Una propuesta para un modelo de privacidad en entornos activos

Abraham Esquivel, Pablo A. Haya, Germán Montoro, Xavier Alamán
Dpto. de Ingeniería Informática y Telecomunicación
UAM-EPS
C. Francisco Tomas y Valiente, 11 28049 Madrid
Abraham.Esquivel@estudiante.uam.es,{Pablo.Haya, German.Montoro, Xavier.Alaman}@uam.es

Resumen

El proyecto UCAT cuenta con un entorno activo formado por diversos elementos, que producen información contextual, publicada en una pizarra central accesible a todos los elementos activos para compartir información e interaccionar entre si. A continuación presentamos un modelo que pretende integrar privacidad, restringiendo y protegiendo la información contextual.

1. Introducción

Los crecientes esfuerzos por aumentar el poder de cálculo de los microprocesadores, la disminución de su tamaño y el avance de las comunicaciones digitales, todo esto a un precio bastante económico, hace factible incluir toda esta tecnología en casi cualquier dispositivo u objeto. De esta forma se impulsa así la visión de Mark Weiser[1,2] sobre el concepto que él bautizara como *Ubiquitous Computing* (también llamada *Pervasive Computing*), en la que imaginaba que los objetos que están a nuestro alrededor se les podría incrustar una computadora y así establecer comunicación entre ellos, para brindar servicios personalizados en las tareas de los humanos.

Desde entonces, muchos grupos de investigación han iniciado proyectos para explorar varias facetas de la visión iniciada por Weiser, empleando la computadora para entender el habla, reconocer expresiones faciales e interactuar con los humanos de manera natural e inteligente, haciendo nuestra vida más fácil e incluso rompiendo algunas barreras para personas de tercera edad o discapacitados. Sin embargo, el hecho de incluir computadoras en casi cualquier lugar y cualquier objeto, abre nuevos temas de discusión, como son la privacidad y la seguridad.

La Computación Ubicua junto con los Entornos Activos son la base de lo que actualmente se conoce como Inteligencia Ambiental. Un Entorno Activo puede ser cualquier espacio (una sala de reuniones, una habitación, un laboratorio…) que tiene la capacidad de interactuar con los usuarios de forma proactiva.

Los Entornos Activos son el marco en el cual desarrollamos nuestra investigación. Actualmente, nos encontramos involucrados en el proyecto U-CAT que persigue el desarrollo de un entorno integrado que facilite la realización de actividades educativas desde cualquier lugar mediante la utilización de distintos dispositivos físicos (ordenadores personales, portátiles, teléfonos móviles y PDAs), y en diferentes contextos y situaciones

La privacidad ha sido tema de numerosas publicaciones y desde diversos enfoques, legal, social, económico y tecnológico [3]. Este último es de particular interés para la Inteligencia Ambiental, donde se conjugan numerosos dispositivos que acumulan información acerca del usuario y sus actividades.

Otro tema muy relacionado es el de la seguridad, que aplicada a Entornos Activos, adopta restricciones muy peculiares, en términos de conectividad, capacidad de cálculo y consumo de energía [4].

En la siguiente sección, presentamos algunos trabajos afines a nuestra investigación, continuamos explicando el modelo de privacidad propuesto, seguimos con una descripción del modelado del entorno, en seguida, indicamos como es que representamos el contexto, después con una explicación de como implementamos el modelo de privacidad, continuamos ejemplificando un escenario y finalizamos con las conclusiones y trabajos futuros.

Actas del Simposio de Computación Ubicua e Inteligencia Ambiental, UCAmI2005, pp.381-388
ISBN: 84-9732-442-0

2. Trabajos previos

La privacidad es un tema tratado con anterioridad en otros marcos de investigación. La red Internet es uno de los que actualmente está teniendo más incidencia. El estándar abierto P3P [5] desarrollado por el *World Wide Web Consortium*, es un estándar de reciente creación que automatiza la manera en que los usuarios obtienen control sobre el uso de su información personal en los sitios web que visitan. Este protocolo permite introducir restricciones en los navegadores, de modo que no se envíe ningún tipo de información a terceros sin nuestro consentimiento. Esta medida de prevención facilita el control de privacidad en lo concerniente al comercio electrónico, sistemas *on-line*, y navegadores de Internet, aunque sin éxito en entornos inteligentes.

