Semantic Web and Knowledge Management in User Data Privacy

Douglas da Silva[1], Mírian Bruckschen[1], Paulo Bridi[1], Roger Granada[1],
Alexandre Agustini[1], Renata Vieira[1],
Caio Northfleet[2], Prasad Rao[2], Tomas Sander[2]

Abstract: This paper discusses knowledge representation for privacy and accountability issues.

Use of personal information from customers is a common practice among companies and governments around the world. Knowing and applying current privacy legislation is an important requirement for IT projects. Inadequate procedures or data breaches can lead to lawsuits and loss of consumer trust for the company [1]. IT project managers are mainly aware of their business goals, but not of specific required actions to assure that the project is privacy-compliant.

Security systems are designed to protect data from unauthorized access. On the other hand, privacy systems must empower the user providing control for its own data and limiting access to it. Slightly different from these two approaches there is the perspective of organizations over client data privacy. The main concern on privacy accountability is to handle personal identifiable information in a secure way avoiding misuse. Examples of previous work in this domain are the Rei [2] and DAML Privacy [3] ontologies.

This paper[3] illustrates how ontologies can be used to model the mapping of intended actions into corresponding required actions in order to comply with privacy regulations. To this, our modeling approach uses OWL-DL [4]. In our proposed model we refer to agents and targets, similarly to Breaux and Antón [5]. An agent is the accountable part that performs "intended actions" and a target is any object that suffers or is involved in a performed intended action. Under certain specific conditions of each particular intended action, the agent will need to take other actions to be compliant with the privacy policy, which are named "required actions".

As an example consider an organization planning to transfer personal data to another country. In this case the intended action is a transborder data flow. For this kind of action

[1] Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS.
{douglas.silva,mirian.bruckschen,paulo.bridi,roger.granada}@cpph.pucrs.br, {alexandre.agustini, renata.vieira}@pucrs.br
[2] Hewlett-Packard – HP. {caio.northfleet, prasad.rao, tomas.sander}@hp.com
[3] This paper was achieved in cooperation with Hewlett-Packard Brasil Ltda. using incentives of Brazilian Informatics Law (Law nº 8.2.48 of 1991).

specific regulations apply in the European Union (EU). There are three possible cases: i) the destination country is considered adequate by the EU; ii) the destination country has a special agreement with the EU; iii) or the destination country is considered non adequate by the EU. In the special agreement case, illustrated here, it is necessary to verify if the target company has signed the special agreement. Next, an ontology excerpt that models this restriction is presented:

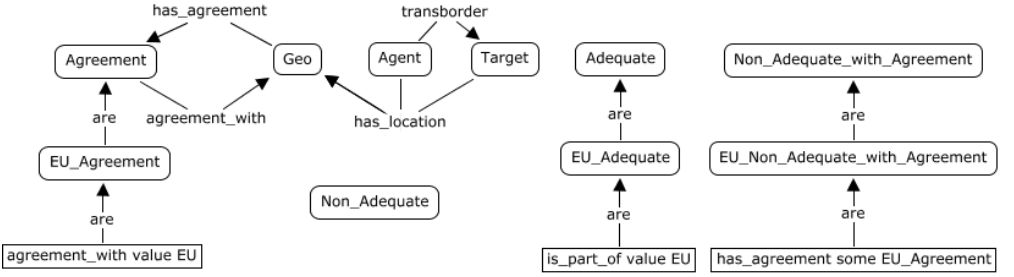

Figure 1. OWL-DL concepts and properties modeling a subset of the privacy domain.

Instances of concepts presented in Figure 1 given as an example of transborder data flow are: Organization X, Subsidiary Y, EU, Spain, USA and Safe Harbor. They are instances of Agent, Target, Geo and Agreement, respectively. In the example, Organization X is located in Spain, Subsidiary Y is located in USA and Organization X performs a transborder data flow to Subsidiary Y. Also, USA has a Safe Harbor agreement, which is an agreement with EU. Having these assertions in the ontology, some inferences can be made: Safe Harbor is classified as an EU Agreement and USA is inferred as EU Non Adequate with Agreement. The required action for case (ii) is defined by a rule. It states that if an agent located in the EU performs a transborder data flow to a non adequate country with agreement then the agent must ensure that the target has signed the agreement.

In our future work, we plan to develop a model for privacy assessment as a way to guide managers on being compliant with customers' data privacy.

References

[1] M. Mont, R. Thyne: *Privacy policy enforcement in enterprises with identity management solutions*. In: PST '06, vol. 380, pp. 1–12 . ACM, New York. (2006)

[2] L. Kagal, M. Paolucci, N. Srinivasan, G. Denker, T. Finin, and K. Sycara: *Authorization and privacy for semantic web services*. IEEE-IS-M, 19(4):50–56. (2004)

[3] G. Denker, L. Kagal, T. Finin, K. Sycara, and M. Paoucci: *Security for DAML web services: Annotation and matchmaking*. Berlin / Heidelberg. Springer. (2003)

[4] J. Heflin: *Web Ontology Language (OWL) Use Cases and Requirements*. (2003)

[5] T. Breaux and A. Antón: *Deriving semantic models from privacy policies*. In POLICY'05, pages 67–76, Washington, DC, USA. IEEE Computer Society. (2005)