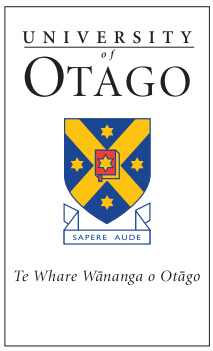


# Building Privacy Infrastructure for Culturally Sensitive Information of New Zealand Maori

Xianglin Deng
Noria Foukia
Bastin Tony Roy Savarimuthu

## The Information Science Discussion Paper Series

Number 2007/03
July 2007
ISSN 1177-455X

**University of Otago**

**Department of Information Science**

The Department of Information Science is one of seven departments that make up the School of Business at the University of Otago. The department offers courses of study leading to a major in Information Science within the BCom, BA and BSc degrees. In addition to undergraduate teaching, the department is also strongly involved in postgraduate research programmes leading to MCom, MA, MSc and PhD degrees. Research projects in spatial information processing, connectionist-based information systems, software engineering and software development, information engineering and database, software metrics, distributed information systems, multimedia information systems and information systems security are particularly well supported.

The views expressed in this paper are not necessarily those of the department as a whole. The accuracy of the information presented in this paper is the sole responsibility of the authors.



**Correspondence**

This paper represents work to date and may not necessarily form the basis for the authors' final conclusions relating to this topic. It is likely, however, that the paper will appear in some form in a journal or in conference proceedings in the near future. The authors would be pleased to receive correspondence in connection with any of the issues raised in this paper, or for subsequent publication details. Please write directly to the authors at the address provided below. (Details of final journal/conference publication venues for these papers are also provided on the Department's publications web pages: http://www.otago.ac.nz/informationscience/pubs/). Any other correspondence concerning the Series should be sent to the DPS Coordinator.

Department of Information Science
University of Otago
P O Box 56
Dunedin
NEW ZEALAND

Fax: +64 3 479 8311
email: dps@infoscience.otago.ac.nz
www: http://www.otago.ac.nz/informationscience/

# Building Privacy Infrastructure for Culturally Sensitive Information of New Zealand Maori

Xianglin Deng[1], Noria Foukia[2], Bastin Tony Roy Savarimuthu[2]
Information Science Department, University of Otago
PO Box 56, Dunedin New Zealand
denxi185@student.otago.ac.nz [1], {nfoukia, TonyR}@infoscience.otago.ac.nz [2]

**Abstract.** This paper proposes to design a mechanism that will allow Maori users to specify their privacy preferences related to their culture when a software system asks for culturally sensitive information. We first identify various concepts associated with sensitive aspects of Maori culture, such as tapu. We propose to build an ontology that describes these concepts and the relations between them in a formal way. This ontology will help service providers integrate Maori cultural protocols in order to make Maori users more confident about the use of the sensitive information related to their culture.

**Keywords:** Privacy, Maori Culturally Sensitive Information

## 1 Problem Statement

Our research deals with building a software infrastructure for protecting culturally sensitive information of Maori people. Modern software systems do not take into account the cultural aspects of Maori. When a Maori person accesses a service on the Internet, there might be some information that she might wish to provide to the service provider due to restrictions imposed on her by her cultural values. Sometimes such a request could be considered as an offense. One particular example is healthcare software systems, which request personal information from Maori people that could be considered taboo.
In this research we propose to design a mechanism that will allow the Maori users to specify their privacy preferences related to their culture when a software system ask for culturally sensitive information.

## 2 Solution

In order to solve the privacy problem related to culturally sensitive information of Maori, we use the Platform for Privacy Preferences Project (P3P) [1], and the P3P Preference Exchange Language (APPEL) [2] specifications. A P3P document that provides information about the privacy policies is stored in a web server. An APPEL file contains the privacy preferences as specified by the user. Both P3P and APPEL use XML based language, which is easier for the humans to read. So, when a user sees the P3P policies specified by the service provider, she can easily understand what

details are required. The user can specify her preferences easily. Another advantage of the use of XML is the easier comparison of APPEL and P3P rules. For automatic comparison of APPEL preferences and P3P policies we have implemented a specific module called *Evaluator*.
In order to explain our solution, we first describe the information that is sensitive to Maori culture. Then, we will take the National Cervical Screening Program (NCSP) [8][9] offered by the New Zealand government as an example to illustrate the process model of various entities dealing with the exchange of personal information.. Finally, we will discuss the implementation of the *Evaluator* module.