Langenheinrich en [6] elaboró una reseña de los aspectos históricos de privacidad, mostrando su evolución desde inicios del siglo XIX, retomando el impacto constitucional y legal referenciado por Warren y Brandeis en [7]. Langenheinrich hace énfasis sobre el concepto de privacidad de información, y lo puntualiza como un problema principal en los entornos activos.

El mismo Langenheinrich elabora un estudio para detectar las diferencias existentes entre la computación ubicua y las demás disciplinas informáticas, y sus conclusiones finalmente son cuatro factores clave:

- *Ubicuidad*. Dado que la infraestructura está por todo el entorno, afecta inherentemente a todo las facetas de la vida cotidiana.
- *Invisibilidad*. La infraestructura no está necesariamente a la vista de los usuarios, por lo que no saben con certeza en que momento y en que lugar están empleando una computadora.
- *Captación*. Los datos de entrada para las múltiples computadoras inmersas en el entorno pueden captar prácticamente todo lo que los usuarios hacen y dicen.
- *Aumento de memoria*. Toda interacción con el entorno, tiene el potencial de ser almacenada, consultada o reproducida.

Nosotros creemos que estos aspectos establecen la diferencia respecto a otras disciplinas, dado que en el mundo de la computación ubicua, las acciones comunes se vuelven inseguras, como el simple hecho de charlar y mencionar en voz alta, por ejemplo, el código de la alarma de seguridad, pues no tenemos certeza de cuantos ni cuales dispositivos están almacenando esa información.

En el ámbito que queremos tratar la privacidad, no nos interesa como producto de una invasión maliciosa, sino como el producto de la convivencia diaria, en un entorno donde hay reglas sociales establecidas y en las que se pueden producir una invasión accidental.

Un aspecto importante a tener en cuenta es que la información producida por varias entidades genera conflictos, el principal, ¿a quién le corresponde determinar el nivel de privacidad? [8].

Hay dos estudios de particular interés con un enfoque afín a nuestra investigación. El primero es de Scott Lederer [9], donde en conjunto con un equipo de la Universidad de Berkeley, elaboró estudios preliminares, análisis y experimentos, dirigidos a detectar los diferentes estados que debería cubrir el diseño de un proyecto para elaborar una interfaz de usuario que administrara la privacidad personal en un entorno de computación ubicua.

Parte de sus resultados, son dos aspectos relevantes a la hora de que la información personal es divulgada, el primero es, ¿Quién es el receptor de la información?, y el segundo, ¿En que contexto se revela la información?

Lamentablemente sus resultados no eran muy alentadores como fundamento para su interfaz propuesta, aunque si revela las preferencias de los usuarios respecto al manejo de su información.

La segunda investigación que nos es relevante, es la elaborada por Tuchinda en [10], dentro del proyecto *Oxygen* del MIT. Tuchinda plantea resolver el problema de la privacidad implementando un control de acceso.

- *Regla de seguridad*. El usuario puede acceder a los recursos, porque tiene el privilegio de usarlos.
- *Regla de privacidad*. El solicitante accede a los recursos, solo si no viola la privacidad de otro usuario.

En su investigación, agrega un tercer aspecto a evaluar, que es la Calidad del Servicio, como un indicador que mide la comodidad del usuario.

Concluye que en un entorno activo, las reglas de un control de acceso no pueden ser rígidas, y la privacidad puede ser violada, solo en caso de que

el beneficio obtenido sea mayor (como en una emergencia).

3. Propuesta de privacidad

Tratar de definir el término privacidad, es una tarea complicada, ya que su definición depende de la época y problemas a los que se aplicó, aunque fundamentalmente podemos partir de que es un asunto de valores e intereses.

