

# Integrating Privacy Aspects into Ubiquitous Computing: A Basic User Interface for Personalization

Dominik Heckmann

Saarland University  
D-66123, Saarbrücken, Germany  
heckmann@dfki.de

## Abstract

Ubiquitous computing will have a unifying influence on user modeling, context-awareness and resource-adaptivity. The idea of this paper is to suggest a basic mechanism to integrate privacy aspects into mobile and ubiquitous computing. The user is enabled to annotate situational and user specific data with privacy settings. The three mayor sections described in this paper cover the "personalization user interface", the world-model "UbisWorld", and the basic data structure of "situational statements".

## Keywords

Privacy Aspects, Ubiquitous Computing, Blocks World, User Modeling, Context Awareness, Situational Statements

## Introduction

In user modeling, context-awareness and resource-adaptive computing, information about the object of interest is gathered and further processed into higher level knowledge in order to receive hypothesis about possibilities for adaption of the system's behavior. Often, data from low-level sensors are integrated into the inference process.

Ubiquitous computing serves here as a motivation for a unifying view, since in a ubiquitous computing scenario, all three kinds of adaptation will interact in a distributed way. Users will live together with intelligent spaces and devices that communicate with each other.

Now the problem arises, that human-related adaptation and data storage needs a specialized treatment for privacy. One reason are law-restrictions (see e.g. [Hinde, 2003]) but the second - more urging - argument is the acceptance of the user. In mobile and ubiquitous computing the treatment of privacy issues seems to be especially difficult, since not every system will be able to interact with the user directly. In this paper we will describe a privacy user interface as part of a user model editor that was introduced in [Heckmann, 2002]. The implementation is under construction.

According to Kobsa ( see e.g. [Kobsa, 2003] ), there are four main arguments, that influence the users' decisions about allowing personalization with their personal data. The first one is: "1. What will be done with their personal data?". This question focuses on the *purpose*. The second one is: "2. Who is going to use their personal data?". This question focuses on the *access* and the *recipient*. The third one is: "3. Which kind of personal data is used?". Thus a differentiation between the type of data is implied. The fourth one is: "4. In which mood or situation is the user

currently?". This last point suggests "user-adaptive user-adaptivity", which probably forms an impossible recursion.

In this paper, we try to contribute to the question that arises on "how to analyze and integrate these privacy aspects into mobile and ubiquitous computing". In the first section we will look at the privacy issues in more detail. In the following section, we describe situational statements, that already allow the combination of privacy information with the information content on the most basic level, see [Heckmann, 2003] for a more profound investigation. In the third section, we will introduce "UbisWorld", a test-bed system for ubiquitous computing, and a basic user interface for personalization. In this paper we do NOT investigate the problem of security in mobile or distributed systems, like encryption techniques or how to defeat attacks. We believe that this problem is orthogonal to privacy. We start with a trust based approach while later security extensions are expected. This work is highly under progress.

## 1 Privacy

Representing, storing and communicating information about the user like her age, or her current time pressure, blood pressure, skin conductivity or information about her interests, goals and plans need special privacy treatment. The most important one is that the user should be able to "control" the systems' private information handling. One point will be the *inspection* of the stored data, another point will be the possibility to *change* it. Another point will be the possibility to turn the whole user-adaptivity off and on, either on a global or individual basis of systems or locations.

The four main arguments from Kobsa for accepting personalization from the introduction part could be extended to the fifth one: "5. How long will the personal data be stored?". This question rises the argument of *retention*, see [P3P, 2003] for a more detailed description. And the sixth one: "6. Can the user inspect or delete the personal data or turn-off the whole user adaptivity?". This questions raises the demand for *control*.

To summarize, the purpose, access, recipient, owner, retention, control and inspection should play an important role in the treatment of privacy.



Figure 1: public access, research purpose, short retention

As an example, figure 1 represents the three variables access, purpose, and retention with the following intended meaning:

- "public access" means that everybody can be the recipient of this information.
- "research purpose" means that this information should not be used for commercial purposes, but only for research issues.
- "short retention" means that this information must be deleted within days.