### 2.1 Sensitive information in Maori culture

In Maori culture, certain concepts are considered taboo that are not taboo in western culture. For example, the Maori word “tapu”, reflects something that is holy or sacred. For Maori, the human body and anything associated with it are tapu. So, these parts should be treated with great respect. For example, photographing a body is culturally unacceptable to Maori because the head is the most sacred part of the body for many Polynesian tribes including Maori. Therefore, permission should be obtained to touch a Maori person’s head or any other body part. “Whakapapa” is the genealogical descent of all living creatures from gods to the present time [3], and is believed to be an identifier of an individual’s intrinsic tapu [4]. Thus, Whakapapa information should only be accessed by individuals after having consulted with the relevant tribes. Also, Maori are sensitive about aggregated data as well. An example of aggregated data is the data collected in the -NCSP, that combines several smear results from different individuals. These aggregated and anonymous data have enormous spiritual and cultural significance for Maori because they contain statistics about Maori that will reveal more profound cultural behaviors belonging to a Maori community. For instance, this aggregated information can be a collective information about descendants and members of the “whanau”. Whanau is a wider concept than just an immediate family made of parents and siblings. The whanau links people of one family to a common ancestor. Each member is an identifiable individual in the whanau [5]. For this aspect, a special group named “Kaitiaki” [10] group is established to protect the aggregated data of Maori women on the NCSP. Moreover, another cultural aspect of whanau is that the information is normally shared with its members. This means that, if a family member is sick, the whanau is involved from day one [6].

### 2.2 Sensitive information in Maori culture

In this section, we will take the NSCP [8][9] as an example to illustrate the process for providing the privacy protection of Maori culturally sensitive information. The NCSP set up in 1990 aims to reduce the incidence of, and mortality from, cervical cancer among women in New Zealand. The program organizes cervical screening to encourage women to have regular cervical smear tests and to check that abnormal results are followed up.

There are three entities involved in this process. Firstly, the National Cervical Screening Program Register (NCSP-R) stores all the data about the women enrolled in the NCSP. Secondly, the Kaitiaki group protects the Maori women summary data by limiting the access to this information. Anyone wants to access the summary data of Maori women, has to get permission from the Kaitiaki group first. The third entity is the user. The users are the people who could potentially use the NCSP-R service, which includes the women registered with the NCSP, and other people requiring information from the NCSP-R, such as health practitioners and scientists working on cervical cancer. The process of information exchange between the three entities is illustrated in Figure 1.

Assume that a Maori patient requires her own cervical screening records, she will contact the NCSP-R. Then the NCSP-R will ask her what kind of information she is interested in. Also assume that she is interested in data about a Maori individual. The register service will ask if the information is about the requester herself. If the data is about herself then her credentials will be verified by the service and the data will be provided. This simple process involves quite a few information exchanges. For example, when the NCSP-R verifies the identity of the woman, it will ask her to provide the evidence that she is the patient. This is when our P3P and APPEL mechanisms are used. For example, the NCSP-R specifies its P3P policy to say that in order to verify the identity of the woman, she needs to provide her full name, date of birth, National Health Index (NHI) and the name of the tribe she belongs to. However, as a Maori patient, if she doesn't want to give the information about her tribe, she can specify her APPEL preference in accordance with that. Thus, APPEL provides a mechanism for users to specify what privacy level they expect. We have implemented an agent-based trust engine using the Opal platform [7] that is capable of matching APPEL preferences specified by the user and the P3P policy specified by the service provider. If the APPEL preferences and P3P policies match, the process will continue. If not, the user will be asked whether she wants to relax her preference. If she decides to relax the APPEL preference to satisfy the server's P3P policy, then the verification step will be carried out before providing the data. Otherwise, the process will end here. The next section explains how the Evaluator is implemented.

Figure 2 shows the infrastructure that we have designed including the privacy agent which is part of the agent-trust engine, the service provider and the different processes of specification, storage and matching of privacy preferences and privacy policies

