Life-Cycle Privacy Policies for the Ambient Intelligence *

Harold van Heerde
Electrical Engineering, Mathematics and Computer Science
University of Twente
Enschede, Netherlands
h.j.w.vanheerde@ewi.utwente.nl

A smart, anticipating and learning environment will have a great impact on privacy. Ambient Intelligence will be everywhere, is invisible, has powerful sensing capabilities and most of all has a memory [2]. This does introduce a privacy risk, because context histories are vulnerable for attacks (hacking the context database, corrupt database administrators, human mistakes, et cetera), so storing of privacy sensitive data is not desirable in privacy perspective. However, high quality and quantity of data improves smartness for the Ambient Intelligence, while less and degraded data improves privacy. Therefore the problem to be solved is how to balance smartness and privacy. We propose to give the control over the life cycle of their data to users, who themselves can balance their needs and wishes in terms of smartness and privacy. Balancing the control and the information flow between owner and collector of data decreases the asymmetry of information and the chance of privacy violations [1].

We let users (the owners of the collected data) specify *Life-Cycle Policies* which will be bound to the acquired data. These data is stored in a privacy aware context database which degrades the data progressively according to the policy. Data is modeled as triplets (time, person, context). Triplets can take values in context states, exhibiting a certain level of accuracy specified in a domain generalization graph of that attribute. The generalization graphs form together a cube, in which each dimension represents the accuracy of an attribute of the original data triplet. A Life-Cycle Policy (LCP) is a set of transitions between elements (states) of this cube and the events which trigger the transitions. With LCPs, users can specify the k-anonymization [3] of context on a individual and event-based level.

A prototype of a system which monitors the browse behavior of users has been implemented. URLs visited by users will be monitored, enabling smart services like ranking websites, contact users with same interests, finding interesting websites visited by members of a certain group and calculation of anonymized statistics. Users can specify policies (e.g., degrade time to hour and id to group after one hour, degrade URL to category after one month, see figure 1), wich are attached to the data and will be stored and executed within a privacy aware context database. The performance of such database has been studied, showing the feasibility of our approach.

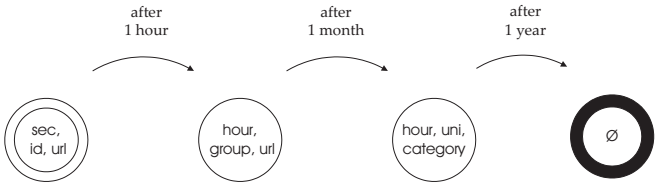

Figure 1: *a possible LCP with states (time, ip, url), $\emptyset$ stands for a deleted (or completely degraded) value.*

References

[1] Xiaodong Jiang, Jason I. Hong, and James A. Landay. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In *UbiComp '02: Proceedings of the 4th international conference on Ubiquitous Computing*, pages 176–193, London, UK, 2002. Springer-Verlag.

[2] Marc Langheinrich. Privacy by design - principles of privacy-aware ubiquitous systems. In *UbiComp '01: Proceedings of the 3rd international conference on Ubiquitous Computing*, pages 273–291, London, UK, 2001. Springer-Verlag.

[3] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal on Uncertainty Fuzziness and Knowledge-based Systems*, pages 557–570, 2002.

*CTIT Symposium "Smart Environments" 2006