Figure 2 represents the three variables access, purpose, and retention with the different selected meaning:



Figure 2: friends, commercial purpose, middle retention

- "friend access" means that only selected friends (friendly systems or locations) can (should) be the recipient of this information. In order to use this fact, a friendship-relation between the owner of the information and the possible recipient must be defined.
- "commercial purpose" means that this information can also be used for commercial purposes like product recommendation.
- "middle retention" means that this information must be deleted within month.

These privacy settings could be attached to individual statements about the situation, or to user model parameters like "time pressure", or even to parameter classes like "all user demographics". See figure 3 for a partial taxonomy of user model parameters.

In terms of knowledge representation, the question arises, if these basic bits of privacy and content information can be represented in a uniform manner. The next section introduces the data structure of situational statements.

## 2 Situational Statements

The challenge of this section is to use a basic, semantically founded, uniform data structure that is simple but still expressive enough to cover all representational needs. An extended triple, which is based on RDF resources is introduced as well as an XML application for so called "Situational Statements". The basic idea behind situational statements is that they should form the main data structure for representation and communication about user-, context-, and resource-adaptation, while all other data structures are surrounding them. The meta level information (here, especially the privacy aspects) of a statement like "who is responsible for this piece of information", or "what is the confidence value for it", is combined with the actual content of the statement like "the cognitive load of this person is high". Furthermore the basic information content is enriched with temporal and spatial constraints like "this property holds between now and tomorrow". Thus, situational statements can contain content data, constraint data and privacy meta data. The underlying concepts are defined in the following sections.

