A Privacy Negotiation Protocol for Web Services

El-Khatib, K.

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

A Privacy Negotiation Protocol for Web Services *

El-Khatib, K.
October 2003

* published in Workshop on Collaboration Agents: Autonomous Agents for Collaborative Environments Halifax, Nova Scotia, Canada. October 13, 2003. NRC 46518.

Canada

A Privacy Negotiation Protocol for Web Services

Khalil El-Khatib
Institute for Information Technology
National Research Council of Canada
Ottawa, Ontario K1A 0R6, Canada
E-mail: Khalil.El-Khatib@nrc.ca

Abstract

Web Services is a new direction for businesses to extend the scope of their business applications outside their firewalls. While service providers might require their consumers to provide some personal or financial information before granting access to their services, consumers are always concerned about the privacy risk associated with revealing such information. Consumers are also becoming aware of the dollar-value of their personal information and are willing sometimes to negotiate for some added-value services in return for this information. The purpose of the Privacy Negotiation Protocol (PnP) presented here is to enable the generation and negotiation of a bilateral privacy policy between consumers and service providers. The paper presents also an architecture that uses the protocol and identifies an extension to the P3P privacy policy description language in order to use it to express various options in a policy template.

1. Introduction

Over the past few years, there has been a widespread increase in the use of web-based services. However, to mature into a mainstream business channel, a number of pressing issues must be resolved, especially the issue of handling consumers' personal identifiable information (PII).

Most of the time, web-based service providers require some personal or financial information from their consumers. Such information could be used for a number of purposes, ranging from regulating access to their on-line services (authentication, authorization), to billing (accounting), to service maintenance, customization or adaptation. While some of this information (such as financial information) requires participation from the consumer, other information (such as service usage pattern or geographic location) can be collected or inferred by the service provider without the direct contribution of the consumer.

For consumers, the temptations to disclose personal information are numerous, including the convenience of putting orders online, and the benefits of personalized and added-value services. But incidents with online privacy violations [1] made most online users concerned with the privacy invasion risk associated with revealing personal information without clear understanding of how this information is handled. The risk has lead consumers to conceal true information or to "garbage in" fake data in order to bypass the information request phase. A number of identity management systems [2,3,4] and software proxies [5,6] help controlling how much information about their users is released. Concealing true information using identity management and proxy systems or even providing fake information works well for web surfing, but not for services that require personal identifiable information to complete business transactions, as is the case with online stores that authenticate the consumer's credit card for billing purposes, or require for a shipping address for the delivery of purchased items.

Added to the problem is the fact that there is not a common denominator as to what information online users consider as private and what is not; different consumers have different perceptions of what is private and should be protected, and what is public and can be openly shared [7]. For instance, some online users are willing to give out their demographic and online contact; others are even reluctant to give out information about their country of residence. Additionally, there is no single data handling practice that is accepted by all online service providers; different service providers are more likely to have different practices in handling collected consumer's private information.

Many researchers agree that an important enabling factor for a comprehensive usage of online services is building consumer's confidence in online service providers when it comes to handling their personal identifiable information. Privacy policy is focal for building such confidence [8]. This is where the Privacy Negotiation Protocol (PnP) presented here comes in to enable service usage through facilitating generation of consumer-based privacy policy. Using the protocol, a privacy policy can be negotiated between the consumer and the service provider before both parties sign the policy as a binding contract. The terms and conditions included in the negotiated policy depend on the service

provider general policy expressed in a template privacy policy, and also on the consumer's privacy preferences. The negotiation protocol can be implemented in software agents that act on the behalf of consumers and service providers to negotiate a binding policy between the two parties. Using the negotiation protocol, a service provider's agent and a consumer's agent embark in a number of offer/answer exchanges of statements regarding the collection and usage of consumer's personal information by the service provider. The service provider's agent uses a policy generator to generate a policy offer and passes it to the consumer's agent. The consumer's agent receives the policy offer and passes it together with the user's privacy preferences, and other additional information to the rule evaluator running on the consumer side. The rule evaluator checks whether the privacy policy satisfies the privacy preferences set by the consumer or not. Based on the consumer's preferences, the consumer's negotiation agent controls how much information about the decision made by the rule evaluator to pass back to the service provider's negotiation agent. The consumer's negotiation agent may simply relay an answer whether the policy offer was accepted or not. But in case the policy offer was rejected, the agent might also add information such as the consumer's privacy rule that caused the refusal of the policy offer. The service provider's negotiation agent passes this information to the policy generator that tries to generate a new privacy policy offer that is more tuned to meet the privacy preferences of the consumer. This offer/answer process is repeated until the consumer's rule evaluator accepts the proposed policy and sends a signed copy to the service provider's agent, which in turn signs the policy and sends it back to the consumer's agent, or until either the consumer or service provider negotiation agent decides to withdraw from the negotiation.

