Some Issues for Semantic-Enabled Privacy Protection Policies in the Ambient Networks

Prof.(Dr.) Yuh-Jong Hu

Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University, Taipei, Taiwan

June-13-2008

Panel for Ambient Semantic Computing (ASC) Workshop 2008

Outline I

1 Unsolvable Issues

2 Privacy Protection on the Web

3 Privacy Protection in the Ambient Networks

4 Challenges

Need to be Clarified!

- *Please tell me where/what/why/how are possible privacy invasions in the ambient networks or other similar sensor, ubiquitous, pervasive, or invisible computing networks*

Need to be Clarified!

- *Please tell me where/what/why/how are possible privacy invasions in the ambient networks or other similar sensor, ubiquitous, pervasive, or invisible computing networks*

- *Then, I will tell you how to represent and enforce the associated semantic-enabled privacy protection languages, policies, and systems in the ambient networks.*

Need to be Clarified!

- *Please tell me where/what/why/how are possible privacy invasions in the ambient networks or other similar sensor, ubiquitous, pervasive, or invisible computing networks*
- *Then, I will tell you how to represent and enforce the associated semantic-enabled privacy protection languages, policies, and systems in the ambient networks.*
- *Finally, I will demonstrate how to proceed auditing and verification of semantic-enable privacy protection policies and systems compliant to the real world's privacy laws or regulations.*

Privacy Protection on the Web

Privacy Protection on Web 1.0

- *Privacy protection policy representation through natural language*
- *Static personal profile and digital traces collection*
- *Information disclosure policies and mechanisms are embedded in a data model, such as relational database.*
- *Do the website's privacy protection mechanisms comply with its policy announcement? People don't know!*

Privacy Protection on the Web

Privacy Protection on Web 1.0

- *Privacy protection policy representation through natural language*
- *Static personal profile and digital traces collection*
- *Information disclosure policies and mechanisms are embedded in a data model, such as relational database.*
- *Do the website's privacy protection mechanisms comply with its policy announcement? People don't know!*

Privacy Protection on Web 2.0

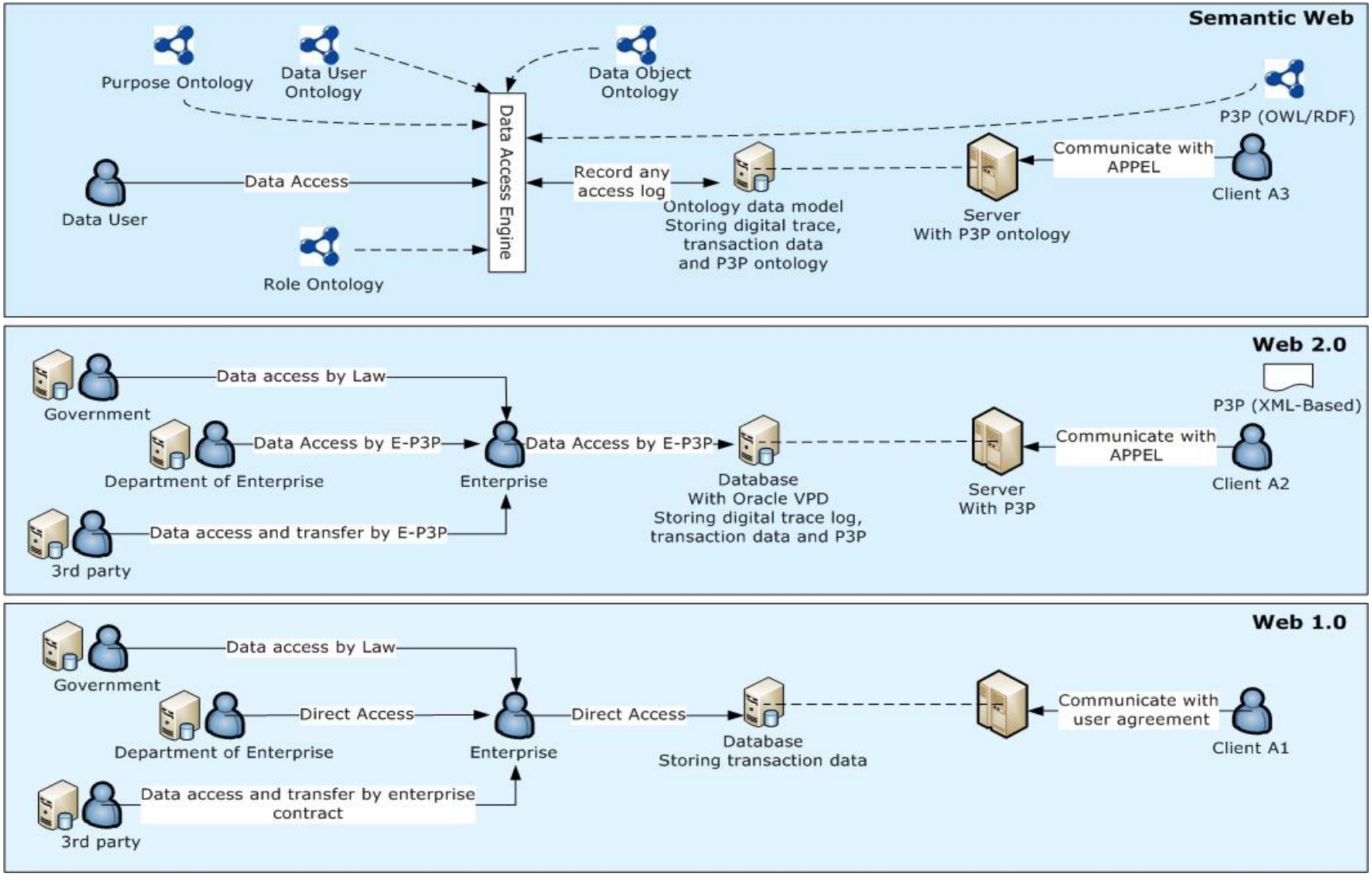
- *P3P/APPEL provides information disclosure's opt-in/opt-out and negotiation mechanisms*
- *More challenging to protect a variety of dynamic digital traces but not so many physical traces*
- *Do the website's privacy protection mechanisms comply with its policy announcement? People don't know either!*

