Rachel Yager
VP, Citigroup

Content filtering across Organizations

We describe a use case to investigate the complexity of language required for managing inter-organizational privacy policy enforcement. The diagram below illustrates 2 organizations, each with unique organizational privacy policy requirements. We propose providing individual business users with user preference template to specify requirements for uses and distribution of the information and content.

The end user may be individual from the organization both providing and accessing content across organizations. The privacy policy to be satisfied while performing this activity will be influenced by his individual privacy requirements, plus organizational and business-specific requirements, as well as, constraints from privacy requirements of the other organizations and users.

The challenges are: (1) managing the dissemination of data/information from unstructured content, and (2) resolving incompatibility of privacy policies between communicating organizations. The users will provide and share content, with the trust that a enforcement software agent will provide the privacy control -- resolving the user and organizational privacy policy constraints and conflicts.

We propose implementing the sticky policies with an ontology representing the privacy policy defined within the organization. Content will be filtered using the ontology's privacy credentials to enforce privacy control of remote entities to local private content. Once the filtered content has been delivered to the querying entity, it is the privacy enforcement agents that enforce privacy at the remote site.

The benefit of a policy template for the end user is to gain transparency as to the scope of the information that he can gain access and share with others.