy listed as part of one of the deliverables, so a general note on privacy definitions and issues, as well as a brief description of ethics, had been produced. However, during the continued development of the prototype, no re-evaluation of the system in light of these issues, or a re-evaluation of such issues in light of the existing prototype was made.

Apart from the aim of gathering implicit knowledge from researchers, the idea of directly asking specific implementation details in order to evaluate a projects privacy invasiveness also turned out to be rather ineffective. In most cases, design choices pertaining to privacy, like data storage and disemination, were not fully specified yet. Even though prototypes might be storing or communication personal sensory data in a specific way, most designers pointed out the temporary nature of such arrangements, which would of course be redesigned should their prototype ever be used in a production system.

4 Conclusions

The troubadour grant application stated that “a troubadour is not sent as a lecturer offering ready-made solutions to existing privacy threats within a project, but instead be a collaborator of the regular project members trying to increase the social acceptance of the project.” While the reception at all projects was warm and quite often with genuine interest in the topic, the

lack of privacy *requirements* in most projects turned out to short-circuit the idea of *collaboratively* sorting out the problem of privacy in the Disappearing Computer initiative: input from the troubadour was welcome, but few people had the time and energy to substantially analyze their own work.

As long as privacy is situated on a non-critical development path, more important issues such as energy effiency, code size, or robustness dominate the researcher's todo-lists. Decisions pertaining to data storage and communication details are often improvised and seen as a temporary solution fit for prototype deployment. Projects which explicitly had privacy issues as part of their deliverables, generally exhibited greater concern for such issues, even though they often stopped short of generating novel ideas and limited themselves to a broad but shallow summary of general privacy issues, without taking project specific design parameters into account.

If a robust culture of privacy awareness is to be fostered among designers of ubiquitous computing systems, making such requirements explicit already as part of the project funding process seems to be the most viable approach. Even if designers feel morally responsible, unless either users (in a comprehensive field study) or project officers ask for it, there will hardly be much time and energy to spare. Having a better set of requirements to test prototype systems against would also contribute to the cause, though such technical issues would probably better be tested by a thorough examination of project documentation, together with singular interviews for clearing up specific implementation details.