Balancing smartness and privacy for the Ambient Intelligence

Harold van Heerde,
Database group, University of Twente, The Netherlands
h.j.w.vanheerde@ewi.utwente.nl

October 10, 2006

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. Because of this *memory* (or *context history*), people sometimes could be confronted with actions and behaviour from the past which otherwise would have been forgotten. One of the main difficulties with privacy and ubiquitous computing is the way how data is collected. When making a transaction with a web shop, it could be quite clear which kind of data has been exchanged. Ubiquitous computing techniques however, such as small sensors or cameras equipped with powerful image recognizing algorithms, often collect data when people are not aware of it [4]. In that case it is possible that people *think* they are in a closed private area (such as coffee rooms), but in *reality* they could be monitored by sensors in that room without having their consent.

Several techniques have been proposed in the literature which let donors of the data specify privacy policies, in order to give control about their data to the owners of that data [5, 2]. Although such policies are rich enough to let people control who, when, how long, and what kind of information can be disclosed to specific applications, enforcing those policies is usually done through access control. Only relying on access control mechanisms to protect against unauthorized disclosure of data, is not sufficient in terms of privacy protection [1]. Perhaps the context databases can be trusted *now*, but they might not be in the future (e.g. due to the change of privacy regulation laws, human mistakes, *et cetera*). Therefore, limited retention techniques are highly desirable to prevent large context histories to be disclosed.

The amount of smartness of applications is bound to the quantity and quality of the data they can use. The more accurate the data is, and the more data has been gathered from a certain individual, the better a smart application can learn from that data without user interaction [3]. The challenge is to find the best balance between the quality and quantity of data at the one side, and the privacy sensitivity of the data at the other side.

To find a balance between smartness and privacy, we propose to physically *degrade* the data according to application requirements and/or user preferences. By degrading data, the goal is to only retain the minimal form of information needed to maintain the desired view of the data. Generating such view by means of degradation functions, and to keep the result of the queries on that view adequate is difficult, since additional information is needed to update the view when new sensor data arrives. To go a step further, progressive degradation (degrade data in multiple steps) and user defined degradation policies can be used to further balance privacy and smartness for the Ambient Intelligence.

References

[1] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Hippocratic databases. In *28th Int'l Conf. on Very Large Databases (VLDB), Hong Kong*, 2002.

[2] Ji-Won Byun and Elisa Bertino. Micro-views, or on how to protect privacy while enhancing data usability. Vision paper CERIAS Tech Report 2005-25, Center for Education and Research in Information Assurance and Security, West Lafayette, IN 47907-2086, 2005.

[3] C. Doom. Get smart: How intelligent technology will enhance our world. Technical report, Computer Sciences Corporation: Leading Edge Forum, 2001. A report available from www.csc.com.

[4] 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.

[5] W3C. Platform for privacy preferences (P3P) project. http://www.w3.org/P3P/, June 2005.