A Privacy Agent in Context-Aware Ubiquitous Computing Environments

Ni (Jenny) Zhang and Chris Todd,

Department of Electronic & Electrical Engineering,
University College London
London WC1E 7JE, United Kingdom
{jenny.zhang, c.todd}@ee.ucl.ac.uk

Abstract. This paper targets personal privacy protection in context-aware ubiquitous computing environments. It proposes a privacy agent technology to help notify people of relevant information disclosure, and to empower them to manage privacy with relative ease. In essence, the development of the privacy agent technology employs privacy terminology and policies specified in Platform for Privacy Preferences Project (P3P) [1], and uses ontological modeling technique to facilitate automated processes of privacy-relevant interactions on behalf of individuals. The development of privacy agent is an integrated part of our ongoing effort towards developing a privacy-respecting context-aware infrastructure.

Keywords: Privacy Protection, Context-Awareness, Ubiquitous Computing, Ontology, P3P.

1 Introduction

In ubiquitous computing environments, sensors and embedded computing devices make it easier than ever to collect and use information about individuals without their knowledge. This has led to a great privacy concern about the potential for abusing personal sensitive information, unease over a potential lack of privacy control, and general desire for privacy-respecting systems [2]. Privacy problems only worsen in context-aware paradigm, where the ubiquitous computing environments discover and take advantage of contextual information (such as user activity, location, time of day, nearby devices) to make decisions about how to dynamically provide services to meet user requirements. Under this circumstance, information that can be used to characterize privacy aspects of an individual comes from various types of sources and with different sensitivity. It is likely that individual privacy preferences towards the dynamic context-aware environment comprise a complex set of rules in response to various situations and changes over time. These make it challenging to provide an adequate privacy protection therein.

Unfortunately, existing approaches focusing on conventional data management environments are inadequate to support dynamic privacy requirements presented in context-aware paradigm. Most of the privacy efforts in the field of ubiquitous

computing have been concerned with integrating access control mechanisms into ubiquitous computing infrastructure [3,4,5,6], and employing conventional encryption and security mechanisms as well as identity management tools (such as anonymity and pseudonymity techniques) to complete privacy protection [3,7]. These solutions addressed parts of privacy challenges faced in context-aware systems, but did not support active participation and choice of individuals to control over their personal data. Quite often people are allowed to specify their privacy requirements only by filling in some forms with predefined layout and options, as exemplified in [4, 8]. Such fairly simple approach would be not useful where a person's willingness to share personal information may depend in part on time, his location, and current activities, and may change over time. Demands for flexible mechanisms and user interface for relatively unobtrusive user participation in controlling information disclosure (including getting notice, feedback, and explicit consent) are significant.

In this paper, we propose an intelligent agent to handle privacy-related interactions on behalf of individuals. The privacy agent aims at addressing two key concerns of preserving privacy in context-aware ubiquitous computing environments: privacy feedback (notifying people of relevant information disclosure) and privacy management (i.e. allowing people to express their privacy preferences and manage privacy levels). The development of the intelligent privacy agent is characterized by developing automated preference mechanisms, considering that the task to take full context-aware controls over how personal information is shared can be overwhelming to individuals and might disrupt their ongoing activities, which could defeat the basis goal to make context-aware environments unobtrusive.

The paper is structured as follows. Section 2 presents a use scenario showing how people could use the envisioned privacy agent to preserve their privacy. In section 3, we introduce briefly a privacy-respecting context-aware architecture prototype of which the design of the privacy agent is an integrated part. Section 4 presents a privacy vocabulary and describes how we use ontological modeling techniques to model the privacy vocabulary, in order to facilitate automated processes of the privacy agent. Section 5 continues with some implementation consideration of the privacy agent. In section 6, we look at relevant research efforts towards privacy protection in ubiquitous computing environments. The paper ends with section 7 where a summary of this paper and a brief description of future work are presented.

2 Use Scenario of Privacy Agent

Imagining a wireless-networked city offers context-aware ubiquitous computing services. The city's tourist information center provides a location-tracking service so that tourists can use personalized shopping-guide applications in each shop.