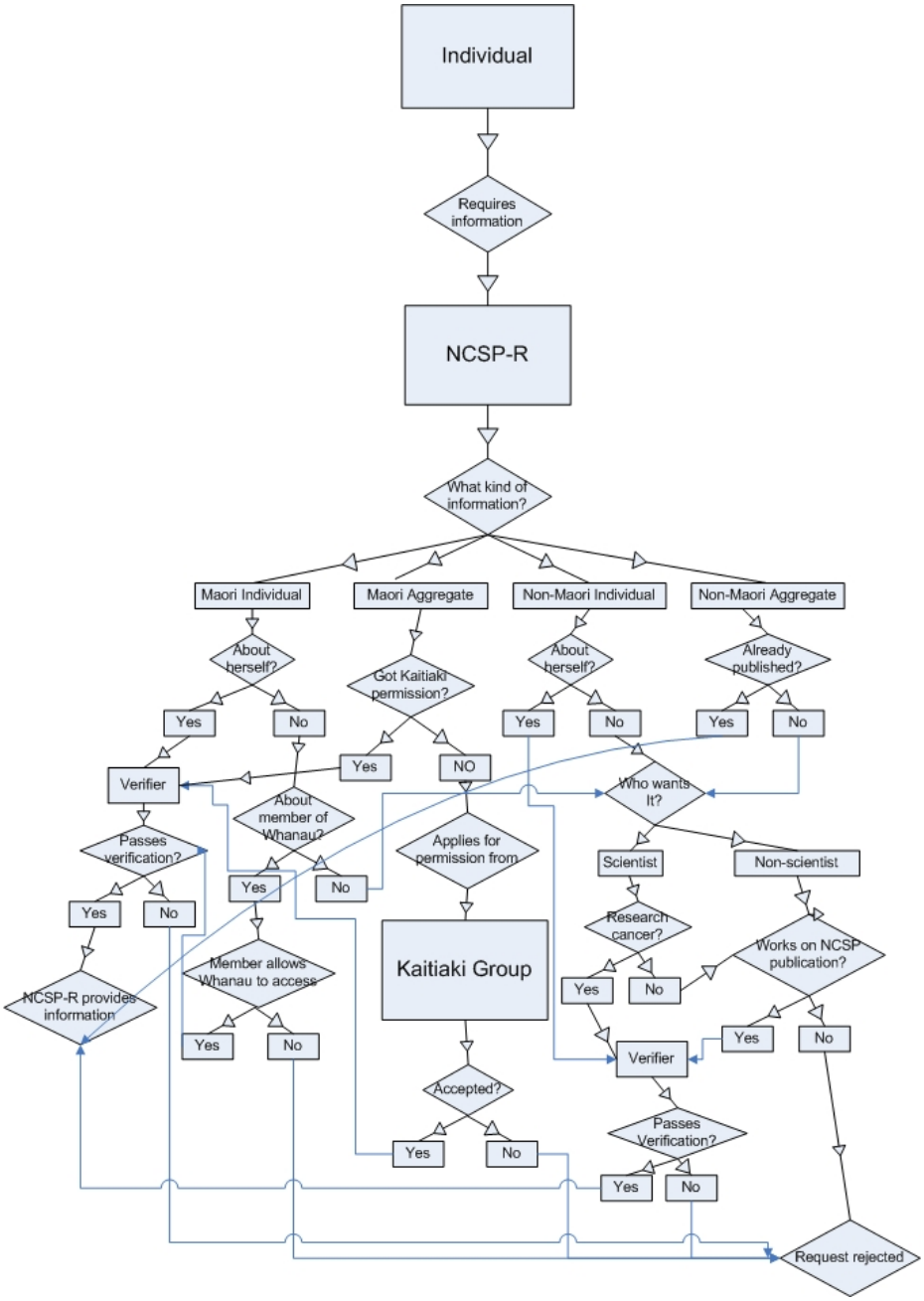


**Fig. 1**. Process associated with an individual accessing the data stored on the NCSP-R.

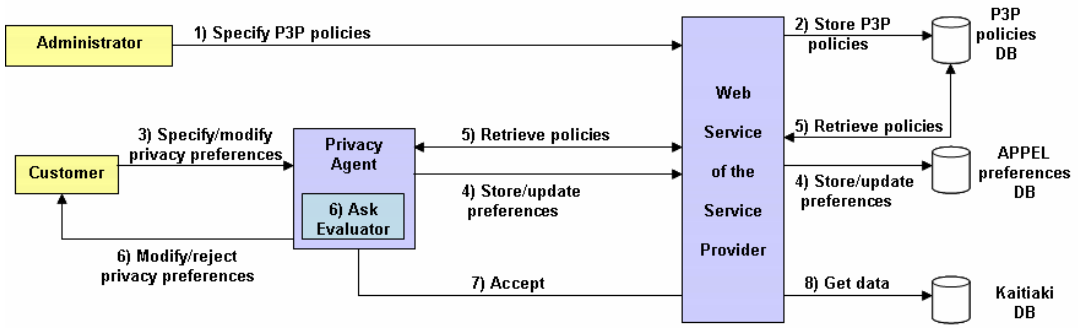


**Fig. 2.** Privacy infrastructure for accessing the data protected by the Kaitiaki group.

### 2.3 Description of how the evaluator works

The purpose of the Evaluator is to compare each APPEL rule (with the P3P rule , and then decide whether the APPEL preferences and the P3P policies match, depending on how strict each APPEL preference is specified by the user. The strictness of the APPEL preference is specified by the "connective" parameter in the APPEL preferences. There are six types of connectives that can be used in APPEL. For example, if a woman using the NCSP service is willing to give her physical contact details, and her NHI number, but she is not willing to give more information she will specify an APPEL preference containing the "or-exact" connective. The APPEL specification that defines what kind of data she is willing to provide is given below.

```
<appel:RULE behavior="request" description=" ">
   <p3p:POLICY>
    <p3p:STATEMENT>
     <p3p:DATA-GROUP>
      <p3p:DATA>
       <p3p:CATEGORIES appel:connective="or-exact">
        <p3p:physical/>
        <p3p:uniqueid/>
       </p3p:CATEGORIES>
      </p3p:DATA>
     </p3p:DATA-GROUP>
```

The evaluator takes each element of the CATEGORIES tag from the APPEL preference, and searches through the CATEGORIES tag in P3P policy, to see whether these elements match. Because the connective is "or-exact", the match will return true only if the P3P policy requires either "physical", or "uniqueid", or both. If the P3P policy requires more information than these two, the match will fail. This Evaluator mechanism enables the automatic comparison between the APPEL preferences and the P3P policies. Our implementation of the Evaluator works for all the six types of connectives of the APPEL specification [2].

## 3 Current Status and Next Steps

Information-sharing practices for Maori are inextricably connected with the wider cultural context. Therefore any digital manipulation of Maori information requires the understanding of the fundamental concepts and principles belonging to the Maori culture. Because digital systems lack the integration of such fundamental concepts, we are designing an ontology related to personal and culturally sensitive information in the context of NCSP. For instance, this ontology would help to integrate the vital role played by the whanau in the NCSP process and in the New Zealand healthcare system in general. We hope that our preliminary work on a Maori ontology will help service providers be aware of culturally sensitive information for Maori and serves as a reminder that providers need to avoid infringing on Maori cultural values.

