Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Privacy Agents and Ontology for the Semantic Web

Dawn Jutla
Saint Mary's University

Liming Xu
Dalhousie University

Privacy Agents and Ontology for the Semantic Web

Dawn Jutla
Sobey School of Business
Saint Mary's University,
Halifax, Nova Scotia, Canada
Dawn.Jutla@smu.ca

Liming Xu
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia, Canada
liming@cs.dal.ca

ABSTRACT

Conducting international e-business requires knowledge about the privacy and consumer protection laws, and regulations that affect transacting parties. To support this requirement, we describe a high-level organization for a Web-privacy ontology composed of a hierarchical organization of formal laws and acts, informal cultural guidelines and standards for business in general, and specific legislation and guidelines for interest groups. A prototype of a Web privacy ontology is built for the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). The ontology is built upon XML infrastructure. We propose that existing and to-be-designed XML-based P3P tags be incorporated in any regulatory privacy ontology to enable future P3P agents to automatically match not only the business' privacy policy with the user preference rules, but also to match the business privacy policy with the privacy laws (for a start), and later with commerce and other-type laws, applicable to the stated legal jurisdiction(s) in which the business operates.

Keywords

P3P agents, privacy ontology, semantic web, e-privacy application, privacy agents

INTRODUCTION

In spite of the meltdown of dotcoms, a march towards ever-increasing adoption of electronic business and commerce is continuing. Extensive research is being conducted on the roles of trust and privacy in adopting e-business and e-commerce, research that results in new technologies and services in support of electronically transacted business. One type of such services includes provision of information on legal laws, industry standards, and cultural guidelines that may affect the transacting parties. To support such services, ontologies will be required to capture the prerequisite knowledge that can be used for mining in order to provide required and useful information to clients and thus to foster their trust and perceived control. This paper describes the first steps towards an ontology for the domain of privacy regulations, laws, and cultural guidelines. It also describes a fragment of the ontology built as a proof of concept. The XML infrastructure is used for exchange of information, the OntoEdit tool (Sure, Staab, and Angele, 2002; Fensel, van Harmelen, Klein, Akkermans, Broekstra, Fluit, van der Meer,, Schnurr, Studer, Hughes, Krohn, Davies, Engels, Bremdal, Ygge, Lau, Novotny, Reimer, and Horrocks 2000) to create the ontology, *Database (DB)* Sesame to store the Ontology using *Resource Development Framework (RDF),* and *Resource Query Language (RQL)* to get answers to user queries.

This paper is organized as follows. In order to properly position such an ontology within existing and emerging e-privacy standards, the following section briefly describes the notion of a P3P-based architecture and Web-services accessing a regulatory privacy ontology. The third section presents a high-level organization for a Web-privacy ontology composed of a hierarchical organization of laws and acts, informal cultural guidelines and standards for people in general, and specific legislation and guidelines for interest groups. A prototype of a fragment of privacy ontology that was created for the *Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)* is presented in the fourth section. The fifth section introduces extensions to P3P to support three way comparisons of user preferences, business privacy policies, and jurisdictional privacy regulations. The final section offers summary and conclusions.

WEB-SERVICES FOR PRIVACY

Empirical results (Jutla, Kelloway, and Saifi, 2004) show that the adoption of user intervention tools, such as P3P, encryption, cookie cutters, pseudonymizers, and anonymizers, increases users trusting beliefs in e-business and in Internet-based trust. These results motivate the creation of client-side privacy architectures that are based on the Industry recommended P3P protocol, and that are open to other user intervention tool add-ons. In this section, we describe how the proposed Web-side privacy ontology fits into privacy architectures, and suggest future privacy Web services made possible by the infrastructure.