Acorde a nuestro criterio, un punto de partida apropiado para una definición de privacidad que se ajuste a entornos activos, es la descrita por Alan Westin [11]:

"Es el derecho de los individuos, para determinar por si mismos cuándo, cómo y qué información privada se divulga."

Tomando en cuenta los resultados de Lederer en [8], sería más conveniente que distinguiéramos de la definición anterior dos partes:

- *La privacidad como derecho del propietario de la información*. Es el derecho de los individuos para determinar por si mismos a quién (un usuario, un grupo, todos los usuarios), dónde (lugar de publicación), cómo (medio de divulgación) y para qué (uso de la información) se divulga la información privada.
- *La privacidad como propiedad de la información*. Es una característica que establece el propietario de la información sobre la posibilidad de que otros usuarios puedan acceder a ella.

De acuerdo a la primer parte, podemos detectar cinco elementos clave para nuestro modelo: Propietario, Receptor, Medio, Contexto y Uso.

1. *Propietario*. Es quién decide como se administra la privacidad de la información. El propietario puede ser una persona, o un grupo. En este segundo caso hay que resolver cuál es el criterio que se aplica. Para ello existen varias soluciones, ya sea por unanimidad, por mayoría, por la opción más restrictiva …
2. *Receptor*. Es quién recibe el derecho para consultar la información. El receptor puede ser tanto otra persona como un componente software. Un aspecto importante es establecer un mecanismo de autentificación que asegure que el receptor es realmente a quién va dirigida la información.
3. *Contexto*. Otro factor de gran importancia es el contexto, tanto del propietario como del receptor. La localización es una variable contextual relevante. La privacidad que se requiere varía dependiendo de donde se está divulgando la información Por ejemplo, una reunión de socios de una firma comercial no se puede realizar en lugar público. También varía dependiendo de dónde se encuentre el propietario. Así, una persona que esta siendo grabada en video tiene reacciones distintas según se encuentre en su hogar o en un evento público. Otro aspecto importante a considerar en el contexto es el número e identidad de las personas que acompañan al receptor. Por ejemplo, si éste recibe un mensaje, el entorno puede decidir enviárselo a la pantalla más cercana, siempre y cuando no se encuentren más personas alrededor suyo, ya que de ser así se podría incurrir en una violación de la privacidad, si estas personas no fueran de la confianza del propietario.
4. El *medio* de comunicación empleado para difundir la información cobra relevancia para el propietario de la información, ya que puede establecer diferentes restricciones de privacidad según emplee un dispositivo u otro.
5. *Uso*. El último de los elementos entra en juego una vez que la información llega al receptor. El destinatario puede hacer mal uso de ella, como almacenarla, modificarla, reproducirla o emitirla hacia otras entidades sin el permiso del propietario.

Respecto a la privacidad como propiedad de la información, creemos que la privacidad es un atributo de la información que puede ser manipulado por su propietario para restringir su divulgación. En nuestro modelo, la información desde el punto de vista del receptor es privada o pública, y el propietario tiene la posibilidad de establecer esta propiedad a uno de esos dos valores dependiendo tanto del receptor como del contexto.

Para poder aplicar las normas de privacidad en un Entorno Activo, debemos tener previamente algún medio que nos permita reflejar las diferentes entidades existentes y el contexto que están generando.

3.1. Modelado de la información

En esta sección, definiremos la terminología empleada en el Entornos Activo desarrollado para el proyecto UCAT. La representación del contexto en este proyecto contempla algunas de las ideas expresadas por Dey en [12], para representar personas, lugares y recursos. Esto se hace mediante la definición de conceptos (o clases) que sirven como plantillas, a partir de las cuales son creadas instancias, también llamadas entidades.

Cada entidad pertenece a un concepto, y se representa mediante un nombre y un conjunto de propiedades. Cada propiedad tiene un nombre y un valor que puede ser una literal o alguna otra entidad. En este caso, se establece una relación entre la primera entidad y la segunda. Las relaciones son unidireccionales, aunque para cada relación siempre se puede definir la inversa.

