



PeCAN: An architecture for users' privacy-aware electronic commerce contexts on the semantic web[☆]

Dawn N. Jutla^{a,*}, Peter Bodorik^b, Yanjun Zhang^b

^a*Computing and Information Systems, Sobey School of Business, Saint Mary's University, 903 Robie Street, Halifax, Nova Scotia, Canada B3H 3C3*

^b*Faculty of Computer Science, Dalhousie University, Halifax, Nova Scotia, Canada*

Received 12 June 2004; received in revised form 14 October 2004; accepted 20 February 2005

Abstract

Supporting e-Commerce on the Semantic Web implies more sophisticated integration of Web services, agent interaction, domain ontologies, and data markup languages than is being done on today's Web. We explore user e-commerce, trust, and privacy scenarios and provide a vision for future e-commerce interactions with a more informed and in-control user. We present the *Personal Context Agent Networking (PeCAN)* knowledge architecture consisting of client-side and web-side architectural data components and services which inform the user of online privacy and trust within e-commerce tasks. A novel organization scheme and the composition of user contexts in this environment are proposed. Client-side ontologies and data structures for representing user contexts are introduced. For proof of concept, we describe a data belief ontology and illustrate PeCAN's compliance to the P3P privacy data schema. We use OWL as an implementation basis for maintaining privacy-aware e-commerce contextual knowledge for effective agent action in the PeCAN environment.

Categories and Subject Descriptors: Semantic Web Application Architecture, Web Information Systems Applications, Electronic Privacy, Decision Support System Application

© 2005 Elsevier B.V. All rights reserved.

Keywords: Privacy; P3P; Context-aware; Online trust and e-privacy architecture; Owl application; e-commerce; Semantic web; Private data management; User decision support; Web services

1. Introduction

Postmortems of failed e-privacy business models reveal three fundamental problems. Firstly, from the user perspective, it is difficult for some to trust the third party provider itself, or more specifically, the human employees in the “trusted” third party

[☆]Recommended by Jian Yang, David Bell and Chris Bussler.

*Corresponding author. Tel.: +902 420 5157;
fax: +902 496 8101.

E-mail address: Dawn.jutla@smu.ca (D.N. Jutla).

provider. The perception of loss of control of personal data is higher when a lot of your data is passed through a third party, and when that third party may persistently hold increasingly larger snapshots of your data. Secondly, those e-privacy businesses that used the advertising business model soon found that they could not compete with players such as Yahoo!, and other large portals, which could cut the cost of advertising on these sites to levels unsustainable for smaller competitors. Thirdly, in many countries such as the US, Canada, and the European Union, privacy is functionally maintained through secure technical channels usually provided by the user's organization or by the organization with which the user is transacting. Thus third parties have not offered sufficient value-added services to maintain "functional" privacy channels in the business-to-business (B2B) or business-to-customer (B2C) markets. Learning from these fundamental problems, knowing the economic value of user's personal information [1–8] and noting that industry analysts, e.g., Gartner Group, project that information privacy will be the number one problem for e-commerce by 2006, we predict that the future success of third party business models for privacy will be in the provision of contextual "information-based" privacy Web services. These Web services will target national and international businesses, global users, and society in general. The provision of successful privacy Web services will depend on advances in contextualized client-side and Web privacy architectures, platforms such as the WC3 Platform for Privacy Preferences (P3P), as well as multiple stakeholder cooperation. In this paper, we describe requirements, design, and implementation of technical components that together form future critical success components in the provision of contextual information privacy for e-commerce.

Specifically, information-based privacy services are needed that can present users with simple privacy-related facts in a given user context. In the last 5 years, stakeholders from industry and academia have made progress towards such a vision. As an example, ATT's Bird (www.privacybird.com) is a useful, and currently free, information-based privacy service for users.

Bird is a P3P agent that is designed for the automatic machine-reading of Web sites' privacy policies and comparison with user privacy preferences specified at the client-side. Businesses' intentions for maintaining user privacy are articulated through organizations' privacy policies for implementing fair information principles, in accordance with privacy acts or laws. These policies are often long and complicated, and users do not like to read them [9]. Bird simplifies this privacy task by automatically reading a business' privacy policy, and outputting a concise summary consisting of a set of statements about what privacy issues are relevant to the user, as per the users' stated preferences. Bird is only a first step, albeit an important step, in the provision of informational privacy services.

More sophisticated informational privacy services than are currently available are required. As a sector example, sites such as www.canlii.org, www.austlii.org, and www.law.cornell.edu, all share a similar mandate to make legal information available and freely accessible to ordinary citizens. However, a current search on privacy law on these sites is not useful, or easily decipherable, to most of us. Examples of potential privacy Web services include: easily seeking out useful knowledge about countries' privacy laws, integrating privacy knowledge from various stakeholders, assessing a country's privacy culture, supporting the discovery of privacy Web services, automating the visualization of privacy information and knowledge according to a range of user profiles, and managing collaborative stakeholder updates to distributed web ontologies containing privacy domain knowledge.

The aim of providing such services is to significantly complement the work started by the W3C on the P3P platform and put trust and privacy personalization squarely in the hands of users. In this paper, we propose the *Personal Context Agent Networking* architecture, PeCAN, which (1) provides the necessary architecture on the client-side to receive and use information from such future Web services, (2) motivates the requirement and uses of Web privacy ontologies to complement the client-side privacy-aware applications, (3) increases user perception of

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات