Using Privacy Policies to Protect Privacy in UBICOMP

Yee, George

Publisher's version / Version de l'éditeur:

Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications, 2005

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

*Using Privacy Policies to Protect Privacy in UBICOMP **

Yee, G.
March 2005

* published in Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005 – Volume II). Tamkang University, Taiwan. March 28-30, 2005. NRC 47432.

Canada

Using Privacy Policies to Protect Privacy in UBICOMP[1]

George Yee
Institute for Information Technology
National Research Council Canada
George.Yee@nrc-cnrc.gc.ca

Abstract

With the increasing deployment of sensors, intelligent devices of all sizes, and wireless networking, ubiquitous computing environments are getting closer and closer to reality. Research in UBICOMP has focused on enabling technologies, such as networking, data management, security, and user interfaces [1]. However, privacy for UBICOMP has been a contentious issue and the privacy concerns that have been raised suggest that privacy may be the greatest barrier to the long-term success of UBICOMP [2]. In this paper, we propose that privacy in UBICOMP can be managed using privacy policies. We propose a UBICOMP model for protecting privacy using privacy policies and derive the content of a UBICOMP privacy policy.

1. Introduction

The popular concept of ubiquitous computing (UBICOMP) began with Mark Weiser's seminal paper [3] in 1991, where he introduced the vision of a person interacting with hundreds of nearby computers wirelessly networked and distributed in his physical environment. Weiser's goal was to emphasize the person rather than the machine, focusing on helping the person in his/her daily life. Weiser's vision has not been realized, but researchers are getting closer and closer. Research has focused on enabling technologies, such as networking, data management, security, and user interfaces [1]. However, privacy for UBICOMP has been a contentious issue and the privacy concerns that have been raised suggest that privacy may be the greatest barrier to the long-term success of UBICOMP [2].

The objectives of this paper are to a) propose a model for protecting privacy using privacy policies in UBICOMP and b) derive the content of personal privacy policies suitable for protecting privacy in UBICOMP. Space limitations for this paper does not allow an in-depth presentation of a). Privacy policy content for UBICOMP will be defined first using requirements from privacy legislation. This will form a minimum content set which will be augmented using privacy risk analysis for UBICOMP from [2].

In the privacy literature for UBICOMP, Hong and Landay [4] have focused on providing tools for designing individual privacy-sensitive applications, while Hong et al [2] suggest the use of privacy risk models to make application designers aware of the privacy concerns and risks in their design. Di Pietro and Mancini [5] have considered broad measures for upholding privacy, such as the use of logical borders to limit propagation of information and the application of anonymous user identities to protect the real users. This work is a departure from the above works in the sense that privacy protection is driven by privacy policies across all applications, rather than focusing on the design of individual applications to respect privacy. Interestingly, Di Pietro and Mancini [5] make a comment (not pursued in their paper) in their conclusion that portends the approach of this work, when they wrote "Finally, we emphasize the need for an easy to configure and manageable personal profile to control the interactions among the many HWW devices that could surround a user. The enforcement of such a profile could be a means to preserve the user's personal privacy." "HWW" stands for hand-held/wearable wireless devices. Finally, there are works targeted at Internet e-services environments dealing with privacy policy derivation [9], privacy policy negotiation [10, 11], privacy policy compliance [12], and treating the protection of privacy as a kind of rights management [13].

Section 2 proposes our UBICOMP model for privacy protection using privacy policies. Section 3 derives the content of a personal privacy policy for UBICOMP. Section 4 discusses some implementation aspects. Section 5 gives conclusions and plans for future research.

2. UBICOMP model for privacy protection using privacy policies

We present our model for using privacy policies to protect privacy. Our model has the following features:

- Users encounter ubiquitous device environments and interact with the devices in each environment sharing their personal information (data sharers) and observing the personal information of others (data observers). A user can be both a data sharer and a data observer. The devices in each environment are networked either wirelessly, with physical lines, or some combination of both.
- Each ubiquitous environment is owned by some organization.
- The organization has a privacy policy that specifies its private information requirements for each device in its environment.
- Each user has a personal privacy policy specifying what private information he/she is willing to share or wishes to observe (or both willing to share and wishes to observe) and under what terms (e.g. retention time) for each device.
- Prior to interacting with the devices of a ubiquitous environment, the user electronically submits his/her personal privacy policies to the organization that owns the environment.
- The organization electronically verifies whether or not the user's privacy policies are compatible with its own. If compatible the user is told he/she can proceed to interact (sharing or observing) with the devices in the environment as determined by the user's privacy policies. If incompatible, there are three possibilities: 1) the user is told which clauses in his/her policy are incompatible and consequently, with which devices he/she can interact (possibly none, this is similar to the way P3P policies for websites work [14]), 2) the user can negotiate with the organization to resolve all the incompatibilities (similar to [10, 11]), 3) some combination of 1) and 2). Note that data observers are observing data only according to the wishes of the data sharers as expressed in the sharers' privacy policies, so their observations are legitimate.
- There is one device within each ubiquitous environment that serves as the *Privacy Controller*. This device has the following features:
  - Receives the user's privacy policy and processes it for compatibility; optionally performs policy negotiations with the user; these two functions are carried out by a *Policy Module (PM)*;
  - Has a *Compliance Module (CM)* that ensures that the organization complies with the user's privacy policies (similar to [12]);
  - Has a *Controller Module (OM)* that controls the other devices within the environment with respect to user accessibility and private information flow.
- Devices in the environment other than the Privacy Controller need to have appropriate interfaces that inter-work with the Privacy Controller to control the device's accessibility to the user (outcome of the policy evaluation) and the flow of private information. For devices with very limited computational capability (e.g. embedded or wearable), these interfaces will have to be commensurate with the computational capability (for these devices the quantity of shared private information will be limited too).

Figure 1 illustrates our proposed UNICOMP model. Some implementation aspects of this model are discussed in Section 4. We next turn our attention to deriving the contents of a personal privacy policy for UBICOMP.

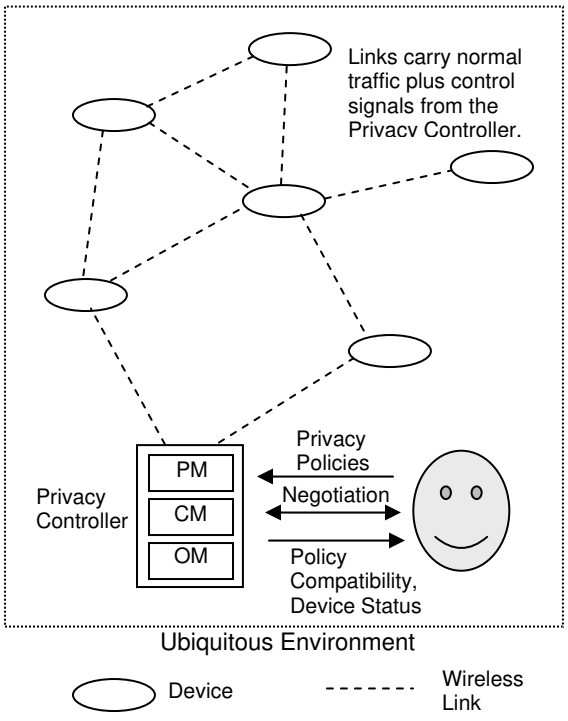

Figure 1. UBICOMP model for privacy protection using privacy policies

3. Privacy policies for UBICOMP

3.1. Privacy legislation

To protect personal privacy, legislative bodies in many countries have enacted legislation that define personal

information and spell out the obligations of a service provider organization with respect to the personal privacy of a service consumer. Such legislation is applicable for this work by interpreting a service provider organization as the organization that owns the ubiquitous computing environment and the service consumer as the user of the environment. In Canada, privacy legislation is enacted in the *Personal Information Protection and Electronic Documents Act (PIPEDA)* [6] and is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* [7] recognized as a national standard in 1996. This Code consists of ten Privacy Principles [7] that for convenience, we label as CSAPP. Data privacy in the European Union is governed by a very comprehensive set of regulations called the Data Protection Directive [8]. The CSAPP (Table 1) is representative of principles behind privacy legislation in many countries, including the European Union., and is therefore appropriate to use here.

Table 1. CSAPP - The Ten Privacy Principles from the Canadian Standards Association [7]

Principle	***Description***
1. Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals accountable for the organization's compliance with the privacy principles.
2. Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. Consent	The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.
4. Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure, and Retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. In addition, personal information shall be retained only as long as necessary for fulfillment of those purposes.
6. Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards	Security safeguards appropriate to the sensitivity of the information shall be used to protect personal information.
8. Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Individual Access	Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

In the following, we use CSAPP.n to denote Principle n of CSAPP. Principle CSAPP.2 implies that there could be different organizations requesting the information, thus implying a *collector* attribute. Principle CSAPP.4 implies that there is a *what* attribute, i.e. what private information is being collected. Principles CSAPP.2, CSAPP.4, and CSAPP.5 state that there are *purposes* for which the private information is being collected. Principles CSAPP.3, CSAPP.5 and CSAPP.9 imply that the private information can be disclosed to other entities (other organizations or applications), giving a *disclose-to* attribute. Principle CSAPP.5 implies a *retention time* attribute for the private information. Thus, from the CSAPP we derive 5 attributes of personal private information, namely *collector*, *what*, *purposes*, *retention time*, and *disclose-to*.

Based on the above examination of CSAPP, the contents of a privacy policy should, for each item of private data, identify a) *collector* – which organization wishes to collect the information, b) *what* - the nature of the information, c) *purposes* - the purposes for which the information is being collected, d) *retention time* – the amount of time for the organization to keep the information, and e) *disclose-to* – the other entities to which the information will be disclosed. The attribute grouping <collector, what, purposes, retention time, disclose-to> is called a *privacy rule*. A personal privacy policy then consists of a header section followed by one or more privacy rules, where there is one rule for each item of private information. The header consists of the fields: *Policy Use* (for what application?), *User* (name of the user who owns the policy), and *Valid* (period of time during which the policy is valid). Figure 2 shows an

example personal privacy policy based on the above development.

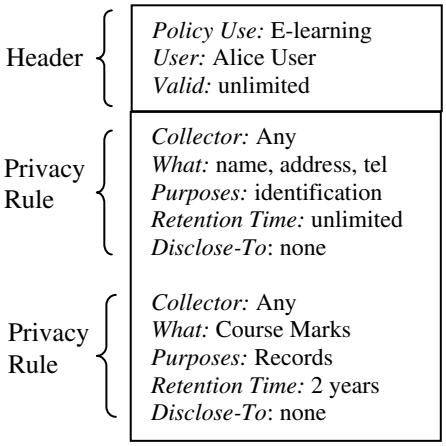

Figure 2. Example personal privacy policy based on the Ten Privacy Principles [7]

The content of the above personal privacy policy is the minimum needed to satisfy legislative requirements for data sharers. Data observers can use a similar format to specify what data they are interested in observing and under what conditions. In addition, it is generic since it is based on legislation that applies across the board. We therefore specialize it to UBICOMP by testing it against a set of questions (Table 2) given by Hong et al [2] for privacy risk analysis of UBICOMP. This testing will identify the extent to which the policy contents address the privacy risks as well as the additions needed to address any remaining risks. The result will be a personal privacy policy for UBICOMP that satisfies legislative requirements. Hong et al organized their questions into two groups: one group looking at the social and organizational context in which an application is embedded, the other group examining the technology used to implement the application. We use PRAQ to refer to these questions and PRAQ.n to refer to question n within PRAQ.

Table 2. PRAQ – Privacy risk analysis questions for UBICOMP from [2]

	Social and Organizational Context
1.	Who are the users of the system? Who are the *data sharers*, the people sharing personal information? Who are the *data observers*, the people that see that information?
2.	What kinds of personal information are shared? Under what circumstances?
3.	What is the value proposition for sharing personal information?
4.	What are the relationships between data sharers and data observers? What is the relevant level, nature, and symmetry of trust? What incentives do data observers have to protect data sharers' personal information (or not, as the case may be)?
5.	Is there the potential for malicious data observers (e.g., spammers and stalkers)? What kinds of personal information are they interested in?
6.	Are there other stakeholders or third parties that might be directly or indirectly impacted by the system?
	Technology
7.	How is personal information collected? Who has control over the computers and sensors used to collect information?
8.	How is personal information shared? Is it opt-in or is it opt-out (or do data sharers even have a choice at all)? Do data sharers push personal information to data observers? Or do data observers pull personal information from data sharers?
9.	How much information is shared? Is it discrete and one-time? Is it continuous?
10.	What is the quality of the information shared? With respect to space, is the data at the room, building, street, or neighborhood level? With respect to time, is it real-time, or is it several hours or even days old? With respect to identity, is it a specific person, a pseudonym, or anonymous?
11.	How long is personal data retained? Where is it stored? Who has access to it?