The World Wide Web's consortium (W3C) has formalized a P3P specification that provides the base ideas/specifications for creating an infrastructure upon which a privacy-architecture can be built. Regardless of some shortcomings, it is the only contender on which to base privacy mechanisms. Indeed, in 2003, 30 percent of the top 100 sites were P3P enabled (Cranor 2003). The P3P platform specifies how resources, site policies, and user preferences can be expressed using XML, RDF (*R*esource *D*escription *F*ramework), and APPEL (*A P*3P *P*reference *E*xchange *L*anguage), and provides general guidelines that should be followed when building P3P agents. Because of the incremental adoption approach to P3P design taken by W3C, a lot of problems are yet to be tackled and many extensions to P3P have been proposed and discussed. These extensions deal with various aspects ranging from more detailed specifications, for instance redefinition of P3P elements, and form-based negotiations, to wider issues dealing with deployment of P3P.

Research building on P3P looks at more stakeholders, such communities and association, and their roles to create societal norms on top of the P3P data contexts. For example, Kaufmann and Powers (2002) propose an interesting idea of creating social contracts to establish norms of behavior as a way to standardize and enforce privacy practices and policies in various domains. They propose an architecture, based on P3P, called the Social Contract Core, that enables groups of users to express their preferences and thus influence and affect formation of policies adopted by site owners. Another example is the semi-autonomous privacy critics, or iCritics (Ackerman and Cranor, 1999), that can help users protect their privacy information. Privacy critics are agents that alert the user with warnings about potential privacy problems. A privacy critic could warn the user about what sensitive information is being revealed as the user surfs or fills out Web forms. Another example supported by Ackerman and Cranor (1999) is that a privacy critic could make a user aware that a site that they are visiting is on a warning list at reputable associations such as the BBBOnline. ATT's Privacy Bird**,** www.privacybird.com**,** is a browser extension based on P3P that provides users with warnings/information about the privacy policies posted by Web services sites in relation to the user's privacy preferences (Brandt 2003, Cranor 2003). For instance, the mechanism can warn a user, sensitive with respect to his/her medical information, about a Web-site that shares her medical data with other parties. Users may not realize how much data large portal sites, with e-commerce stores, chat rooms, newsgroups, and hundreds of services from strategic partners, can collect on them and use in various ways.

In (Bodorik and Jutla, 2003, Jutla and Bodorik, 2004), a privacy architecture based on the P3P platform is proposed and elaborated. The architecture fosters user's perception of control and thus increases user's trusting intentions to conduct e-business. It shows two components: a client-side component and a Web-side component (the privacy ontology). An *internal Regulatory* agent maintains user privacy preferences about privacy regulations, guidelines, rules, and any user-pertinent privacy governance information that guide the user privacy agents during user transactions with service-sites. This agent keeps an up-to-date knowledge base by accepting and filtering external feeds such as from Web watches of sites such as epic.org, BBBOnline, hilwatch.com, and privcom.gc.ca.

There are two types of external agents. *Service-site agents,* located at the service sites, provide the user with services by interacting with the user or the user agents – it is this interaction that requires private information to be supplied by the user and for which the supporting privacy mechanisms are provided. The other type of external agents effect trust intervention mechanisms by the government, community, association, and business stakeholders (Jutla, 2003). Three representative external or Web-services agents for privacy, including those mentioned above are, iCritics (Ackerman and Cranor, 1999), Social Core (Kaufmann and Powers, 2002), and the external regulatory agents that represent Web-privacy services agents. The Web privacy ontology structure discussed in the following sections are built for support of both internal and external regulatory agents.

WEB-SIDE REGULATORY PRIVACY ONTOLOGY FOR AGENTS

Knowledge bases built upon ontologies are accepted as the major infrastructural element for the Semantic Web (Fensel, van Harmelen, McGuiness, and Patel-Schneider, 2001, Kim, Joffman, and Martin 2002). Privacy agents, providing Web-services around various legal regulations, cultural and ethical guidelines, and standards created by various industries and other entities, require a privacy knowledge base supported by an ontology. More specifically, a number of privacy ontologies spanning various countries and cultures will be required. In this section we describe a high-level model for building privacy ontologies.