Privacy Protection on the Web (conti.)

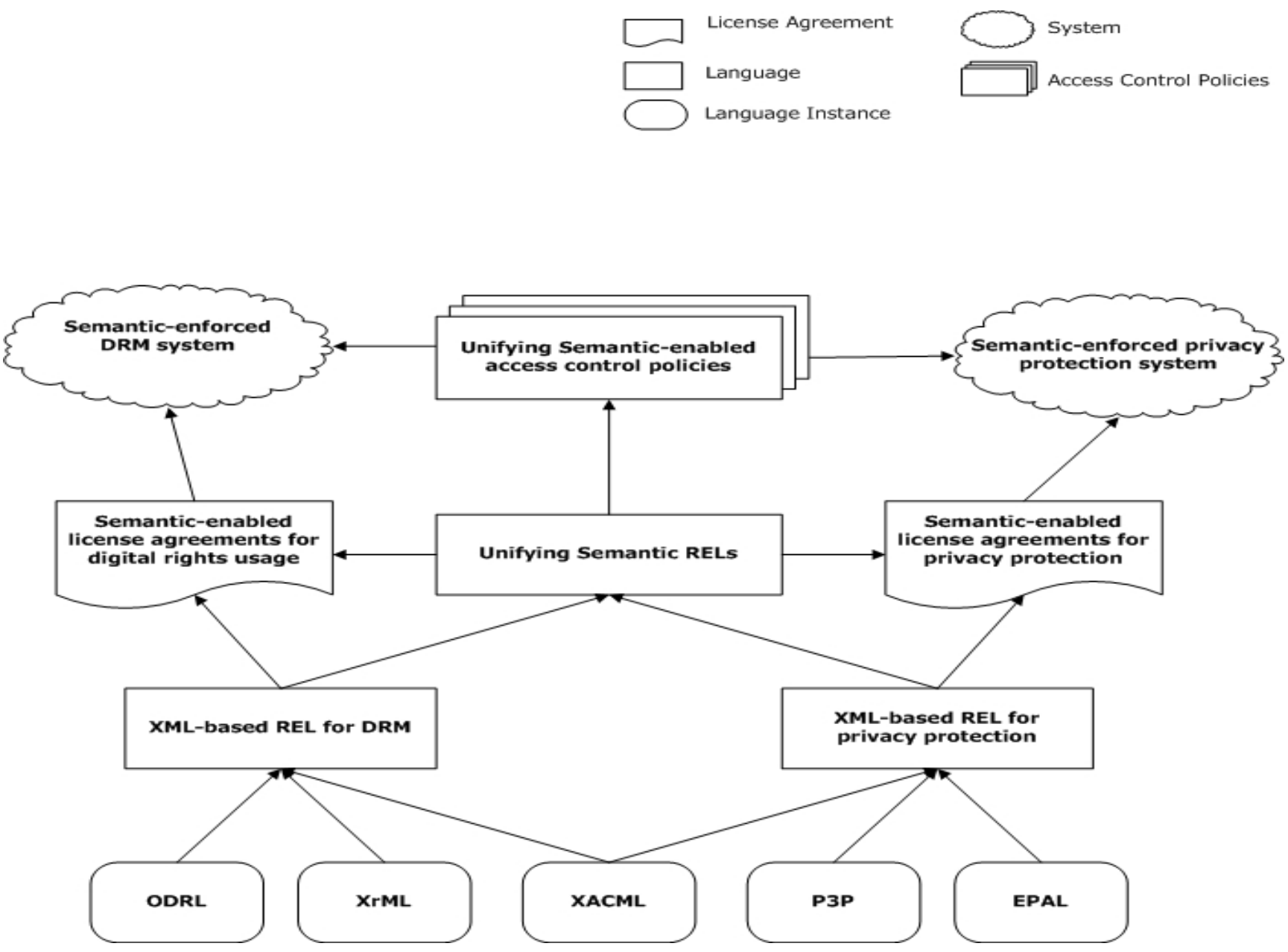
Privacy Protection on Web 3.0

- *We have a separation of privacy protection protection policies and mechanisms.*
- *Personal profile and digital traces are semantic-enabled data model.*
- *Automatic enforcement of the semantic-enabled privacy protection policies and systems*
- *Do we have sound and complete semantic-enabled policies with respect to the privacy protection laws? I don't think so!*
- *Auditing and verifying the compliance of privacy policies for privacy laws are still very hard! Why?*

Privacy Protection for Web 1.0, Web 2.0, and Web 3.0



A Unifying Semantic REL



Privacy Protection for Ambient Networks

- *Computers will provide us the right information at the right time based on conditions of interest (COI)? But you don't know my personal concern so it turns out to be conflicts of interest (COI)?*

Privacy Protection for Ambient Networks

- *Computers will provide us the right information at the right time based on conditions of interest (COI)? But you don't know my personal concern so it turns out to be conflicts of interest (COI)?*

- *Furthermore, we are unaware of who/why/what/how our personal profiles, physical traces, and digital traces are collected and used, which means the privacy invasion is much more easy! Is that true, I think so.*

Privacy Protection for Ambient Networks (conti.)