The rest of the paper is organized as follows. Section 2 presents a privacy policy negotiation scenario between an online bookstore and a customer. Section 3 includes a review of research work on privacy policies in the literature. Section 4 presents the Privacy Negotiation Protocol (PnP), including the exchanged messages and state transition diagrams for all agents. In Section 5, we show how the protocol can be implemented in a simple architecture, and highlight the building components of the architecture. A required extension to the P3P specification language is introduced in Section 6. The extension is required if the P3P is to be used to express a policy template. Finally, we conclude in Section 7.

2. Usage scenario

The scenario presented in this section illustrates a possible negotiation between an online bookstore and a customer. Let us suppose that the negotiation is about how the customer's shipping information (address) provided by the customer could be used by the bookstore.

Let us assume that the customer is highly concerned about her privacy and does not want the shipping information she provides to the bookstore to be used in any way other than for shipping purposes. On the other hand, the bookstore requires definitely the shipping address to deliver the purchased goods. The promotion department of the bookstore may also use the shipping information and the type of books sold to find out what type of books to stock on. The bookstore may also sell this information to other bookstores or libraries for the same purpose. It may also sell this information to business development companies that can study the demographic distribution of the readers to find the best location for a library or a bookstore.

The online bookstore recognizes the importance of the shipping data, but since it cannot share it or use it without the consensus of the customer and in order to get her approval, it decides to offer multiple options to the customer, each with a certain discount incentive on the price of the merchandise. The negotiation between the bookstore and the customer on possible recipients of this shipping information can be expressed in terms of offers from the bookstore, and decisions on the offers from the customer, as shown in table 1. The left column in the table shows the offer from the bookstore, and the right column shows the customer's reply to the offer.

Table 1. A negotiation example for sharing shipping information.

On-line bookstore proposal on data recipients	**Customer's reply on the proposal**
A 10% discount, but we can use your shipping information for shipping purposes, and for doing in-house analysis. We can share the information with other bookstores or libraries, and also with other business development companies.	No, I refuse to share my address with any business development company.
A 7% discount if we can use your shipping information for shipping purposes, for doing in-house analysis, and if we can share it with other bookstores or libraries.	No, I refuse to share my address with other bookstores
A 5% discount if we can use your shipping information for shipping purposes and for doing in-house analysis.	No, I refuse using my information for in-house analysis.
You will be charged full price of the book, without discount. Your shipping information will be used only for shipping purposes.	I accept.

3. Related works

There has been a significant amount of work focusing on standardization of web services [9, 10, 11], yet little work on the privacy implication of their usage. The work in [12] presented an approach for preserving privacy in government web services. The approach is based on digital privacy credentials, data filters, and mobile privacy enforcement agents. The architecture is based on the concept that web service users must have credentials to get access to certain web services. Data filters use also these credentials to protect the privacy of requested data, in conformance with the preferences of the data owner. In order to protect the privacy of the information when exchanged with a third party, the architecture makes use of agent technology, where released data is sent together with a privacy enabling agent that enforces the privacy rules of the data on remote systems.

In [13], the authors presented an agent-based negotiation architecture that uses Case-Based Reasoning technique to capture and re-use previously successful negotiation experiences in the course of current negotiation session. Negotiation agents can use the information about previous negotiation to decide on the negotiation strategy for each episode of the negotiation. Negotiation experiences are hierarchically arranged and similarity between experiences is based on the concessions made during the negotiation. An approach for bilateral negotiation between an e-service provider and an e-service consumer in the presence of uncertainty is presented in [14]. During the negotiation, an agent makes use of the experience of other reputable agents to make an offer or a counteroffer.