We suggest that the onion layer model is representative of the privacy domain whereby each ring represents a privacy layer provided by a tier of governance or an important stakeholder. This model is an important reference point for the development of informational privacy Web services. Table 1 shows a mixture of formal and legal laws and acts, informal and cultural guidelines and standards for the general masses, and specific legislation and guidelines for interest groups. The table intends to capture the different privacy protection mechanisms at various stakeholder layers.

Privacy guidelines and international agreements among some trading countries exist at the level of the United Nations (UN), Organization for Economic Cooperation and Development (OECD), and the World Trade Organization (WTO). The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks are some examples.

A mixture of Bennett's (1992) government privacy models is applicable at different levels of government, and the strength of the privacy protection can differ across levels of government. Reflective of the mixture of models is that some provinces have provincial privacy commissioners, and some do not, instead relying on the federal data commissioner. The US expresses a mixture of voluntary control for corporations and subject control where citizens can readily take privacy infractions to the courts. Since 1993, the province of Quebec, Canada, had stronger privacy legislation for business than that enacted at federal level; indeed the strongest privacy protection in North America from 1993 until 2001 (when the rest of Canada adopted PIPEDA), was implemented by the francophones in Quebec.

Mechanism	*Internat-ional (e.g UN)*	*National/ Federal*	*Provincial /State*	*Munici-pal/ Local*	*Sectoral (e.g. Health, Finance)*	*Association (e.g Business Chambers*	*Organiz -ation*	*User*
Guidelines	x	x	x	x	x	x	x	x
Acts/Laws	x	x	x	x				
Standards	x	x	x	x	x	x	x	x
Policy	x	x	x	x	x	x	x	x
Privacy Champion		x	x	x	x	x	x	
Technology (e.g. P3P)	x	x	x	x	x	x	x	x
Social contracts						x	x	x

Table 1. Privacy Layers

Innovation networks and associations, such as the World Chambers Network and International Chambers of Commerce, create policies, standards, and can create social contracts to provide structural assurance for online privacy and trust. Novel approaches use technology to speed up an associations view on policy preferences for its membership to business in general. The World Wide Web Consortium's (W3C) P3P mechanism embodies fair information principles and intends for service sites and users to compare privacy policies and privacy preferences respectively. Negotiation protocols between site and user agents are not yet part of the W3C P3P standard.

Businesses have many intervention mechanisms for online privacy, such as online privacy seals, privacy statements coded in XML to support P3P agents, and corporate privacy governance. The latter consists of business policies for risk management for loss of privacy data, assessment of privacy threats, and selection of security and privacy protocols according to industry standards.

On the last privacy layer, the user stakeholder perceptually weights the distance among layers. That is, the user tends to be more concerned or feel more impacted by the layers closest to her/him. The user is more concerned with the privacy practices of the corporations he/she is dealing with in contrast to the perceived distance of the UN's declaration of privacy as a human right. We suggest that cultural influences will occur mostly at the community, organisation, and user level within each country; perhaps mainly at organization and user implementation of privacy controls. Cultural variables may affect users' willingness to investigate and adopt privacy tools such as anonymizers. Federal or state protection controls are more distanced from organizational variables and appear to be more influenced by OECD, WTO, and UN guidelines on privacy which tend to be culturally universal.