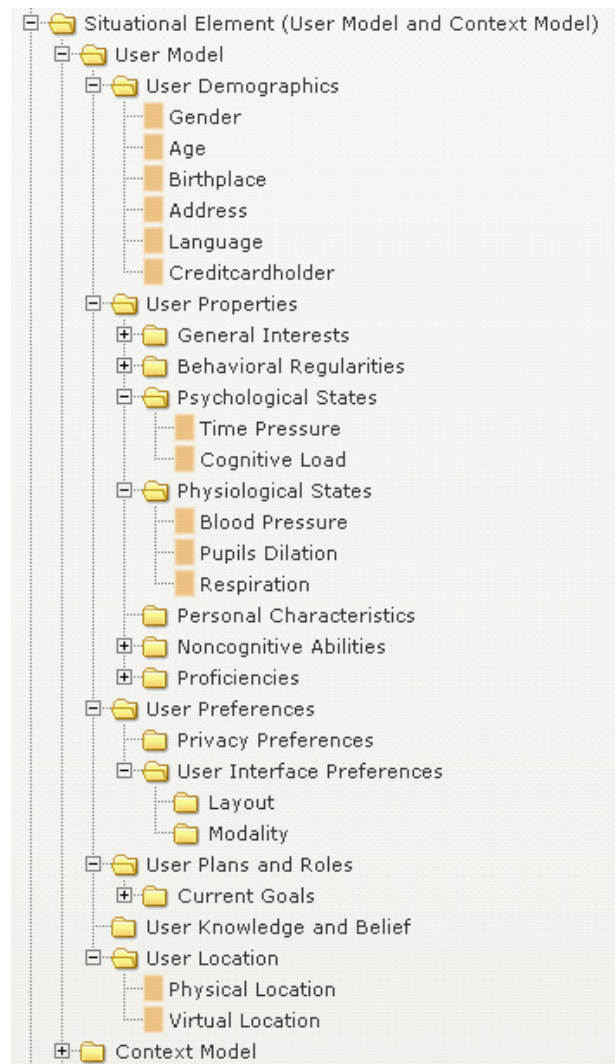


Figure 3: A Part of the UserOL Taxonomy

### 2.1 The Model with Resources and Triples

The underlying model is based on the ideas of RDF/RDFS, (see e.g. W3C or [Champin, 2001]), which means that it works with descriptions about "resources" that are qualified with URIs and namespaces. Resources in this sense here should not be mistaken with the "device" resources, instead they can be considered as being the basic entities of a graph. Situational statements identify resources with qualified Uniform Resource Identifiers (URI) as described in [Lassila *et al.*, 1999], with the slight difference that URIs can have an optional fragment identifier: a text added to the URI with a "#" between them. Situational Statements consider every qualified URI (with or without fragment identifier) as a full resource by itself. Since every qualified URI is unique, one could consider resources as linking unique IDs to the referred objects and concepts. Resources are not in the main focus but they allow to simplify the representation of complex structures. In order to keep the representation simple, the qualified URIs can be abbreviated by XML namespaces. For the sake of clarity, we will rather use the XML non-expanded notation; that is, prefixes UserOL: and UbisWorld: will be used instead of <http://www.u2m.org/UserOL#> and <http://www.u2m.org/UbisWorld#> respectively. Thus, resources are conceptual mappings to entities,

and with situational statements, a predefined structure of such mappings is suggested.



Figure 4: The Model of the Basic Triple

### Basic Triples

The base element of the model about situational statements is the (RDF) triple: a resource (the subject) is linked to another resource (the object denoting the value) through an arc labelled with a third resource (the predicate). We will say that the subject has a property predicate valued by object. See figure 4 for a graphical representation. For example, the triple in figure 5 could be read as "the subject *Peter of UbiWorld* has the property *CognitiveLoad of the UserOL Ontology* with the value *high*".



Figure 5: "Peter has a high cognitive load"

### Extended Triples

An "Extended Triple" is a 7-tuple, that extends the basic triple (subject, predicate, object) with temporal- and spatial restrictions as well as meta-data about ownership & privacy and evidences & confidence. The idea is to allow more powerful, but still structured, statements about situations. See figure 6 for a conceptual graph of a general extended triple. The new arrow type in the extended triples has the meaning of "adding information" to the basic triples.

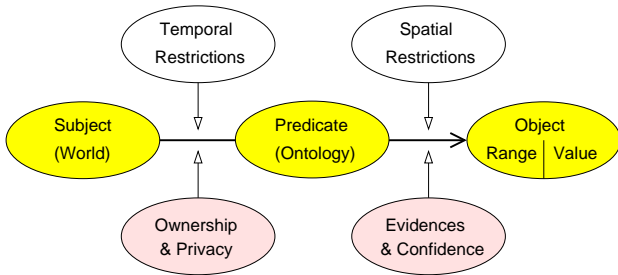


Figure 6: The Concept for Extended Triples

## 2.2 The Semantics of this Model

In order to allow a clear interpretation of this model, there is a need to define the meaning of the concept. In a logical approach, these sets can be defined properly. The axioms, constraints and relations could also be expressed formally but here only some of them are listed.

- The content is only valid according the time constraint, which means between the start time and the added duration. After expiry the content is either unknown or the confidence value is adjusted.
- The content is only valid as long no new information from the same source is available. This means that the content can be overwritten.

- The confidence value lays between 0 and 1 and is based on a list of evidences.
- The situational statements may only be used if the owner allows this according to his privacy settings.
- The location of measurement is, if applicable, of interest and can be expressed.

The meaning of situational statements can differ from application to application, but a clear semantic definition can be supported. In this description most details are underspecified. In the following subsection, an XML representation for a special instance of situational statements is presented.

## 2.3 XML for Situational Statements

Using XML as knowledge representation language has the advantage that it can be used directly in the Internet environment.

```
<SituationalStatement>
  <content>
    <subject><UbiWorld:Peter /></subject>
    <predicate><UserOL:CognitiveLoad /></predicate>
    <object>High</object>
  </content>
  <constraint>
    <start>2003-05-17T14:03:34</start>
    <duration>600s</duration>
    <location>not-specified</location>
  </constraint>
  <privacy>
    <owner><UbiWorld:Peter /></owner>
    <access><UbiWorld:friends /></access>
    <purpose><UbiWorld:research /></purpose>
    <retention><UbiWorld:short /></retention>
  </privacy>
</SituationalStatement>
```

This representation is based on the RDF resource idea, which means that the resources are only stated or linked as IDs. The semantics for example for `<UserOL:CognitiveLoad />` is defined in a document with the name "UserOL". See figure 3 for a small part of its taxonomy. One advantage of this modularized approach is that the ontology and the representational formalism are separated, which means that everybody could use his own ontology while using the same representation and tools. Another idea of this approach is to enable communication about partial user models via the Internet. With the help of the newly defined XML application UserML (see <http://www.u2m.org/>) the user and context information can be send to the nearest user interface. In the next section the user interface for UbiWorld is presented. UbiWorld is based on these privacy issues and the situational statements from section 2.