Finalmente, se pueden definir conjuntos de parámetros que pueden ir asociados tanto a un concepto, o a una entidad, o a una propiedad o una relación.

3.2. Capa de contexto

La proliferación de las redes de comunicación y la diversidad de protocolos [13], complican la integración de dispositivos en un entorno. Proponemos una capa de contexto que sirve de interfaz entre los diversos dispositivos de cómputo, hacia la integración de un entorno activo [14]. Creemos que un modelo centralizado del mundo real es el medio más óptimo de lograr la interacción entre los dispositivos.

La capa de contexto proporciona, primero, un repositorio donde las entidades son almacenadas. Y segundo, una interfaz que se encarga de abstraer los detalles de los protocolos de comunicación con los dispositivos físicos.

La implementación de la capa de contexto da origen a una estructura de datos global, llamada pizarra [15]. Esta pizarra almacena un modelo abstracto del mundo, donde se almacena la información más importante relacionada al entorno (incluyendo a los usuarios). Por lo tanto, cada dispositivo, usuario y recurso del entorno activo estará representado mediante una entidad en la pizarra. Además, contiene una representación del flujo de información existente entre los dispositivos físicos (micrófonos, altavoces, cámaras, pantallas, etc.).

```
<entity name="name" type="type">
 <property name="name">
  <paramSet name="name">
   <param name="name">value</param>
   <param name="name">value</param>
    ……
  </paramSet>
 </property>
 <relation name="name" dest="name"/>
</entity>
```

Figura 1. Representación de una entidad en XML.

La información de la pizarra es utilizada por los diferentes dispositivos para comprender el contexto y adaptarse a éste. Cada pizarra es un servidor que puede ser accedido mediante el protocolo cliente-servidor TCP/IP. HTTP ha sido escogido como el protocolo de transporte por su simpleza y amplia cobertura. Para el intercambio de información entre las aplicaciones y la pizarra en el servidor, se emplea el lenguaje XML.

La pizarra proporciona las siguientes operaciones básicas: *Add* (agrega dinámicamente entidades a la pizarra), *Remove* (recíproco al anterior), *Get* (consulta valores de la pizarra), *Set* (cambia un valor de la pizarra, y comunica el cambio al contexto, en si, altera el mundo físico), *AddRelation* (captura la información contextual, al relacionar entidades), *RemoveRelation* (recíproca a la anterior), *Subscribe* (permite que una aplicación subscriba cambios a la pizarra) y *Unsubscribe* (una aplicación deja de obtener los cambios del contexto).

3.3. Implementación

Como se menciona en los apartados anteriores, las entidades que forman la pizarra, están representadas en lenguaje XML.

En la figura 1 se pueden apreciar cuatro partes básicas de la entidad (*entity*), formada por propiedades (*property*, *relation*), y conjuntos de parámetros (*paramSet*) que complementan la definición de la entidad.

La implementación de nuestra propuesta de privacidad se basa en añadir un conjunto de parámetros denominado *privacy*. Este conjunto

delimitará la privacidad de toda la entidad, o de una propiedad.

A continuación se reflejan los diferentes parámetros que forman parte del conjunto *privacy*. Para integrar las soluciones, implementamos un administrador de privacidad, que se auxilia de cuatro parámetros, que son: tipo (*type*), receptores (*receivers*), entorno (*environment*) y uso (*use*).

El primero de ellos es el tipo (type) que delimita el alcance que puede tener la información. El propietario la puede clasificar en tres tipos diferentes:

- Privada. (*private*) Una entidad, propiedad o relación de tipo privada solo será accesible a su propietario. Por lo tanto, nadie diferente a él, podrá accederla.
- Pública. (*public*) Cuando una entidad, propiedad o relación es de tipo público, cualquier otra entidad o relación distinto de su propietario podrá consultarlo e incluso modificarle.
- Protegida. (*protected*) Una entidad, propiedad o relación de tipo protegido, se auxiliará de una lista elaborada por el propietario de la entidad, que contiene el identificador de las entidades que tienen permitido el acceso.