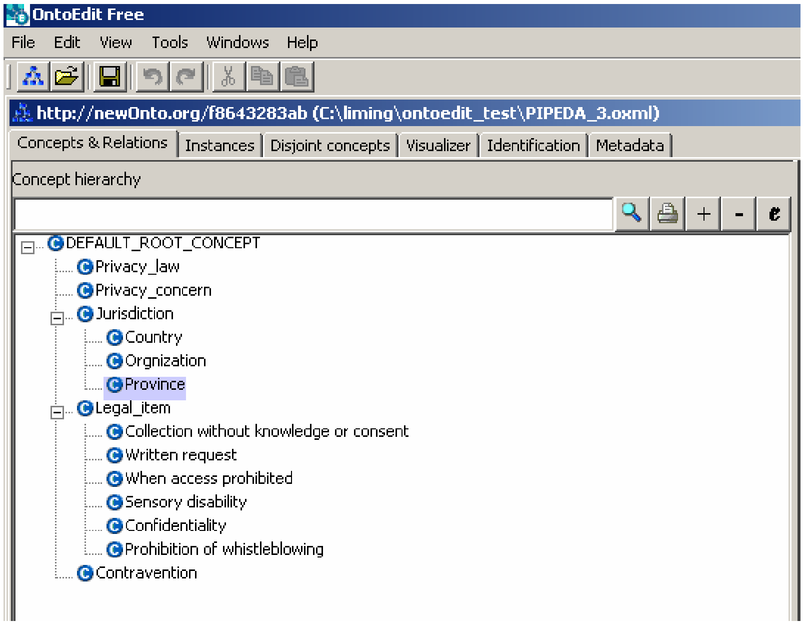
ELABORATING THE FEDERAL LAYER OF THE REGULATORY ONTOLOGY USING PIPEDA

For illustration of the implementation of a privacy layer in a Web privacy ontology, we have chosen privacy regulations at the national level, using the federal-level, Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA became in force on January 1, 2004.

We used two approaches to create the ontology, one automated and one manual. One initial idea was to compare the automatic and manual creation of ontologies. For automatic creation of the ontology we tried the OntoExtract tool, but found that legal documents such as PIPEDA are discourse-poor and thus we needed to perform manual extraction of concepts and relationships. To create the ontology manually, we use OntoEdit (http://www.ontoprise.de/products/ontoedit). OntoEdit provides an ontology-engineering environment that allows users to create, browse, and modify an ontology using a GUI interface. In addition it has a data visualization tool, called Visualizer, which displays the concepts and their relationship. OntoEdit supports the W3C standards, and offers a multifunctional export interface to many major ontology representation languages including RDF and DAML+OIL. The created ontology was stored in Sesame, an RDF database that stores semantic information about objects in the form of triplets. Furthermore, for import/export, the RDF triplets are transported using XML. Thus, OntoEdit performs the "usual" transformation of the created ontology to RDF representation (Fensel et al 2001, Decker and Melnik, 2000). The Sesame DB is queried using RQL.

To manually create the PIPEDA ontology we followed the usual set of guidelines, for instance as those presented in (Noy, 2001). We successively identify and enter into the ontology important classes, defined properties of classes, class hierarchies, and instances. Following this we define relationships between main concepts.

To determine the important concepts, we examine the PIPEDA document for terms that a potential user might like to have explained. Certainly, *Privacy Law* should be one of the concepts for future support of other countries' laws or for even different state/provincial privacy laws. Usually every privacy law defines the circumstances under which the law applies, when the law is coming into force, and what the purpose of the law is. When doing business on the Internet, the user would like to know which privacy law can be applied to the location where the service site is at, or which law applies to the country the consumer resides in, so that the *Jurisdiction* is another term in our ontology. Some example sub-concepts of Jurisdiction are Country, Province, and Organization. *Country* refers to country level jurisdiction; *Province* refers to province level jurisdiction; *Organization* refers to organization level jurisdiction. We associate a property with the Jurisdiction concept that defines which privacy law a particular jurisdiction uses. In addition, the class Organization and Province, subclasses of Jurisdiction, have one more property – Belong_country. For an organization, it defines in what country the organization is headquartered.



http://newOnto.org/f8643283ab (C:\liming\ontoedit_test\PIPEDA_3.oxml)

- DEFAULT_ROOT_CONCEPT
  - Privacy_law
  - Privacy_concern
  - Jurisdiction
    - Country
    - Orgnization
    - Province
  - Legal_item
    - Collection without knowledge or consent
    - Written request
    - When access prohibited
    - Sensory disability
    - Confidentiality
    - Prohibition of whistleblowing
  - Contravention

Figure 1. Class Hierarchy in Regulatory Privacy Ontology

The *Legal_item* concept refers to specific legal information in PIPEDA referencing the fair information and privacy principles; legal item contains sub-concepts of data *collection* without knowledge or consent among others. *Written request* is yet another concept specified in a subclass of *Legal_item*; it addresses user access to personal information. Other concepts stem from providing user recourse if her privacy has been violated, or that the privacy act has been contravened – thus we identify the *Contravention* class with subclasses: *Delegation, Reporting method, Powers of Commissioner*, and *Time limit*. The minimum class hierarchy is shown in Figure 1.

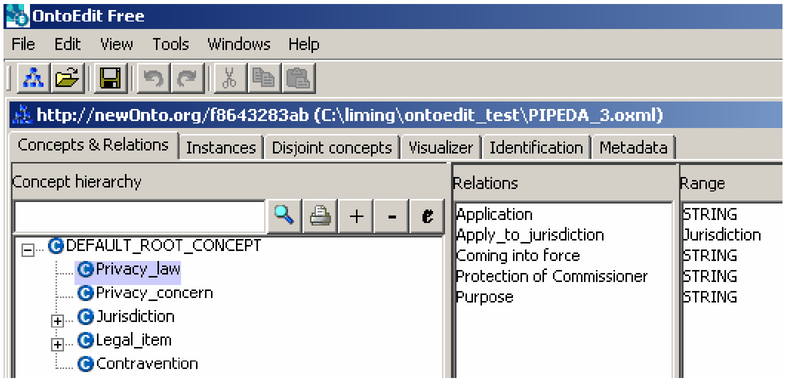
A key purpose of our ontology is to inform users about what user privacy concerns and fair information practices regarding users' personal information a privacy law covers. P3P elements and attributes, as defined in the P3P specification version 1.0 (2003), provide an XML-based vocabulary for expressing a privacy policy associated with Web pages or content elements of a Web site. Table 2 provides the corresponding P3P tags and APPEL rule behaviors for major fair information principles identified in most privacy laws, and specifically in PIPEDA. These XML-based tags defined in the P3P specification allow users to express their preferences and/or business to express their privacy practices.

We define these fair information practices, shown in Table 2, in a class called *Privacy_concern*. We also define a property to facilitate queries about which user privacy concern or fair information practice is defined in which law.

PIPEDA Fair Information Principles	**P3P tags and APPEL rules that in combination aid in achieving the PIPEDA principles**
Consent	User: <appel: RULE behavior = "request"> Business: <REQUIRED> , <opt-in>
Limiting use, disclosure, and retention	<PURPOSE>, <RETENTION>, <RECIPIENT>, <POLICY> <opturi> User: <appel: RULE behavior = "limited">
Identifying Purposes	<PURPOSE>
Individual Access	<ACCESS>
Accountability	Not applicable as it involves appointing a person to be responsible for a company's compliance to PIPEDA, and the development and implementation of privacy policies for the business. It may be useful to have a Boolean tag added to P3P that would indicate whether or not a company has appointed a person accountable for compliance. The closest that P3P 1.0 supports is the <service> sub-element under <DISPUTES> – but this refers to publicly publishing contact information for the customer service representative(s) who handles privacy complaints.
Provide Recourse	<DISPUTES> <service> <independent>, <REMEDIES>
Limiting Collecting	User: <appel: RULE behavior = "limited">
Accuracy	It would be useful for the user to have a way to express to a company whether the use or disclosure of out of date or incomplete information would be harmful to him/her. It would also be useful to indicate what subset of the data falls in this category.
Safeguards	These refer to security measures for protecting personal information (in any format) against unauthorized access, disclosure, copying, use, modification, and loss or theft. It may be useful to create a P3P tag to allow companies to convey to the users that measures such as firewalls, virus/intrusion detection, encryption etc. are in use.
Openness	<POLICY> <discuri> addresses availability of the privacy policy. But openness also refers to making sure the policies and practices are understandable.
Exceptions	Exceptions to the consent and access principles are also provided in PIPEDA. Example exceptions include refusal of access to personal information collected during dispute resolution process. It may be useful to have P3P tags /APPEL rules that can express such exceptions. A negation connective may be useful in Appel for this purpose.