We consider each question in turn, as follows:

- PRAQ.1: The users of the system are the data sharers and the data observers. However, it is important in privacy management for data sharers to specify who the data observers are, and vice versa, and this is not reflected in our collector attribute, which refers to the organization that owns the system. Thus we make the following changes: i) for sharer policies, replace "Collector" with "Data Observers", ii) for observer policies, replace "Collector" with "Data Sharers", and iii) insert "Organization", reflecting the organization owner of the UBICOMP system, in the header.
- PRAQ.2: This is taken care of by our policy using the "what" and "purposes" attributes.
- PRAQ.3: The value proposition is reflected in the "Policy Use" attribute. Users would engage (submit their privacy policies) the ubiquitous system only if they receive some value in doing so.
- PRAQ.4: This question assesses the level of trust between data sharers and data observers to see if data sharers would be comfortable in sharing their information. In addition, the question attempts to reinforce that trust by asking if the data observer has incentives to protect the data sharers' information. In our use of privacy policies, the organization has to

comply with the users' privacy policies and we require foolproof compliance mechanisms (e.g. [12]) to be in place. Therefore, users are assured that their wishes are respected. Trust is still relevant for us, since it will partially determine whether or not users will use the system. In our privacy policies, trust will be reflected in the choice of data observers specified.

- PRAQ.5: This question is intended to determine if the private information shared needs protection. If not, the data sharer can freely share his/her information. This question is taken care of by our use of privacy policies since we require protection of private information using appropriate security mechanisms as well as policy compliance.
- PRAQ.6: This question aims to find out if other stakeholders or third parties could suffer some loss of privacy due to the way the system works. This is a valid question that should be answered and appropriate remedies taken prior to system deployment. However, it does not require a change to our privacy policy.
- PRAQ.7: The user supplies the personal information when requested by the system. The organization owner of the ubiquitous system controls the computers and sensors used to collect personal information. This question does not impact our privacy policy.
- PRAQ.8: There is opt-in/opt-out in the sense that the user can opt-out if his/her privacy policy is not compatible with the organization's privacy policy to the granularity of a single item of private information. Data observers pull information from users. This question does not impact our privacy policy.
- PRAQ.9: The information shared can be discrete, one-time, or continuous. Whatever form it takes is protected by a privacy policy. This question also does not require changes in our privacy policy.
- PRAQ.10: This question assesses the quality of the information to see if it needs protection in terms of risk. It is like PRAQ.5. Again, in our use of privacy policies, all private information is protected. This question does not require changes in our privacy policy.
- PRAQ.11: Retention time is part of our privacy policies. Data observers specified in sharers' policies together with the sharers have access. The data is stored in either a central, distributed, or combined central and distributed fashion, as determined by the design of the ubiquitous system.

The above tests of our privacy policy have revealed changes needed due to PRAQ.1. In addition, we would like to add a "Device" attribute to the header, since our model for privacy protection requires a privacy policy per device. Figure 3 shows the format of the new data sharer personal privacy policy for UBICOMP. The data observer privacy policy is the same except with "Data Sharers" instead of "Data Observers".

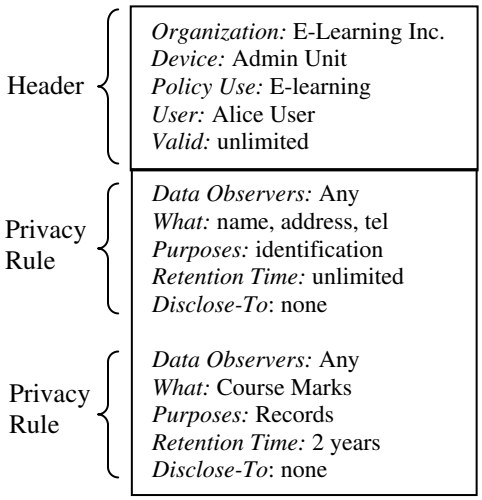

Figure 3. Example personal privacy policy for UBICOMP

4. Implementation notes

We consider here some implementation aspects of our scheme for protecting personal privacy.

How does the user come up with his/her personal privacy policies (one for each device of interest)? We propose that the organization gives the user its policies that the user can then modify to his/her liking through a suitably easy to use tool. The organization's privacy policies would also be made up of policies that are similar to Figure 3, except perhaps without the "*User*" field in the header and without the "*Data Observers*", "*Data Sharers*" fields in the privacy rules. Alternatively, the user can employ a scheme similar to [9], where the privacy rules can be selected according to the level of privacy desired using a privacy slider. The organization is assumed to have sufficient resources to generate its privacy policies.

Since users access the ubiquitous system at different times, a user who is waiting to observe data from a data sharer will need to be informed once the data sharer accesses the system. The frequency of such updates will need to be determined.