## 3 Ubi's World

Human-computer interaction in ubiquitous computing needs a uniform virtual world model in order to simulate, represent and compare research issues. The examples of this paper are embedded in a world model called Ubi's World, see [Heckmann, 2003] Ubi's World can be used to represent some parts of the real world like an office, a shop, a museum or an airport. It represents persons, objects, locations as well as times, events and their properties and features. The main focus lays on issues of ubiquitous computing, user modeling and privacy. Apart from the representational function, Ubi's World can be used for simulation, inspection and control.

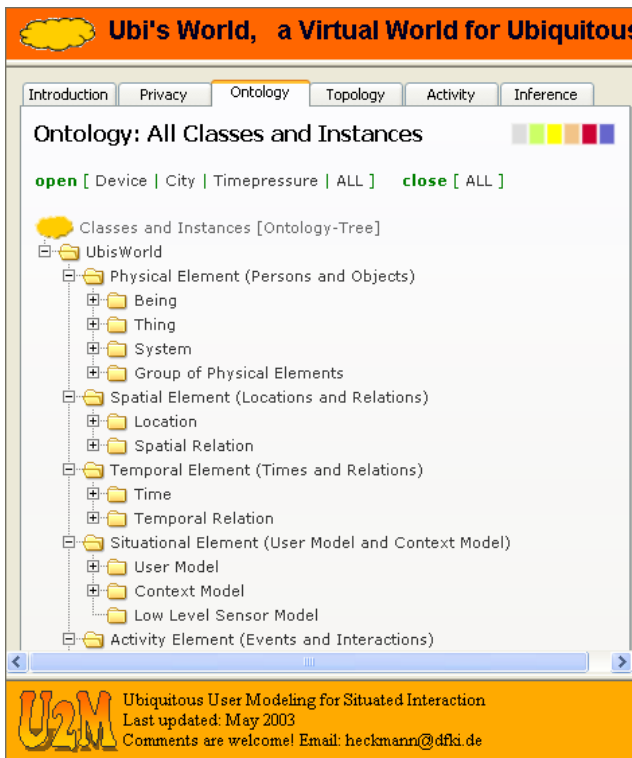


Figure 7: "The top-level taxonomy-tree of UbisWorld"

### 3.1 Ontology

One key feature of our approach is to allow an open uniform ontology that covers all elements from physical objects, locations, times, their properties and features, but also the activity and the inference elements. The complete ontology can be found at <http://www.u2m.org/ubisworld.htm>. The top-level taxonomy tree of this ontology can be seen in figure 7. We use an unfoldable tree to represent this graph, which means that multiple inheritance is realized by branch-copying.

#### Physical Elements

With physical elements we think of persons, devices, objects, furniture, goods, food and so on. Device elements are for example: Keyboard, Display, Mouse, Speaker, Microphone, Projector, IR Bark, ID TAG, Notebook, Mobile Phone and so on.

#### Spatial Elements

Spatial elements are rooms, buildings, cities, streets and so on. All spatial and physical elements can be spatially arranged. Thus we define spatial relations like "is-nested-in".

#### Other Element Types

Other elements are "Temporal Elements", with timestamps and temporal relations, "Situational Elements" with parameters about users, systems, location and so on. A situational parameter for a location could for example be the noise level, or the available light, a situational parameter for a person could for example be his blood pressure, his cognitive load or his interests. A situational parameter about a system could for example be its remaining battery power. "Activity Elements" describe the changes in the world and the most prominent one is "A-moves-to-B". And "Inference Elements" define the rules of intelligent instrumented environments.