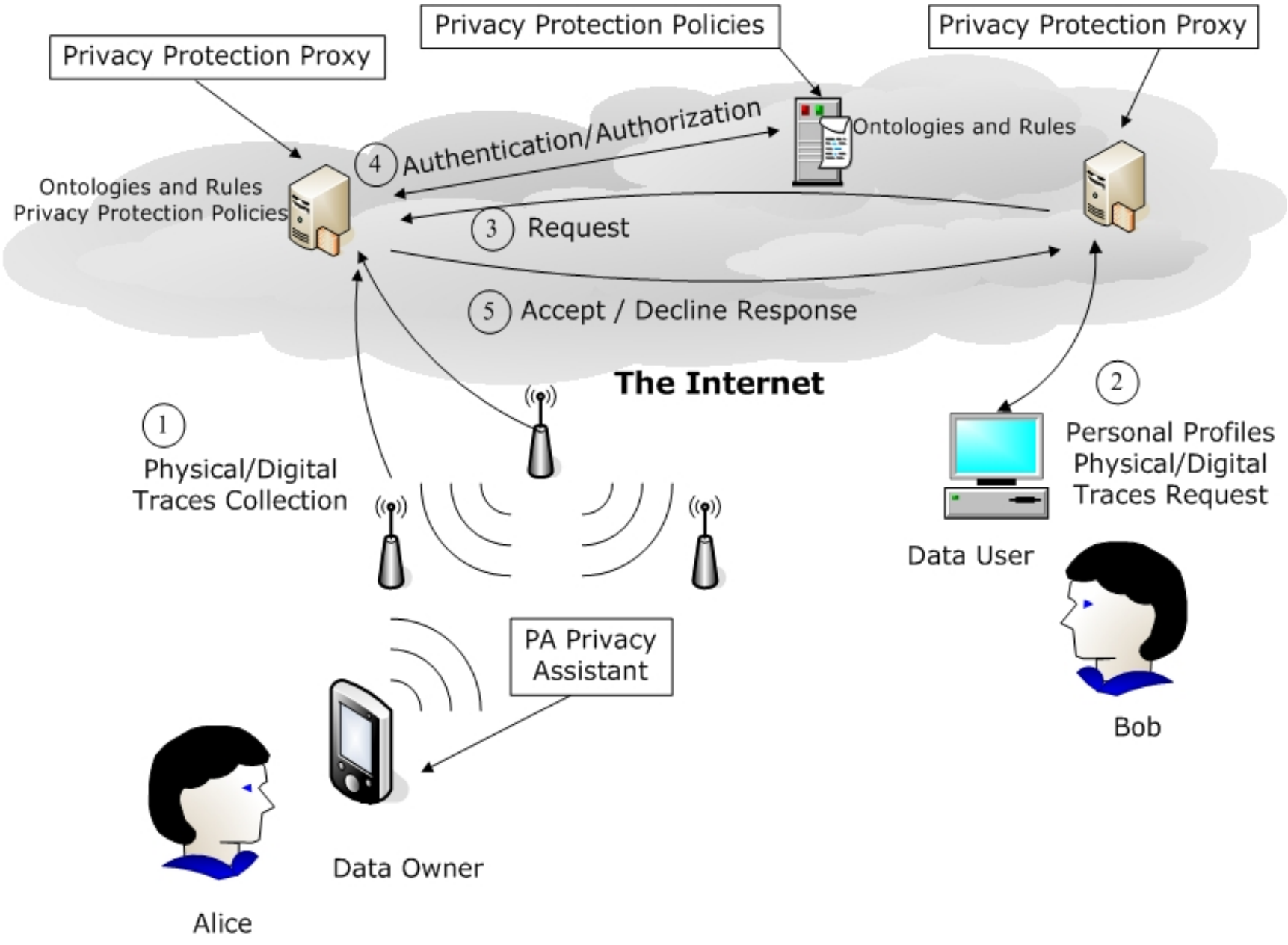
- *Do you think people in the Ubicomp community seriously consider the privacy protection issues in the first place? I don't think so. Maybe they think it is not so important or is not so urgent. The truth is, privacy protection issues are contrary to the Ubicomp system's data collection and usage purposes.*

Privacy Protection for Ambient Networks (conti.)

- *Do you think people in the Ubicomp community seriously consider the privacy protection issues in the first place? I don't think so. Maybe they think it is not so important or is not so urgent. The truth is, privacy protection issues are contrary to the Ubicomp system's data collection and usage purposes.*

- *I would said your Ubicomp's system does not possibly to know my concerns while collecting and using my own data!*
- *In fact, resolving the problem of semantic-enabled privacy protection policies and systems in the ambient networks is almost impossible! Why?*
- *Conclusion: The ambient networks or other similar networks and systems cannot be possibly widely deployed in the real world for serving human activities!*

Semantic-Enabled Privacy Protection in the Ambient Networks
revised from [3]



Challenges
Semantic-Enabled Privacy Protection in the Ambient Networks

- *How to exploit the semantic-enabled policy languages for privacy protection in the ambient networks?*