Table 2. P3P and Appel vocabularies for expressing fair information practices for user privacy

For each class/sub-class, its properties are defined. For instance, the properties of the concept/class *Privacy_law* are shown in Figure 2. OntoEdit shows the properties in the Relations pane. Properties that have a range specified as another concept/class represent relationships between classes. Consider Figure 2. The property *Application* defines where and to whom the privacy law can apply. Its range is *String* and its value is the string in the PIPEDA document where the *Application* is defined. The property *Apply_to_jurisdiction* defines which jurisdiction uses this privacy law. Its range is the class or a subclass of *Jurisdiction* and it thus represents relationships between the classes. Of course as a privacy law can apply to more than one jurisdiction, the *Privacy_law* class can be related to more than one instance of *Jurisdiction* in the property of *Apply_to_jurisdication*. The property *Coming into force* defines the date when the entities legislated by the privacy law must comply with it. The *Protection of authority* property defines how the privacy law protects the authority that enforces it, while the *Purpose* property defines the purpose of the privacy law. Its range is its legal definition of *Purpose* in the privacy law.



Relations	Range
Application	STRING
Apply_to_jurisdiction	Jurisdiction
Coming into force	STRING
Protection of Commissioner	STRING
Purpose	STRING

Figure 2. Properties of the Privacy_law Class

Our prototype for this regulatory Web privacy ontology is stored in the Sesame server DB in RDF format. It can be queried using RQL. We show below an example query – the query "When can my personal information be used without my consent?" was (manually) translated to the following RQL query:

```
select X, Y
from  {X} ns3:Is {Y}, {X} rdf:type {Z}
where Z like "http://newOnto.org/f8643283ab#Collection_without_knowledge_or_consent"
using namespace
    ns3 = http://newOnto.org/f8643283ab ,
    rdf = http://www.w3.org/1999/02/22-rdf-syntax-ns#
```

The following are examples of questions that can be successfully answered using the ontology:

- What kinds of privacy concerns are defined in PIPEDA?
- What is the purpose of PIPEDA?
- When will PIPEDA come into force?
- Is privacy concern 'consent' defined in PIPEDA?
- How is the privacy concern 'consent' defined in PIPEDA?
- How could I use the information I collected via Internet?
- When can my personal information be used without my consent?
- What will happen if I contravene PIPEDA?
- How will I be protected if I report a violation?
- What privacy law(s) apply if I do business with a Canadian company?

A PROPOSAL FOR A 3-WAY P3P AGENT COMPARISON AMONG USER PREFERENCES, BUSINESS PRACTICES, AND GOVERNMENT LEGISLATION

By adding P3P tags to the concepts in the regulatory privacy ontology, we facilitate a P3P-agent to perform a three-way comparison among user preferences, business practices, and government regulations. This comparison could be useful to an Internet user in several ways. A comparison between the contents of P3P elements representing business privacy practices and those representing privacy law may result in highlighting to the user (1) omissions in the business' P3P policy statements, or (2) concerns of mismatch of interpretation of privacy legislation. As an example, corporate lawyers often advise their clients against committing to the wording as set out in the DISPUTES and REMEDIES P3P elements. In a September 2003 draft on proposed changes to P3P elements (see http://www.w3.org/P3P/2003/p3p-translation.htm, a legal attorney commented that most corporate lawyers would "advise their clients against specifying (the P3P) REMEDIES (element), since prospectively binding the company to redress without legal mandate or business incentive may be considered a disservice to the shareholders". Although the REMEDIES wording is changed in the November 2003 draft specification changes for P3P version 1.1, it is clear that many different wordings and hence interpretations are possible within privacy policies. The P3P specification is not yet mature enough in terms of element definitions to cleanly handle many legal subtleties – hence P3P agents can be useful to the user in flagging mismatches between fair information principles regarding privacy as defined in law and the business' practices expressed in their P3P policies.