Alice is a tourist visiting the city and carries her smart phone in order to use context-aware ubiquitous computing services. The smart phone serves as a personal assistant and provides Alice an interface to specify her privacy preferences. The privacy preferences are uploaded to and stored at Alice's Privacy Agent (PA) residing somewhere on network.

It is assumed that Alice has specified that any services or applications can use pseudonyms stored on her smart phone to deliver personalized services without alerting her, while any services or applications requiring her real identity and exact location must have her explicit consent.

As soon as Alice enters the city's tourist information center, the location-tracking service advertises itself. The advertisement states tourist guide applications that Alice will benefit from, as well as accompanying data collecting policies which specify data collectors, requested information with desired level of granularity, intended use, expected duration of use, potential third parties, etc. Alice's PA reads the collecting policies, compares them with Alice's privacy preferences. A conflicting interest is detected as the location-tracking service asks for Alice's exact location in order for tourist guide applications to function. The PA then notifies Alice (through her smart phone) of the privacy conflict and wait for her approval or rejection. In case no conflict of interest is detected, the Privacy Agent will not intrusively notify or alert Alice.

Alice then finds that the service offer is interesting and replies to her PA that she would like to accept the service offer in compromising her wish for privacy. Then, when Alice walks into a supermarket, a personalized advertisement service based on Alice's personal profile (e.g. gender, age, occupation, purchase history, etc.) is offered. Alice's PA recognizes the need of a unique identity to use this service, but continues to respect Alice's privacy by offering a pseudonym in place of her real identity. Only when Alice checks out, the Privacy Agent uses Alice's credit card (with real identity information) for payment.

3 A Privacy-Respecting Context-Aware Architecture Prototype

The above scenario outlined basic notions of preserving privacy in context-aware ubiquitous computing environments. To work with the scenario, we have developed a privacy-respecting context-aware architecture prototype within which privacy agents play an important role in implementing privacy protection mechanisms.

As illustrated in Figure 1, a layered architecture and components framed by broken lines in the right of the figure present an architectural support for developing context-aware systems. It provisions four key functionalities of Context Collecting, Storage, Processing and Dissemination [9]. Context Processing Layer is responsible for manipulating raw context data to appropriate levels of abstraction that are desired by context clients; Context Repository Layer provides ability to manage and store context information; Context Coordinate and Context Association Manager work together to direct the collecting of context information from various sources and the dissemination to clients who issue requests.

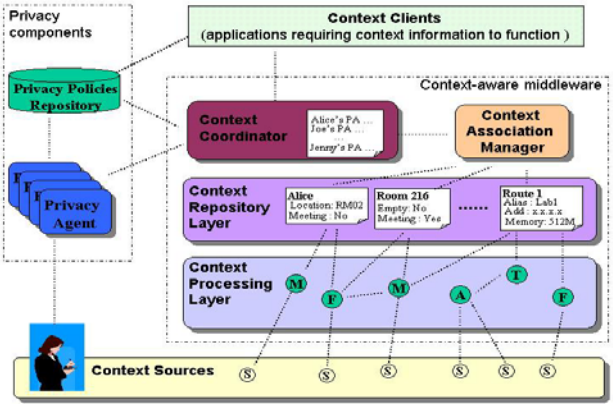

Fig. 1. Context-awareness architecture prototype and privacy components

The context-aware architecture provides features to preserve personal privacy through interactions between Context Coordinator, Privacy Agent, Privacy Policies Repository, as well as context sources (i.e. human users) and clients (i.e. context-aware applications). The Context Coordinator serves as an interface to context clients, where context information is requested and a basic access control is performed. The basic access control checks if a further fine-grained privacy check by the Privacy Agent in accordance with individuals' privacy preferences is required. Once the privacy check is resolved, an information disclosure agreement between the user and the context client will be stored in the Privacy Policies Repository. Figure 2 illustrates how various components in our architecture work together to preserve privacy when the location-tracking service in our use scenario requests Alice's location information.

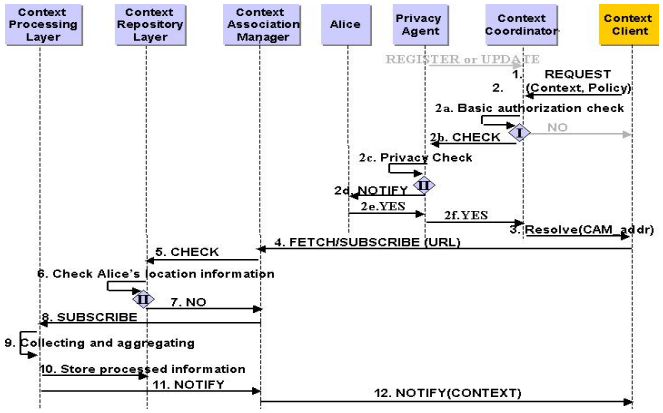

Fig. 2. Sequence of messages that characterizes an authorized context request

4 Privacy Vocabulary and Privacy Rule Ontology

Privacy agent is designed to relieve people from the burden of managing their privacy preferences toward dynamic context-aware environments, in addition to notifying them of relevant information disclosure. It has two major functionalities. On the one hand, it mediates privacy-related interactions between a user and data collectors, including notifying the user of relevant information disclosure and negotiating on behalf of the user with data collectors in accordance with his privacy preferences. On the other hand, the privacy agent serves as a continuously running service that can be contacted and queried by the user anytime, allowing instant access and adjustment to privacy preferences.

To cope with the concern that individuals' privacy preferences might change over time and in response to contexts, some level of automated preference mechanisms (i.e. automatically computing an individual's privacy preferences according to his initial settings) is required, and the privacy agent has an inference engine planted in order to compute disclosure policies in various context. To facilitate the automated processes of the privacy agent, we have been developing a privacy vocabulary to represent privacy data and rules, and using ontological modeling techniques to model the privacy vocabulary. The following subsections introduce the development of the privacy vocabulary and the privacy rule ontology respectively.

4.1 Privacy Vocabulary

Recalling the use scenario of privacy agent, Alice's privacy agent parses and compares the context-aware application's collecting policies against her privacy preferences, negotiates on behalf of Alice with the context-aware application if conflicting interest occurs, and produces a concise report once information disclosure is agreed. The collecting policy of the context-aware application, the privacy preferences set by Alice, and the disclosure agreement are all expressed with a shared set of privacy vocabulary. The privacy vocabulary consists of an unambiguous representation of privacy data, as well as descriptions of disclosure conditions of the privacy data, by which both parties (Alice and the application) and privacy-related functional components involved in our architecture (i.e. Privacy Agent, Privacy Policies Repository, Context Coordinator) could have a common understanding about privacy requirements while interacting with one another.

We have been developing the privacy vocabulary based on the terminology and policies specified in Platform for Privacy Preferences Project (P3P) [1], and adopted P3P policies as a basic data format in privacy data exchanges, with the intention of benefiting from the substantial legal and social expertise that has been put into the development of the P3P standards. However, since the P3P is initially an attempt to provide privacy mechanisms for Web, it only takes into account a person's identifying information (such as name, birthday, home-address, credit card details, etc.) as private data to be protected. In context-aware environments, staple contextual information (such as a user's location) is also sensitive, but is not covered by the P3P specification. Some extensions are thus necessary to P3P base data schema and regular policy elements before P3P practices could be adopted in context-aware

ubiquitous computing environments. In particular, we define a new location data element <Location> to represent a user's current location, and extend P3P's <PURPOSE> element to enable data collectors (i.e. context-aware applications) to explicitly describe their purpose of data collecting practices (in other words, the type of service they offer). Figure 3 below shows a high-level skeleton of the P3P policies file that is used in privacy interactions in our architecture, with two blocks in shadow highlighting the extensions of <Location> and <SERVICETYPE> elements.

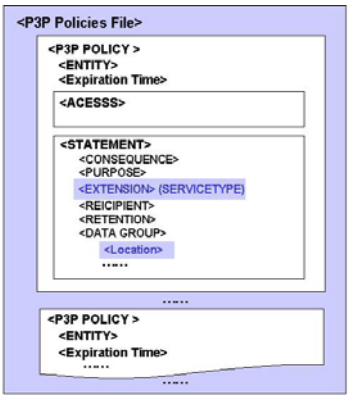

Fig. 3. A high-level skeleton of a P3P policies file (a full explanation about regular P3P policy elements is available in P3P specification [1])

4.2 Privacy Rule Ontology

In the field of knowledge management, ontology represents a formal description of concepts in a domain, properties of each concept, and restrictions on those properties, and has inherent strength in capturing relationships between the concepts and properties [10]. This can be used by inference engine planted in privacy agents to reason over ontology descriptions as a means to support privacy check and matching.

We have been experimenting on using ontological modeling techniques to model the privacy vocabulary (including both privacy data elements and disclosure conditions), and attempting to take advantage of existing description logic inference tools to implement ontology-based reasoning. Figure 4 below illustrates a subset of the ontological specification of privacy rules that correspond to P3P specification.

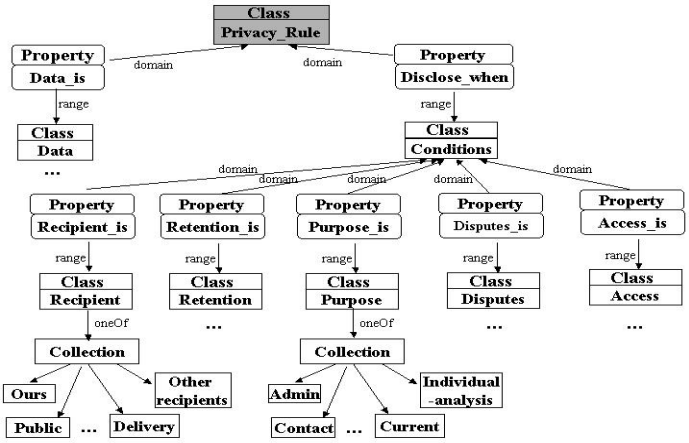

Fig. 4. A subset of the ontological specification of privacy rules

As illustrated in the Figure 4, a Privacy_Rule class is defined to represent privacy preferences set by a person. Every privacy rule is expressed with two elements: Data (Data class) and Conditions (Condition class). The Conditions class contains all conditions under which a person is willing to disclose personal data. According to P3P specification [1], the conditions can be classified based on various personal concerns including recipients of data, purposes of data collection, duration that data will be kept by recipients, a user's access privilege to his personal data once stored by recipients, and ways of handling disputes. The Privacy_Rule class has two properties: Data_is and Disclose_when, forming a triple expression that can effectively describe the relationships between privacy rule, data and disclosure conditions. Both Disclose_when and Data_is are allowed to have multiple values, since a set of data may have same disclosure conditions.

The Data element specified in the Privacy Rule Ontology represents sensitive personal information that asks for privacy protection. The information includes P3P base data scheme and our extensions of location-related contextual information. Since data schema in the P3P specification is structured hierarchically (by using a dotted notation, such as user.home-info.telecom.telephone), it is reasonable to use ontological modeling technologies to capture the multiple-level hierarchy of P3P data scheme. With logic relationships inherent in the ontology-based representation of data scheme, our approach provides some powerful inference capabilities that are not supported by other P3P rule matching languages, such as APPEL [11]. For instance, knowing that a user does not want to reveal her home address and that home telephone number is associated with home address, the privacy agent could reason that it should also keep secret of the user's home phone number.

5 Implementation of Privacy Rule Ontology and Privacy Agent

Privacy Rule Ontology has been developing by using Web Ontology Language (OWL) [12]. HP's Jena platform [13] has been chosen as a programming environment for developing privacy rule inference mechanisms.