Siguiendo con los elementos que integraban la definición de privacidad descrita anteriormente, un elemento importante consistía en asegurar que la información era entregada al receptor correcto. Para ello, integramos el parámetro receptores (*receivers*), en el que el propietario de la entidad, define los identificadores de todas las entidades a las que se les permite el acceso.

Los identificadores que pueden ir dentro del parámetro *receptores* pueden corresponder tanto a una entidad individual (una persona, o un componente software) como a un grupo. Por lo tanto, cuando una entidad quiere acceder a los recursos de otra, se verifica si su identificador se encuentra dentro del parámetro *receptores* o si se encuentra dentro de uno de los grupos incluidos en este parámetro.

Otro elemento que se describió anteriormente es la localización del propietario de la información. Integramos un tercer parámetro entorno (*environment*), en el que el propietario de una entidad, define en que lugares se aplicará un determinado conjunto de parámetros *privacy*. Así, cuando se quiere acceder a una información, primero se verificará en que entorno está el propietario, y en función de la localización se aplicará la privacidad del conjunto de parámetros que incluya dicho entorno.

Por último, añadimos un cuarto parámetro uso (*use*) que permite restringir el uso de la información una vez que el receptor ya ha accedido a ella.

Clasificamos el uso de la información en tres tipos diferentes:

- *Almacenable*. (*Recording*) es el permiso que otorga el propietario de la entidad a su receptor para que pueda almacenar una copia de su información.
- *Difusión*. (*Broadcasting*) permiso otorgado para que la información se pueda difundir a otras entidades.
- *Visualizado*. (*viewing*) permiso otorgado para que una persona pueda ver la información.

De esta manera tratamos de restringir lo que el receptor final de la información pueda hacer con ella, una vez que le pertenece.

La segunda parte de la privacidad, consistía en que el propietario de la información puede manipular ciertos atributos de la información. Establecemos que la información representada en la pizarra de contexto, tiene dos atributos el primero, que sea de solo lectura (*read*), y el segundo que se pueda modificar (*write*).

Anteriormente mencionamos que en el parámetro receptores (*receivers*), se encuentra una lista de entidades y grupos que pueden acceder a la información. De modo que cada identificador de entidad o grupo está concatenado al permiso de lectura y/o escritura sobre la información (+r, +w, +rw).

En la figura 2, mostramos un ejemplo de cómo añadimos el modelo de privacidad a las entidades de la pizarra.

Como se puede apreciar en la figura 2, la entidad puede definir una privacidad global, por lo tanto, su ámbito alcanza a sus propiedades y relaciones definidas dentro de ella. En el ejemplo de la figura se ha establecido que la entidad es pública, lo cual significa que en principio cualquier entidad podría acceder a las propiedades y relaciones de la entidad.

Ahora bien, la propiedad *localización* se define como privada, lo cual restringe el acceso a esa propiedad a todos los receptores.

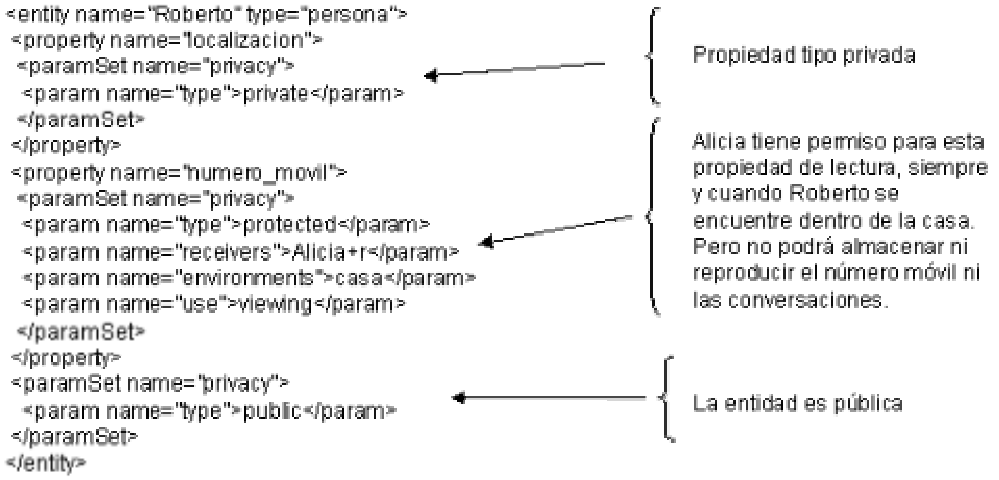

Figura 2. Una entidad con parámetros de privacidad

En cambio, la segunda propiedad *número_móvil* se establece como protegida. Esto implica que se podrá acceder según las restricciones que imponen los parámetros *receptores*, *entornos* y *uso*.

También se puede establecer la privacidad sobre una relación. Si la relación es privada ésta no se mostrará al receptor cuando se acceda a la entidad. En cambio, si la relación es pública o protegida, el receptor podrá conocer de la existencia de la relación. Ahora bien, la entidad destino de la relación puede tener una privacidad distinta de la entidad origen, de modo, que se puede dar el caso que el receptor pueda acceder la información de la entidad origen pero no a la información de la entidad destino.

4. Escenario

Se ha desarrollado un prototipo de entorno activo. Este consiste de un laboratorio acondicionado como el salón de una casa moderna [14].

Los dispositivos instalados se dividen en tres categorías:

- *Domótica*. Se compone de varios sistemas independientes, como el portero electrónico que controla la apertura de la puerta, el sistema de tarjetas inteligentes que informa de quién está entrando en la habitación, y varios dispositivos EIB, tales como relés electrónicos para controlar las luces, interruptores, pantallas alfanuméricas, etc.
- *Información audio-visual*. incluye una televisión, dos altavoces hi-fi, varios altavoces normales, una radio, un DVD, y varias pantallas planas. Por último, una cámara de video IP permite monitorizar la actividad de la habitación.
- *Interacción vocal*. Varios micrófonos inalámbricos permiten interaccionar con un gestor de diálogos, permitiendo al usuario que se mueva libremente por la habitación.

Hay varios escenarios en los que podemos hacer pruebas del modelo de privacidad. A continuación explicamos uno:

Suponga que tenemos dos usuarios: Alicia y Roberto. Alicia se encuentra en su oficina y necesita enviar un mensaje a Roberto, que se encuentra en su casa. Ambos entornos son activos. Hay varias maneras de hacérselo llegar, SMS, correo electrónico, llamada telefónica, etc., veamos un conjunto de acciones que puede emprender Alicia para resolver su problema:

1. Como la oficina cuenta con un gestor de diálogos, Alicia le comunica que necesita enviar un mensaje a Roberto.
2. La oficina, a través del administrador de privacidad, comienza a verificar si Alicia tiene permiso de consultar la entidad de Roberto. Para ello, o bien la entidad de Roberto es de tipo pública, o bien, si es de tipo protegido,

entre los receptores se tiene que encontrar Alicia.

3. En caso de que Alicia tenga acceso a la entidad Roberto, el administrador de privacidad comenzaría a verificar a cuales de las propiedades de la entidad Roberto, tiene permiso para acceder.
4. Dentro de las propiedades de Roberto, él definió las siguientes: número_móvil, e-mail, teléfono_del_trabajo.
5. Según la figura 2., Roberto concedió autorización a Alicia de consultar su número_móvil (type="protected"), siempre y cuando él se encuentre dentro de su casa (environment="casa"). Además, el uso lo tiene limitado a (use="viewing"), lo que indica que puede hablar con Roberto, pero no puede grabar la conversación, ni difundirla.
6. El manejador de privacidad, marca el número_móvil, y comunica la llamada a Alicia.
7. Alicia puede pedir al entorno, que le pase la llamada por los altavoces, el administrador de privacidad verificará si tiene los permisos suficientes, y en caso de si tenerlos, le transfiere la llamada por este medio.
8. Ahora que sabemos que Alicia tiene los suficientes permisos para emplear los altavoces, suponga que se encuentra alguna otra persona dentro del entorno. El administrador de privacidad, negaría trasladar la salida de la llamada telefónica por los altavoces, dado de que no tiene permiso de difusión (*broadcasting*).