Accessing privacy ontologies containing P3P tags associated with concepts and relationships can facilitate the user in populating their user preferences in a more informed way. A P3P-agent comparison of user privacy preferences and the corresponding concepts in a regulatory Web privacy ontology can flag user inattention to details in their user preferences ruleset.

Another area where the 3-way comparison could be useful is in the arena of multiple jurisdictions where a user may be dealing with a Web "multinational". Especially helpful to this scenario would be the addition of a <JURISDICTION> tag to the XML-based P3P vocabulary. The problem of sharing data with partnering companies in multiple jurisdictions can also be flagged to a business under different assumptions. For example, a P3P agent can be directed to the Safe Harbor framework for further information if partnering companies are members of the Safe Harbor initiative. From a user perspective, under a weakest link assumption, a user can decide that his/her personal information is at risk as long as a partnering company, with which data is shared by the user's service site, exists in a jurisdiction where there is no legislation for privacy. A European Union consumer would be assured that under the Brussels Regulation, jurisdiction is in the home country of the user.

We note here that there are possibly many laws to which a business must comply when handling customer personal information such as consumer protection laws and sector-dependent laws such as the Alberta Health Information Act in Canada or HIPAA in the US. Labor laws govern employee personal information. Depending on the circumstances of the dispute, one law can have precedence over the other. Future work is required to incorporate much more sophisticated querying of regulatory ontologies and knowledge bases through complex combinations of semantic Web services to provide the user with reliable advice.

SUMMARY AND CONCLUSIONS

This paper describes Web architectural support in terms of a Web privacy ontology for agent-based e-privacy applications. We present a high-level organization of a Web-privacy ontology for laws and acts, informal cultural guidelines, and standards and guidelines for interest groups. As a proof of concept we have created a prototype for a fragment of the ontology, only that of the Federal-level layer, containing the model of PIPEDA, Canadian federal privacy law for business. We used a popular ontology editor, OntoEdit, which support graphical interface for creation of concepts/classes, sub-classes, attributes, and definitions of constraints and axioms.

Further, we propose the incorporation of XML-based P3P elements and its attributes into the ontology so that P3P-based agents can do more sophisticated matching among privacy stakeholders. Although specific agent implementation is not provided here, applicable agent technologies and models including the assumption based truth maintenance system and AGM frameworks (de Kleer, 1986, Shapiro, 2003) are suitable for maintaining the integrity of the knowledge bases with which the agents must work.

There are a number of problems that need to be tackled before ontological services can be brought to fruition. For instance, a suitable interface to communicate with the user must exist. The user may pose questions in the natural language that must be translated into queries posed to the knowledge base(s). Which ontology is to be queried must be identified, the query must be posed in a suitable language and results delivered back to the user, again in a suitable form while the underlying infrastructure would be based on Web-services. Consequently, a broker that keeps information on pertinent and available knowledge bases will be required, perhaps similar to the one described for pervasive environments in (Chen, Finin, and Joshi, 2003). Our initial steps for privacy ontology formation were guided by the objective of creating a simple service that would provide some useful information to answer queries pertaining to the regulatory area of the e-privacy domain.

A Resource Centre on P3P, part of the *Joint Research Centre (JRC)* of the European Commission, has long-term plans to build an ontology for data protection where the participation of numerous stakeholders is anticipated (JRContology 2004). This Resource Centre on P3P has a basic privacy architecture that does not include access to Web-services or cooperation with *Trusted Third Parties (TTP)* as yet. It is promising for the future of customers' privacy and international business that plans are being announced to work on the creation of privacy ontologies for the Web. The work presented in this paper is a useful starting point.