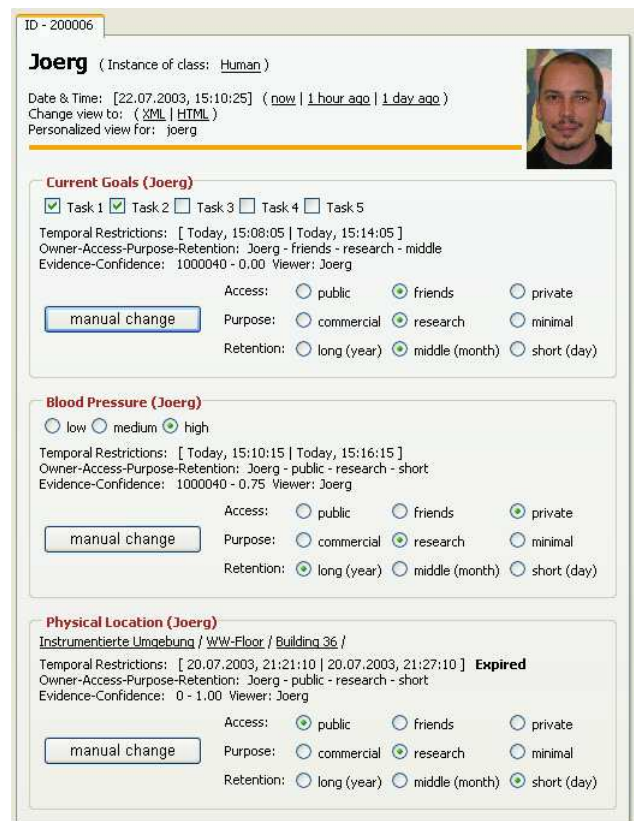


Figure 8: "Personalized Privacy Editor for Joerg"

### 3.2 Virtual Representatives

Each element of the described world has as a virtual counter part an own page in the world wide web, where descriptions, parameters and meta information can be inspected and changed according to the privacy regulations.

### 3.3 The integrated Privacy Editor

If an an intelligent environment or any interaction system collects data about a user, this person can inspect and edit this model in a human readable format in it's virtual representative web page. Figure 8 shows for example the web page of "joerg", adapted to the fact that joerg himself is logged in. He can inspect his current location and is able to change it on this page. He can also inspect his individual privacy settings and change them. Thus this page serves as an editing tool for user models of different user-adaptive systems. This feature can be of high interest especially in ubiquitous computing, since not every ubiquitous user-adaptive system will have a user interface by it's own.

Figure 9 shows the web page of "virtual joerg", adapted to the fact that not he himself, but a friend is logged in. This friend can see the current goals and the physical location of joerg, but not the blood pressure, since this information is private. As a friend, he can only inspect this information, but not change it.

The version of the same page for a public viewer or recipient is even more restricted. Figure 10 shows that the values of the "current goals" of joerg are hidden, but still the predicate "current goals" is stated, which expresses, that there is information about joergs current goals, but they are not available for everybody. A possible extension at this point could be the allowance of negotiation.

ID - 200006

**Joerg** (Instance of class: Human)

Date & Time: [22.07.2003, 15:28:24] ( [now](#) | [1 hour ago](#) | [1 day ago](#) )  
 Change view to: ( [XML](#) | [HTML](#) )  
 Personalized view for: dominik

**Current Goals (Joerg)**

Task 1  Task 2  Task 3  Task 4  Task 5

Temporal Restrictions: [ Today, 15:26:40 | Today, 15:32:40 ]  
 Owner-Access-Purpose-Retention: Joerg - friends - research - middle  
 Evidence-Confidence: 1000040 - 0.00 Viewer: Dominik

**Physical Location (Joerg)**

Instrumentierte Umgebung / WWW-Floor / Building 36 /

Temporal Restrictions: [ 20.07.2003, 21:21:10 | 20.07.2003, 21:27:10 ] **Expired**  
 Owner-Access-Purpose-Retention: Joerg - public - research - short  
 Evidence-Confidence: 0 - 1.00 Viewer: Dominik

Figure 9: "Virtual Joerg's" page view for friends

ID - 200006

**Joerg** (Instance of class: Human)

Date & Time: [22.07.2003, 15:30:41] ( [now](#) | [1 hour ago](#) | [1 day ago](#) )  
 Change view to: ( [XML](#) | [HTML](#) )

**Current Goals (Joerg)**

This information is not public.