- *How to design/implement the semantic-enabled language, policies, and systems for the ambient networks?*
- *How to demonstrate the semantic-enabled of privacy protection systems in the ambient networks?*

Challenges (conti.)
Semantic-Enabled Privacy Protection in the Ambient Networks

- *Can we also apply formal semantic P3P/EPAL to the ambient networks? Yes/No!*
- *How to construct a formal semantics model on P3P/EPAL for the ambient networks?*
- *How to exploit the semantic enforcement of privacy protection policies for the ambient networks?*
- *How to implement a semantic-enabled privacy protection system for the ambient networks?*

References I


M. Langheinrich.
A privacy awareness systems for ubiquitous computing environments.
In *Proceedings of the 3rd International Conference on Ubiquitous Computing (UbiComp) 2001*.


M. Langheinrich.
Privacy by design - principles of privacy-aware ubiquitous systems.
In *Proceedings of the 4th International Conference on Ubiquitous Computing (UbiComp) 2002*, LNCS 2498.


M. Langheinrich et al.
Privacy-aware ubiquitous-computing systems: A research topic of the distributed systems group, 2008.
`http://www.vs.inf.ethz.ch`.

References II

J. D. Tygar.
Privacy in sensor webs and distributed information systems.
In M. Okada et al., editors, *Software Security*, pages 84–95.
Springer, 2003.