In the World Wide Web service architecture, the Platform for Privacy Preferences (P3P) [15] is a specification language designed to inform users about the privacy policies of visited web sites. When a P3P compliant client browser requests a resource, the web service replies with a machine-readable privacy policy, which includes a declaration of the service identity and its privacy practice. The privacy practice lists the data elements that the service proposes to collect, how each data will be used, how long the data will be retained for and with whom it is shared. Acting on behalf of the user, a user agent can parse the declared privacy policy and compares it against a set of privacy preferences defined by the user. The user's preferences are expressed as a set of rules in the APPEL specification language [16]. The result of the comparison might be to proceed with the request with no condition, proceed with the request but provide the minimum information required to still get the requested resource, or to block the request.

While on-line service provider can use P3P to express all terms and conditions of their privacy policy, P3P lacks the ability to support negotiation of the terms and conditions of the privacy policy between the service provider and consumer [17]. The P3P/APPEL model can be categorized as a "take-it-or-leave-it" model, which is suitable for web browsing but not for the business service architecture, which is based on the benefits of service consumption and user's satisfaction. Additionally, the P3P model does not incorporate the notion of signing the agreement by both negotiating party.

4. Privacy negotiation protocol

To establish a bi-laterally binding agreement, negotiating agents must use a common negotiation protocol. The Privacy Negotiation Protocol (PnP) presented here is such a protocol that could be used between two agents for the generation and negotiation of a privacy policy. Such a negotiation protocol would define the syntax as well as the semantic of the exchanged messages between the negotiating agents. More importantly, the protocol would define the negotiation states for each agent as well as the possible actions that each negotiation agent can undertake in each state. In this section, we will present first all possible messages that each negotiation agent can send to its negotiation partner. We will leverage the existing P3P protocol to express the terms and conditions of the privacy policy carried in these messages. We will then use state transition diagrams to explain the possible states and actions of both consumer's and service provider's agents.

4.1 Types of exchanged messages

During the negotiation session, each negotiation agent can use a number of messages when communicating with the other negotiation agent. On the service provider's side, the service provider's agent should be able to put forward in a message a privacy policy offer (**Offer** message) when it receives an initial request for its service, or after it receives a refusal answer for the last privacy offer. It should also be able to sign and send a policy offer (**Commit** message) that is already accepted and signed by the consumer's agent. We will leverage the existing P3P protocol to express the terms and conditions of the privacy policy. On the consumer's side, the consumer's agent should be able to send a reply containing the decision of the agent on the received privacy policy offer. A refusal message (**Refusal** message) might also contain some additional information about the decision of the consumer's agent. The consumer's agent should also be able to sign and send a received policy offer (**Accept** message) to the service provider's agent. Finally, both agents should also be able to send a termination message (**Bye** message) if they decide to give up the negotiation process for any reason.

Table 2 summarizes the various messages that are exchanged by the agents with a short description of each one of them.

Table 2. Messages exchanged by the negotiation agents.

Message Type	**Meaning**
Offer	The service provider's agent sends an **Offer** message to the consumer's agent that contains a privacy policy.
Refusal	The consumer's agent sends a **Refusal** message to the policy included in the last **Offer** message received from the service provider's agent. This message might also include additional information about the decision, which the policy generator can use to speed up the negotiation phase by generating a more customized policy.
Accept	The consumer's agent sends an **Accept** message to the service provider's agent including a signed copy of the policy included in the last **Offer** message.
Commit	The service provider's agent sends a **Commit** message to the consumer's agent containing a signed copy of the signed policy from the **Accept** message.
Bye	Either the service provider's agent or the consumer's agent sends a **Bye** message to terminate the negotiations.

4.2 State transition diagrams

A state transition diagram for an agent using the negotiation is usually used to represent the behavior of the agent. The states in the diagram represents the states that an agent can assume at a certain time during the negotiation session, while the labels on the edges in the graph represent actions an agent can undertake or events that happen which result in a change of the agent's state. Figures 1 and 2 show the state transition diagrams of the protocol for the consumer's and service provider's agent respectively. We use the question mark symbol "?" to represent the event of message arrival and the exclamation mark symbol "!" to represent the action of message sending.