5. Conclusiones y trabajo futuro

En este artículo, se ha presentado un proyecto que pretende integrar privacidad a los diferentes tipos de entidades que conforman nuestro entorno activo. Se propone un modelo que busca proteger la privacidad de la información, a partir de quién puede consultar la información, en dónde se encuentra propietario, y que uso le dará. Por ahora nuestro proyecto tiene implementado un gestor de privacidad que gestiona los accesos a la información en la pizarra en función del tipo de privacidad, los receptores y el entorno. A corto plazo desarrollaremos un demostrador para comenzar a realizar pruebas que nos permitan obtener resultados que nos indiquen la eficiencia del modelo.

Un aspecto que no se contempla en el modelo es la resolución de la información. Tal como está implementado una vez que se concede el derecho se puede acceder a toda la información. En un futuro se piensa añadir para ciertas entidades la posibilidad de permitir el acceso a una misma información con baja resolución o con alta resolución.

A más largo plazo, tenemos también contemplado integrar políticas de seguridad, que nos permitan complementar la privacidad.

Agradecimientos

Este proyecto está financiado por el Ministerio de Ciencia y Tecnología con código TIN2004-03140.

Referencias

[1] Weiser M. The Computer for the Twenty-First Century. Scientific American. 265(3): 94-104, Sep 1991.

[2] Weiser M. Some computer science issues in ubiquitous computing. Communications of the ACM. July 1993 /Vol. 36, No. 7, 1993.

[3] Jürgen B., Coroama V., Langheinrich M., Mattern F. and Rohs M.: Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In: W. Weber, J. Rabaey, E. Aarts (Eds.): Ambient Intelligence. Springer-Verlag, pp. 5-29, 2005.

[4] Stajano F. Security for Ubiquitous Computing. Wiley Series in Communications Networking & Destributed Systems. 2002.

[5] http://www.w3.org/P3P/

[6] Langheinrich M.: Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Gregory D. Abowd, Barry Brumitt, Steven A. Shafer (Eds.): Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001), LNCS No. 2201, Springer-Verlag, pp. 273--291, Atlanta, USA, 2001.

[7] Warren S. and Brandeis L. The Right to Privacy. Harvard Law Review, vol. 4, pp. 193-220, 1890. http://www.swiss.ai.mit.edu/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[8] Lederer S. Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing. Research Project Report, Master of Science, Computer Science Division, University of California, Berkeley, December 2003.
[9] Lederer S., I. Hong J., Jiang X., K. Dey A., A. Landay J. and Mankoff J. Towards Everyday Privacy for Ubiquitous Computing. University of California, Berkeley, Computer Science Division, Technical Report UCB-CSD-03-1283, October 2003.
[10] Tuchinda, R.. Security and Privacy in the Intelligent Room. Master's Thesis for MIT. M. Eng Thesis, 2002.
[11] Westin, A. Privacy and Freedom. New York, NY, Atheneum. 1967.
[12] Dey A. Understanding and using context. Personal and Ubiquitous Computing, 5(1), 2001.
[13] Haya, P., Alamán X. and Montoro G. A Comparative Study of Communication Infraestructuras for the Implementation of Ubiquitous Computing. UPGRADE 2(5), 2001
[14] Haya, P, Montoro G. and Alamán X., A prototype of a context-based architecture for intelligent home environments, CoopIS, 2004.
[15] Engelmore, R., Morgan, T. Blackboard Systems. Addison-Wesley, 1998.