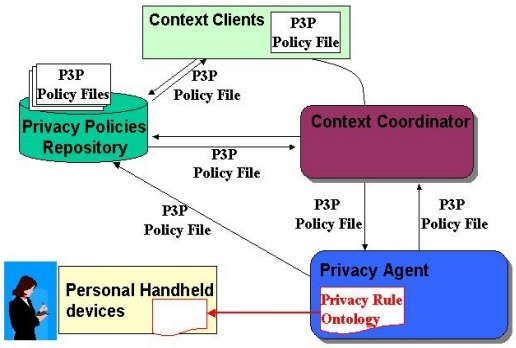

Fig. 5. Privacy Rule Ontology and P3P policy files in privacy-related interactions

As illustrated in Figure 5, the Privacy Rule Ontology (in an OWL file) resides in personal Privacy Agent and is made available to users via their personal handheld devices (such as PDA, Smartphone, etc). The OWL file contains all classes and properties that are required to construct privacy rules, but it does not include rule instances. The rule instances are dynamically generated when users specify manually their privacy preferences. Each time a user edits his privacy preferences, his personal handheld device refers to the Privacy Rule Ontology that is preloaded to the device's memory. Once the new privacy preference is created and sent to the person's Privacy Agent, the Privacy Agent invokes the privacy rule OWL file through Jena API, and creates automatically the instance of Privacy_Rule, Data and Conditions classes, as well as associates the instances with relevant properties.

Privacy agents could be implemented as programming codes and embedded into personal handheld devices or other data management tools, or deployed as a proxy server. In our implementation, we prefer placing privacy agents somewhere on network that is always accessible whenever requested, rather than embedding them into personal handheld devices. The preference is primarily driven by the consideration of saving power and an availability reason. In our proposal, ontology-based reasoning capabilities and a powerful inference engine are required to enable efficient privacy check and rule matching, which probably imposes high requirements on resource-constrained devices like PDA. In addition, in context-aware environments where personal devices might suffer from intermittent connectivity, a remotely located privacy agent could potentially carry out its function independent of the envisioned poor connectivity.

6 Related Work

The development of the privacy agent is an integrated part of our ongoing effort towards developing privacy protection solutions for context-aware systems. During the design of the privacy-respecting context-aware architecture, we had investigated some ubiquitous computing prototypes and systems that were specifically designed with privacy protection in mind, such as Confab [2] by Hong, PawS [7] by Langheinrich, Privacy solutions in AURA project [5] and IETF's Geopriv framework [3]. Our privacy solution has been building upon their experience and attempted to build privacy flavor into the initial architecture design, in order to lessen the risks of providing only shallow and short-lived privacy solution. More importantly, the privacy work proposed in this paper is meant to empower people with appropriate mechanisms to express and manage their privacy preferences with relative ease, which has not been a focus of the privacy work mentioned above.

Applying P3P practices to ubiquitous computing environments has been proposed by [7, 14]. In particular, PawS [7] by Langheinrich presented an informative work that adapted the P3P policies to be applicable in ubiquitous computing environments, which serves as an important supplement and is compatible to our work. However, there is a key difference between our work and other privacy work that has attempted to use P3P. We have been employing P3P terminology and policies, both for data collectors to state collecting policies and for individuals to express privacy preferences. On the contrary, the P3P itself and most of the privacy work built upon the P3P limited the use of P3P policies only as a vehicle for data collectors to state their collecting requirements. They must employ other preference formulation languages, such as APPEL [11], to allow users to express their privacy preferences.

Increasing interest in ontologies in the last few years has led to emerging ontology-based context modeling approaches. Ontology-based context models have been independently developed by several research groups [4,10,15,16]. This trend reflects the potential of ontology-based approaches to address critical issues including formal context representation, knowledge sharing and logic-based reasoning about context. However, unlike context ontologies above (except [16]), which limited the use of ontologies only to represent context information and relationships between context information, we have employed the ontological modeling approach to express privacy vocabulary. By taking advantage of the real power of ontologies as an enabler for logic-based inference, personal privacy agents could have efficient privacy check and matching processes to judge the acceptability of data collectors' collecting policies, therefore taking appropriate actions on behalf of individuals.