There are a number of points that we would like to highlight about the protocol. The first point is that the protocol is not an alternating offer model, in the sense that the consumer's agent does not make any counter-proposal to the received privacy policy proposal received from the service provider's agent. It is only the service provider's agent that makes a proposal, and waits for the acceptance or refusal from the consumer's agent.

The second point about the protocol is the added states related to the signing act of the policy as a binding non-repudiated contract for handling the private information. When the rule evaluator on the consumer's side finds no conflict between the terms and conditions of the policy offer and the consumer's privacy preferences, the consumer's agent can sign the policy and sends the signed copy to the service provider's agent, that in turn, signs the policy and sends a copy to the consumer's agent for the record. This double-signed policy constitutes a non-repudiable binding agreement between the two entities. The actual signature of the privacy policy expressed in P3P can be implemented using XML signature [18].

While the idea of having an agent that acts on behalf of the user in singing legal binding contracts might sound simple, there are still a number of issues that require further research before this scheme could be fully accepted. Of these issues is the subject of having trusted environments where the agents can run safely. Generally speaking, the user must have full guarantees that the environment is tamperproof before she can delegate signing tasks to user agents running in such environment. Another issue is how to design systems, where the users are held accountable for the actions of their own agents. Such systems would definitely require elaborated feedback mechanisms and interfaces [19], and would also require the user to actively participate in the signing process.

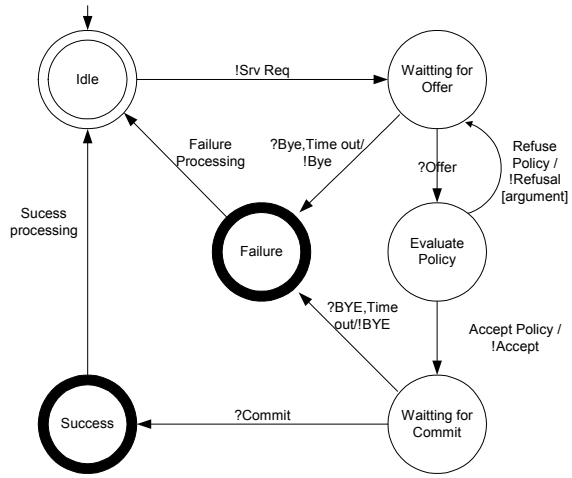

Figure 1. Consumer's agent state transition diagram

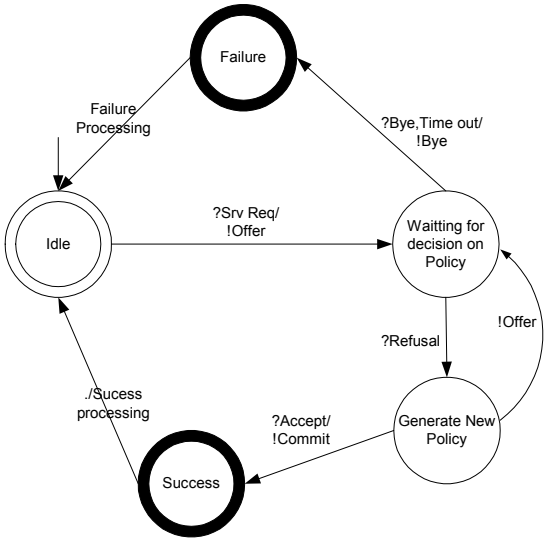

Figure 2. Service provider's agent state transition diagram

5. A Privacy Negotiation Architecture

To show how the Privacy Negotiation Protocol presented earlier can be used, we present here an architecture for negotiating terms and conditions of a privacy policy between a consumer and the service provider. The architecture has four major components: a policy generator, a rule evaluator, a consumer's agent and service provider's agent. A layout of the architecture showing the interaction between all these components is shown is Figure 3.

5.1 Policy generator

Privacy negotiation requires one or both negotiating entities (in our protocol, only the service provider generates these offers) to generate a number of potential privacy policies and finally arriving to a mutual agreed-on privacy policy or aborting the negotiation process entirely, and ending up with a negotiation failure. Using negotiation agent has shown fast convergence toward mutually accepted contracts [20, 21]. But Fully automating the negotiation process requires also automating the privacy policy generation process. Therefore, we suggest that the service provider to have a policy template that contains all alternatives for each term and condition as well as the rules for including them into the policy offers.