Our work has focussed on building a privacy infrastructure for protecting culturally sensitive information of Maori in New Zealand. In this context we have used P3P and APPEL to represent user preferences and service provider policies. We believe that our privacy infrastructure can be used as a reference in those societies where the privacy of the members is directly impacted by the cultural aspects.

One crucial outcome is for health care providers to become more comfortable with the use of Maori culturally sensitive information when they interact with a Maori patient. To guage our success in this goal, we envisage utilizing a questionnaire to gather feedback from healthcare practitioners. For this purpose, we will build a prototype tool integrating the ontology (using simulated data and scenarios) to show to some practitioners to get their feedback

## References


1. Platform for Privacy Preferences (P3P) Project. Available: http://www.w3.org/P3P/
2. A P3P Preference Exchange Language. Available: http://www.w3.org/TR/2002/WD-P3P-preferences-20020415/
3. Barlow, C., “Tikanga Whakaaro: Key Concepts in Maori Culture”. Oxford University Press, Auckland, New Zealand, 1994.
4. Glover, M., “Kaupapa Maori Health Research Methodology: a literature review and commentary on the use of a kaupapa Maori approach within a doctoral study of Maori smoking cessation”. Applied Behavioural Science, University of Auckland, New Zealand, 2002.
5. Te Puni Kukiri - Ministry of Mauri Development, “The Privacy Act 1993, Maori guide to the Privacy Act - Te Ture Matatuakiri”, Matatupa 1993 PO Box 3943 Wellington, 1994.
6. Te Puni Kukiri - Ministry of Mauri Development, “Privacy of Health Information - Te Matatuakiri me te Matatapu o Ngc Kurero Hauora”, 1994.
7. Nowostawski, M., Purvis, M., and Cranefield, S., “OPAL A Multi-level Infrastructure for Agent-Oriented Development”. In Proceedings of the 1st. International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS 2002). ACM Press (2002) pp.88-89.
8. The National Cervical Screening Program: http://www.moh.govt.nz/nationalcervicalscreeningprogramme
9. http://www.healthywomen.org.nz
10. The Kaitiaki Group: http://www.kaitiaki.org.nz/