7 Conclusions and Future Work

This paper has presented an attempt to develop intelligent agent technologies to enable individuals to manage their privacy requirements toward dynamic context-aware environments with relative ease. The privacy agent approach taken by our work serves as a supplement to privacy protection through conventional access control and security mechanisms.

The development of the privacy vocabulary and ontology presented in this work is among the first step to provision automated preference mechanisms in privacy agents. We are developing a rule-based privacy policy language to be used for expressing and reasoning context-dependent privacy preferences. In addition, we plan to enhance our privacy protection framework by taking into account the deployment of security mechanisms and a trust model in the proposed context-aware architecture.

References

1. Cranor, L., Dobbs, B., Egelman, S., Hogben, G., and Schunter, M.: The Platform for Privacy Preferences 1.1 (P3P1.1), http://www.w3.org/P3P/, July 2005
2. Hong, J.I., and Landay, J.A.: An Architecture for Privacy Sensitive Ubiquitous Computing. In Proceedings of the 2nd international conference on mobile systems, applications, and services (MobiSYS '04), Boston, USA, June 6-9, 2004, ACM Press, (2004) 177–189
3. Cuellar, J., Morris J., Mulligan, D., Peterson, J., and Polk J.: Geopriv Requirement, RFC 3693, IETF, http://www.ietf.org/rfc/rfc3693.txt, February 2004
4. Gandon, F. L., and Sadeh, N. M.: Semantic Web Technologies to Reconcile Privacy and Context Awareness. Web Semantics Journal Vol.1 (3), (2004)
5. Hengartner, U., and Steenkiste, P.: Access Control to Information in Pervasive Computing Environments. In 9th Workshop on Hot Topics in Operating Systems, Hawaii, May 2003
6. Zhang, G. and Parashar, M.: Context-aware Dynamic Access Control for Pervasive Applications. In Proceedings of Communication Network and Distributed Systems Modeling and Simulation Conference, San Diego, USA (2004)
7. Langheinrich, M.: Personal Privacy in Ubiquitous Computing – Tools and System Support. PhD thesis, No. 16100, ETH Zurich, Zurich, Switzerland, May 2005.
8. Hull, R., Kumar, B., Lieuwen D., and Patel-Schneider, P.: Enabling Context-Aware and Privacy-Conscious User Data Sharing, In Proceedings of the IEEE International Conference on Mobile Data Management, Berkeley, USA, January 2004, 187-198.
9. Zhang, N., and Todd, C.: A Generic Context-aware Architecture Prototype, In Proceedings of London Communication Symposium 2005, London, UK, September 2005
10. Wang X. H., Zhang, D. Q., Gu, T., and Pung, H. K.: Ontology Based Context Modeling and Reasoning Using OWL, In Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PerCom'04), Orlando, USA, March 2004, 18-22
11. Cranor, L., Langheinrich, M., and Marchiori, M.: A P3P Preference Exchange Language 1.0 (APPEL1.0) W3C Working Draft, April 2001, http://www.w3.org/TR/P3P-preferences
12. Smith, M.K., Welty, C., and McGuinness, D. L.: OWL Web Ontology Language Guide, http://www.w3.org/TR/owl-guide/ , February 2004
13. Jena Semantic Web Framework, http://jena.sourceforge.net/
14. Myles, G., Friay, A., and Davies, N.: Preserving Privacy in Environments with Location-based Applications. IEEE Pervasive Computing, Vol.2 (1), (2003) 56-64
15. Henricksen, K., Livingstone, S., and Indulska, J.: Towards a Hybrid Approach to Context Modeling, Reasoning and Interoperation, In Proceedings of the 1st International Workshop on Advanced Context Modeling, Reasoning, and Management in UbiComp'04, Nottingham, England, September 2004
16. Chen, H., Finin, T. and Joshi, A.: Semantic Web in the Context Broker Architecture. In Proceedings of the 2nd IEEE Conference on Pervasive Computing and Communications (PerCom'04), Orlando, Florida, USA, March 2004, 277-286