Generally speaking, a policy template would form the seed to generate all possible policy offers. It would contain the rules and constraints on a number of input parameters in order to include certain terms or conditions in the derived policy. These rules constitute what is usually called the negotiation strategy of the service provider. Section 6 presents an extension to the P3P specification language in order to use it to express the policy template.

Input parameters might include for instance the identity or class of the targeted consumer of the service. An important input to the policy generator, if available, is the declined policy from the previous negotiation round, as well as the arguments as for why the previously proposed privacy policy was refused. The policy generator can use this information to produce a policy offer that is more tuned to meet the consumer's preferences for privacy.

An important point that we should mention here is that in case the consumer refuses the privacy policy offer, the consumer's agent has a spectrum of options as to what to send back to the service provider's agent. On one end of the spectrum, the consumer's agent might only send the final decision (**Accept** or **Refusal**) to the service provider; on the other end of the spectrum, the agent might send the complete list of consumer privacy preferences to the service provider's agent in order to help the service provider's agent to formulate a new privacy policy; in between these two options, the consumer's agent might send the refusal decision with some added explanation as to which part of the proposal caused the refusal, or even the single user's privacy preference that caused the policy to get refused. Each option along the spectrum has a certain privacy invasion risk to the consumer, and some consideration must be taken to circumvent that risk [22].

5.2 Rule evaluator

The rule evaluator is a process running on the consumer's side that compares the privacy policy offer received from the service provider with the consumer's privacy preferences. As we mentioned earlier, the World Wide Web consortium has developed the APPEL [16] specification language that can be used to express online user's privacy preference or rule set, as APPEL calls them. A special-purpose APPEL engine could be used as a rule evaluator in our architecture, but existing database engine or trust engine [23] may also serve the same purpose. Typically, a rule evaluator returns an answer whether to accept or refuse the policy offer. In addition, a rule evaluator may also return an explanation string, the user's preference that caused the policy offer to be accepted or refused, and/or even a proof as to how the rule evaluator arrived to the decision. The communication of this information to the policy generator is controlled by the user's preferences as well, as we mentioned in the previous section.

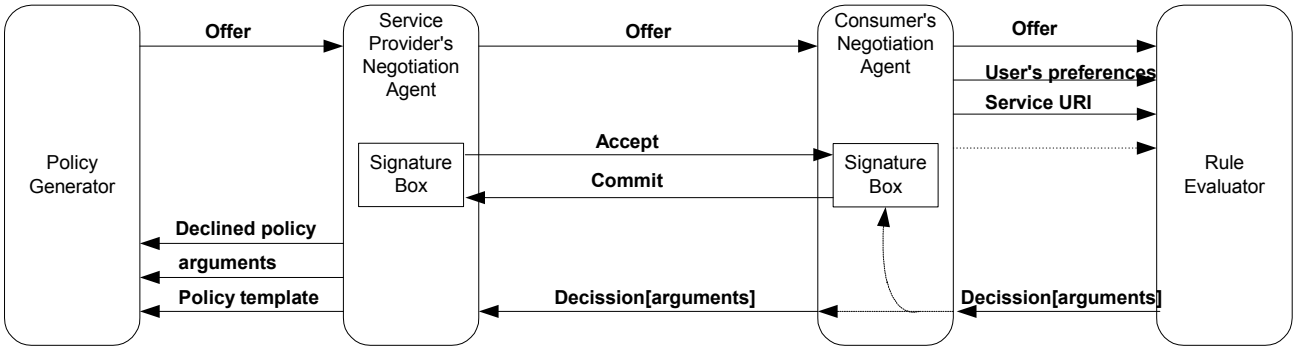

Figure 2. Policy negotiation architecture

5.3 Service provider's negotiation agent

Together with the policy generator, the service provider negotiation agent executes the service provider side of the privacy negotiation protocol presented in Section 4. It interacts with the consumer's negotiation agent by sending it the newly generated privacy policy by the policy generator and receiving the decision of the consumer's negotiation agent on that policy. When the consumer's agent announces its acceptance of the privacy policy, it sends a signed copy of the policy to the service provider's negotiation agent. In this case, the service provider's negotiation agent signs the policy and sends a copy to the consumer negotiation's agent. This double-signed policy can be used as a proof in case of dispute between the consumer and service provider.

5.4 Consumer's negotiation agent

On the consumer side, the consumer's negotiation agent implements the PnP without the policy evaluation part. The consumer negotiation agent acts as an interface to the rule evaluator and communicates with the service provider's negotiation agent on the service provider side. It communicates the privacy policy provided by the service provider's negotiation agent to rule evaluator, together with the consumer's privacy preferences (if present) and any additional information such as the URI of the requested service or service provider. If the rule evaluator finds that the privacy policy conforms to the preferences of the consumer, the consumer's negotiation agent signs the policy and sends a copy of the signed policy to the service provider's negotiation agent.

6. P3P extension to represent policy template

During the course of negotiation, the service provider is required to tune the negotiated privacy policy to make it acceptable by the consumer. Based on some parameters, such as the refused policy offer, the arguments on the refused policy, and other additional information provider by the consumer, the service provider refines the refused policy offer, expecting that the consumer would accept the new generated policy.

Generating different policies targeted to different types of consumers is a complex job for the service provider, and automating this process is a key for fast-automated convergence toward a bilateral accepted agreement. To automate the privacy negotiation process and cater for the largest possible consumer population, the service provider should be able to express all possible acceptable changes to the terms and conditions on the issued privacy policy in a policy template. The service provider's agent can use this policy template during the negotiation session.

To represent this policy template, we have looked at the P3P specification language since the privacy policy itself could be expressed in P3P. We have found out that, where as P3P is suitable to express the privacy policy a service provider presents to the consumer, it lacks the mechanisms to express alternative terms and conditions that can be offered in a policy to the consumer. Therefore, we suggest an extension to the P3P, which can only be used in the policy template to enable it to express policy templates.

The extension to the P3P would be to use a new element <*alt* [*condition*]> inside the P3P schema to allow the service provider to list, if possible, all possible alternatives for some terms and conditions inside the privacy policy. The *condition* parameter part of the *alt* element allows the service provider to control the conditions as to when each alternative is included in the policy offer. The standardized XACML [24] condition language could be used to express these conditions. A term or condition with only one alternative does not require the use of the <*alt*> element.

Examining the P3P schema, we have identified elements to which the extension could be applied. These elements are: <ACCESS>, <DISPUTES>, <REMEDIES>, <PURPOSES>, <RECIPIENTS>, <RETENTION> and <DATA-GROUP>. A description of these elements can be found in the P3P specification. The decision on whether an element can use the *<alt>* extension is based on the observation that each of these elements may have different values for different consumers.

To continue with our example presented in Section 2, we assume that the bookstore keeps a variable "Recipients_Set" that holds the name of all possible recipients of the shipping data provided by the consumer. According to the P3P specifications, the element "RECIPIENT" is used to express this preference, and it can take several values including "**ours**", **same**", "**delivery**", "**other-recipient**", "**unrelated**" and "**public**". Each time the consumer does not approve a certain recipient, the recipient is removed from the "Recipients_Set" set. Let us assume that, according to the bookstore policy, alternatives for data recipients are generated in the following order:

1- Companies performing delivery services (<**delivery**>), agents of the service provider (<**ours**>), other providers following the same practices as the service provider (<**same**>), and other companies following different practices (<**other-recipient**>) with a 10% discount on the merchandise.
2- Companies performing delivery services (<**delivery**>), agents of the service provider (<**ours**>), and other providers following the same practices as the service provider (<**same**>) with a 7% discount on the merchandise.
3- Companies performing delivery services (<**delivery**>), and agents of the service provider (<**ours**>) with a 5% discount on the merchandise.
4- Only companies performing delivery services (<**delivery**>) with no discount.

Using the extended P3P specification and simple string equality, we can express these alternatives in the policy template as follows:

```
<RECIPIENT>
  <alt Recipients_Set={delivery, ours, same, other-
                                        recipient}>
       <delivery>,<ours>,<same>,<other-recipient>
  </alt>

  <alt Recipients_Set = {delivery, ours, same} >
       <delivery>, <ours>,<same>
  </alt>

  <alt Recipients_Set = { delivery, ours} >
       <delivery>, <ours>
  </alt>

  <alt >
      <delivery>
  </alt>
 </RECIPIENT>
```

7. Conclusion

As web services become more of a mainstream business direction, one of the key issues that need to be addressed is the issue of privacy of consumer's personal identifiable information. But as there is a difference in classifying what is private and what is not, service provider and consumer should be able to negotiate what information the service provider is allowed to collect and how does it handle this information. In this paper, we have presented a negotiation protocol that can be used to negotiate a binding privacy policy between the two entities. We have also presented an architecture that uses the protocol and identified an extension to the P3P specification to enable it to express a policy template with all possible alternatives for each term in the policy. Our next step is to carry out some more analysis on the convergence of the protocol. We are also considering implementing the protocol in order to study its suitability and performance.