REFERENCES

1. Ackerman, M. S., and Cranor, L., (1999), Privacy Critics: UI components to safeguard users' privacy. Proceeding of the Computer Human Interaction Conference, CHI'99,ACM Press. 1999.
2. Brandt, A (2002), Privacy Watch: A Little Bird That Guards Your Online Privacy. *PCWorld*, December 2002.
3. Bennett, C. J. (1992), Regulating Privacy: Data Protection and Public Policy in Europe and the United States, New York: Cornell University Press.
4. Bodorik P. and Jutla D.N. (2003), Architecture for User-controlled e-Privacy, ACM Symposium on Applied Computing, SAC 2003, Technical Track on E-commerce Technologies, 609-616.
5. Chen H., Finin T., and Joshi A. (2003), Using OWL in a Pervasive Computing Broker. Workshop on Ontologies in Agent Systems, *AAMAS 2003*. Melbourne, Australia.
6. Cranor L.F. (2003), P3P: Making Privacy Policies More Useful, IEEE Security & Privacy, November/December 2003, 50-55.
7. Decker, S. and Melnik, S (2000), The Semantic Web: The Roles of XML and RDF. IEEE Internet Computing, September/October 2000, 63-74.
8. de Kleer J. (1986), An Assumption-based TMS, Artificial Intelligence, 28:127-162.
9. Fensel, D., van Harmelen, F., Klein, M., Akkermans, H., Broekstra, J., Fluit, C., van der Meer, J., Schnurr, H-P, Studer, R., Hughes, J., Krohn, U., Davies, J., Engels, R., Bremdal, B., Ygge, F., Lau, T., Novotny, B., Reimer, U., and Horrocks, I (2000). Ontoknowledge: Ontology-based Tools for Knowledge Management, *In Proceedings of the eBusiness and eWork 2000 Conference,* Madrid, Spain.
10. Fensel, D., van Harmelen, F., McGuiness, D.L., and Patel-Schneider, P.F. (2001), OIL: An Ontology Infrastructure for the Semantic Web. IEEE Intelligent Systems, March/April 2001, 38-45.
11. JRContologie (2004), Ontology for Data Protection: (PRONTO), http://p3p.jrc.it/presentations/OntologyEOI.doc, last viewed January 12, 2004.
12. Jutla D. N. (2003), Online Trust: Is Privacy In or Out?, *In e-Business in the 21st Century*, eds. Sharma S.K., and Gupta J., IDEAS Publishing, Australia, 313-336.
13. Jutla D.N., and Bodorik P. (2004), PeCAN: An Architecture for User Privacy and Profiles in Electronic Commerce Contexts on the Semantic Web, Technical Report, SMU-MSC119, Saint Mary's University.
14. Jutla D.N., Kelloway, E.K., Saifi, S. (2004), Evaluation of the Impact of User Intervention Mechanisms for Privacy on SME Online Trust, IEEE Conference on e-Commerce, San Diego, California, 2004.
15. Kim, A., Joffman, L.J., and Martin, C.D. (2002), Building Privacy into the Semantic Web: An Ontology Needed Now. Semantic Web Workshop 2002, Hawaii USA.
16. Noy, N. F. and McGuinness, D.L.: Ontology Development 101: A Guide to Creating Your First Ontology. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001.
17. Kaufmann, J., H. and Powers, C. (2002), The social contract core. WWW 2002, May 7-11, Hawaii, USA, 210-220.
18. P3P (2004); Platform for Privacy Preferences Project, http://www.w3.org/P3P/, viewed on January 12, 2004.
19. Shapiro, S.C (2003), Knowledge Representation. In Lynn Nadel, Ed., Encyclopedia of Cognitive Science, Volume 2, Macmillan Publishers Ltd., 2003, 671-680.
20. Sure, Y., Staab, S, and Angele, J. (2002) OntoEdit: Guiding Ontology Development by Methodology and Inferencing. 0 Proceedings of the International Conference on Ontologies, Databases and Applications of SEmantics ODBASE 2002, October 28 - November 1, 2002, University of California, Irvine, USA, Springer, LNCS.
21. W3C P3P Guiding Principles (1998), at http://www.w3.org/TR/NOTE-P3P10-principles, viewed on July 24, 2003.