What does compatibility of policies mean? There needs to be a way of comparing two policies using some measure of compatibility such as levels of privacy [16]. However, our policies need to be compared based on the "*Data Observers*", "*Data Sharers*" fields as well, which is an added dimension not covered in [16].

Protocols need to be defined for the control signals between the Privacy Controller and the devices in the ubiquitous environment.

Privacy policies need to be amenable to machine processing. Policy languages such as APPEL [15] and EPAL [17] that are XML-based are good choices.

The organization should satisfy CSAPP.1 and CSAPP.2. CSAPP.2 can be satisfied through the organization giving the user its privacy policies, as mentioned above for use by the user in creating his/her policies. CSAPP.3 is automatically satisfied when the user submits his/her policy to the organization.

Finally, the user's private information needs to be secured from attack (CSAPP.7). Appropriate security mechanisms will need to be applied or developed and applied.

5. Conclusions and future research

We have proposed a UBICOMP model with the purpose of protecting personal privacy using personal privacy policies. We have also derived the content of such policies for use in our model. We suggest the use of privacy policies as an effective way to protect privacy in a ubiquitous computing environment. Such use gives the user flexibility and control over his/her private information, and inspires user trust in the system that in turn increases the likelihood that the system will be used.

As future work, we plan to provide greater detail for our model by constructing a prototype to answer the implementation concerns noted above.

6. References

[1] P. Boddupalli, F. Al-Bin-Ali, N. Davis, A. Friday, O. Storz, and M. Wu, "Payment Support in Ubiquitous Computing Environments", Proceedings of the Fifth IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2003), Monterey, California, Oct. 9-10, 2003.

[2] J.I. Hong, J.D. Ng, S. Lederer, and J.A. Landay, "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems", Proceedings, ACM conference on Designing Interactive Systems (DIS2004), Cambridge, Massachusetts, August 1-4, 2004.

[3] M. Weiser, "The Computer for the Twenty-First Century", *Scientific American*, September 1991, pp. 94-100.

[4] J.I. Hong and J.A. Landay, "An Architecture for Privacy-Sensitive Ubiquitous Computing", Proceedings, The Second International Conference on Mobile Systems, Applications, and Services (MobiSys2004), Boston, Massachusetts, June 6-9, 2004.

[5] R. Di Pietro and L.V. Mancini, "Security and Privacy Issues of Handheld and Wearable Wireless Devices", *Communications of the ACM*, Vol. 46, No. 9, Sept. 2003.

[6] Department of Justice, Privacy Provisions Highlights, http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

[7] Canadian Standards Association, "Model Code for the Protection of Personal Information", retrieved Sept. 5, 2003 from: http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=English

[8] European Union, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", unofficial text retrieved Sept. 5, 2003 from: http://aspe.hhs.gov/datacncl/eudirect.htm

[9] G. Yee, L. Korba, "Semi-Automated Derivation of Personal Privacy Policies", Proceedings, 15th IRMA International Conference, New Orleans, Louisiana, May 23-26, 2004.

[10] G. Yee, L. Korba, "Bilateral E-services Negotiation Under Uncertainty", Proceedings, The 2003 International Symposium on Applications and the Internet (SAINT2003), Orlando, Florida, Jan. 27-31, 2003.

[11] G. Yee, L. Korba, "The Negotiation of Privacy Policies in Distance Education", Proceedings, 14th IRMA International Conference, Philadelphia, Pennsylvania, May 18-21, 2003.

[12] G. Yee, L. Korba, "Privacy Policy Compliance for Web Services", Proceedings, 2004 IEEE International Conference on Web Services (ICWS 2004), San Diego, California, July 6-9, 2004.

[13] S. Kenny and L. Korba, "Adapting Digital Rights Management to Privacy Rights Management", Computers & Security, Vol. 21, No. 7, November 2002, 648-664.

[14] W3C, "The Platform for Privacy Preferences", http://www.w3.org/P3P/

[15] W3C, "A P3P Preference Exchange Language 1.0 (APPEL 1.0)", retrieved April 22, 2004 at: http://www.w3.org/TR/P3P-preferences/

[16] G. Yee, L. Korba, "The Comparison of Privacy Policies", Proceedings, 16th IRMA International Conference, San Diego, California, May 15-18, 2005.

[17] Enterprise Privacy Architecture Language (EPAL), available at: http://www.zurich.ibm.com/security/enterprise-privacy/epal/

[1] NRC Paper Number: NRC 47432