8. Acknowledgement

The author would like to thank Dr. George Yee for his constructive feedback on this paper.

9. References

[1] In the Matter of GeoCities, a corporation, FTC File No. 9823015 <http://www.ftc.gov/os/1999/9902/9823015cmp.htm>.

[2] J. Borking, "Proposal for Building a Privacy Guardian for the Electronic Age", in H. Federrath, editor, *Anonymity 2000*, Volume 2009 of Lecture Notes in Computer Science, Pages 130-140, Springer-Verlag, 2000.

[3] R. Hes and J. Borking, "Privacy-Enhancing Technolgies: The Path to Anonymity", Revised Edition. A&V-11. Den Haag: Registratiekamer, 1998.

[4] http://www.maxware.com

[5] http://www.anonymizer.com

[6] E. Gabber, P. Gibbons, Y. Matias, and A. Mayer, "*How to make personalized web browsing simple, secure, and anonymous*", In Proc. of Financial Cryptography '97 (1997).

[7] A. Adams, " The implications of users' privacy perception on communication and information privacy policies", Proceedings *of Telecommunications Policy Research Conference*, Washington DC, 1999.

[8] http://www.lawsch.uga.edu/jipl/vol7/Killingsworth.html

[9] W3C. SOAP: Simple Object Access Protocol, http://www.w3.org/TR/soap, 2002.

[10] W3C. WSDL: Web Service Description Language, http://www.w3.org/TR/wsdl, 2002.

[11] W3C. UDDI: Universal Description, Discovery, and Integration, http://www.uddi.org, 2002.

[12] A. Rezgui, M. Ouzzani, A. Bouguettaya, and B. Medjahed, "Preserving privacy in web services", *Proceedings of the International workshop on Web Information and Data Management*, pp. 56-62, 2002.

[13] D. M. Zhang and W. Y. Wong, "A Web-Based Negotiation Agent Using CBR", *PRICAI Workshops 2000*, pp. 183-198.

[14] G. Yee, L. Korba, "Bilateral E-services Negotiation Under Uncertainty", Proceedings, *the 2003 International Symposium on Applications and the Internet (SAINT2003)*, Orlando, Florida, Jan. 27-31, 2003.

[15] http://w3c.org/p3p

[16] http://w3c.org/APPEL

[17] http://dollar.ecom.cmu.edu/p3pcritique/CritP3P.PDF

[18] http://www.w3.org/Signature

[19] A. Patrick and S. Kenny, "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human- Computer Interfaces, *Privacy Enhancing Technologies Workshop (PET2003),* Dresden, Germany, 26-28 March, 2003.

[20] J. Collins, W. Ketter, and M. Gini, "A Multi-Agent Negotiation Testbed for Contracting Tasks with Temporal and Precedence Constraints", *International J*ournal of Electronic Commerce, 2002.

[21] J. Collins, M. Gini, and B. Mobasher, "Multi-agent negotiation using combinatorial auctions with precedence constraints", Technical Report 02-009, University of Minnesota, Department of Computer Science and Engineering, Minneapolis, Minnesota, February 2002.

[22] K. E. Seamons, M. Winslett, T. Yu, L. Yu, and R. Jarvis, ``Protecting Privacy during On-line Trust Negotiation," *2nd Workshop on Privacy Enhancing Technologies*, San Francisco, April 2002.

[23] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The KeyNote Trust Management System, Version 2", IETF Request for Comments 2704, Available at http://www.ietf.org/rfc/rfc2704.txt, 1999.

[24] OASIS. *eXtensible Access Control Markup Language (XACML)*, OASIS Standard, 18 February 2003, Available at: http://www.oasis-open.org/committees/xacml