Temporal Restrictions: [ Today, 15:26:40 | Today, 15:32:40 ]  
 Owner-Access-Purpose-Retention: Joerg - friends - research - middle  
 Evidence-Confidence: 1000040 - 0.00 Viewer: Anonym

**Physical Location (Joerg)**

Instrumentierte Umgebung / WWW-Floor / Building 36 /

Temporal Restrictions: [ 20.07.2003, 21:21:10 | 20.07.2003, 21:27:10 ] **Expired**  
 Owner-Access-Purpose-Retention: Joerg - public - research - short  
 Evidence-Confidence: 0 - 1.00 Viewer: Anonym

Figure 10: "Virtual Joerg's" public page view

## Conclusion

This paper describes the three mayor topics: privacy, situational statements and the world model "UbisWorld" with the integrated privacy editor. In order to gain the user's acceptance of user-adaptivity in ubiquitous computing, the arguments of inspect-ability, control, privacy ( owner, access, purpose, retention, viewer ) are integrated into the basic data structure of situational statements, the world model and the user interface. The main technical idea of "Situational Statements" is to use the concept of resources in order to point to global available ontologies like UserOL. The blocks-world for ubiquitous computing with the ontology-based semantics, is described here. The privacy user interface allows the owner of the personal information to implicitly give it free for public access, or grant the information only to selected users or systems. In this paper, we have put the focus on the aspect of integrating privacy.

## Acknowledgments

This work is supported by the European Post-Graduate College "Language Technology and Cognitive Systems".

## References

- [Kobsa, 2003] Kobsa, A. and J. Schreck. "Privacy through Pseudonymity in User-Adaptive Systems". *ACM Transactions on Internet Technology* 3 (2), 149-183 .
- [Hinde, 2003] Stephen Hinde. "Privacy legislation: a comparison of the US and European approaches". *Computers and Security*, 22(5) (2003) 378-387

- [Weiser, 1991] Marc Weiser. "The Computer for the 21st Century". *Scientific American*, 265(3) (1991)
- [Orwant, 1995] Jon Orwant. "Heterogeneous Learning in the Doppelgänger User Modeling System", *User Modeling and User-Adapted Interaction* 4 (1995)
- [Jameson, 2001] Anthony Jameson. "Modeling Both the Context and the User", *Personal Technologies*, 5 (2001)
- [Heckmann, 2001] Dominik Heckmann. "Ubiquitous User Modeling for Situated Interaction", *UM2001*
- [Heckmann, 2002] Dominik Heckmann. "Towards User Modeling in Ubiquitous Computing", *AIMS2002*
- [Heckmann, 2003] Dominik Heckmann. "Introducing Situational Statements as an integrating Data Structure for User Modeling, Context-Awareness and Resource-Adaptive Computing", *ABIS2003*
- [Wasinger, 2003] Rainer Wainger et. al. "Adapting Spoken and Visual Output for a Pedestrian Navigation System, based on given Situational Statements", *ABIS2003*
- [Heckmann, 2003] Dominik Heckmann. "UbisWorld for IE6" <http://www.u2m.org/ubisworld.htm>
- [P3P, 2003] W3C P3P. "Platform for Privacy Preferences (P3P) Project" <http://www.w3.org/P3P/>
- [Lassila et al., 1999] Ora Lassila and Ralph R. Swick. Resource Description Framework (RDF) Model and Syntax Specification. W3C recommendation, feb 1999.
- [Champin, 2001] Pierre-Antoine Champin. RDF tutorial for developers. <http://www710.univ-lyon1.fr/~champin/rdf-tutorial/>, april 2001
- [Bray et al., 1999] Tim Bray, Dave Hollander, and Andrew Layman. Namespaces in XML. W3C recommendation, jan 1999.