Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features

Elahe Kani-Zabihi and Martin Helmhout

Information Security Group, Royal Holloway University of London,
Egham, Surrey, TW20 0EX
{Elahe.Kani,Martin.Helmhout}@rhul.ac.uk

Abstract. The work presented in this paper introduces the concept of *On-line Interactive (OI) privacy feature* which is defined as any on-line interactive tool, component or user-interface that creates privacy awareness and supports users in understanding their on-line privacy risks. These features have been developed as an *interactive social translucence map* that discloses the flow of personal information, a *privacy enquiry* for a direct chat about users' privacy concerns and a *discussion forum* presenting users' privacy concerns using their language in an interactive FAQ format. The paper presents an evaluation of a prototype of this set of embedded OI privacy features. The field study presented evaluates the prototype's usability and its effect on users' privacy awareness, understanding and attitude. 100 participants took part in the study and were drawn from groups of *experienced* and *less experienced* users. Both quantitative and qualitative data collection methods were used. Findings suggest that OI privacy features increase users' privacy awareness and encourage users to find out more about the uses of their personal data. However, users' ICT skills and Internet experience significantly influence whether a feature is favoured or otherwise. In general, it is concluded that privacy features are very much welcomed and necessary to empower users to manage their privacy concerns but some groups need to be further supported by social and institutional privacy management processes.

Keywords: On-line privacy, interactive privacy feature, privacy awareness, privacy concern, usability study, mixed-method research method, privacy transparency, user study, social translucence, HCI.

1 Introduction

This paper continues previous research [13] and is part of a project entitled **Visualisation and Other Methods of Expression (VOME)**. VOME's main objective is to develop methods of expressing privacy that enable a wider range of privacy concerns to be articulated. An increasing number of organisations deliver their products and services on the Internet, which attracts people (on-line service users) from all walks of life to use these services. For the past two years we have studied and participated in privacy and security related workshops and nevertheless, it is clear that there

P. Laud (Ed.): NordSec 2011, LNCS 7161, pp. 131–148, 2012.

Table 1. Service Users' Requirements

The on-line service platform should consider the following:
1. Display information about the service provider on screen before the registration process.
2. Display feedback from other organisations and service users about the service provider.
3. Inform service users of their personal information requirements before the registration process.
4. Display the service provider's privacy policy on screen.
5. The information provided on privacy policy should be readable, concise, noticeable and in a language understandable by all types of users.
6. Display the service agreement between service user and service provider on screen.
7. Provide a printable and saveable service agreement between the service user and the service provider.
8. Inform the service user about what is going on by providing appropriate feedback within reasonable time.
9. Allow the service user to frequently engage in an interaction practice at each stage of the registration process enabling the user to raise concerns through a communication channel with the service provider.
10. Provide information on the security technology implemented by the service provider.
11. Provide a secure channel only available to a valid service user.
12. Request only personal information that is necessary for delivering the service.
13. Immediately inform users of any changes made to an online service by the service provider.
14. Give service users a reasonable amount of freedom to decide on how they will maintain their relationship with the service provider.
15. Adapt to the service users' characteristics.
16. The service users should have control over personal information collected by the service provider.
17. Inform the service user of the purpose for collecting each personal detail.

is still a gap between the current privacy related studies and the real need of users with respect to their on-line privacy concerns.

On-line service users have privacy concerns when they are forced to disclose their personal information [11, 13]. On the one hand, service users want to know what happens to their data [15]. On the other hand, system developers have ignored the importance of privacy in technology design [16, 24]. A study in Belgium [15] reported that young adults are more vulnerable to privacy threats and at risk when revealing personal information has become easier. Moreover, it is stated that service users disclose personal information more frequently without any indication of the possible consequences. Therefore, one of the aims of VOME is to address this issue by introducing new On-line Interactive (OI) privacy features, which enable users to make clearer on-line disclosure choices. The term 'on-line interactive privacy feature' is defined as any on-line interactive tool, component or user-interface that creates privacy awareness and support users in understanding their on-line privacy risks. OI privacy features can increase users' privacy awareness by informing them on how their personal information is used by the service provider(s). The study presented in this paper introduces the first version of a user-centric web service prototype with embedded OI privacy features. The central component of the prototype is a 'translucence[1] map' presenting service users' data flow between user and service-provider(s).

[1] Translucence in this paper is defined as semi or partly transparency. For example in the context of information: anonymised information or aggregated information.

Other OI privacy features were selected from current on-line interaction tools such as an on-line chat system and a forum. In this paper we also present the results obtained from a user study. We evaluated the privacy features and tested them concerning usability and change of privacy awareness. Consequently, in this paper, the importance of embedding OI privacy features during on-line registration process has been argued. In the attempt to design a user-centred prototype [14] of an on-line service, we elicited users' requirements with respect to on-line privacy. Based on the result which has been reported in [13] and [9], a list of user requirements for on-line services was gathered (Table 1). Hence the first version of an on-line service platform with embedded OI privacy features prototype was designed. The description of the design and design principles are provided in section 3. In order to test and evaluate the usability of OI privacy features, a user-centred study approach was conducted. Hence users were asked to interact with the prototype. The outcome of this study is reported in section 4. Finally, in section 5 we conclude our study and discuss our future work.

2 Related Work

The world is moving towards a virtual environment where users benefit from the convenience of using services on-line but are also expected to be digitally enabled and confident in all aspects regarding the use of on-line services. Considering that there are few system developers who think about privacy in their technology design [24], our research explores how recent privacy research has contributed to a better communication and interaction between both service users and service providers. We conducted a literature review and gathered a list of the relevant long term privacy projects running worldwide:

Ensuring Consent & Revocation (EnCoRe) project is working on a prototype system to allow users to have more control over their data[2]. Our research is similar to EnCoRe by looking at users' requirements with regards to privacy and more meaningful consent. However, our study takes a step further by eliciting these requirements from service users implicitly as well as explicitly (more details given in next section). Moreover, we are designing an interactive system where both users and service providers can exchange information about on-line privacy.

Privacy Value Networks (PVNets) project is developing and applying new methodologies for the study of privacy[3]. Our study (with a different focus) is in line with PVNets by looking at an appropriate research methodology to study privacy. However, while PVNets explores privacy value chains, our research is focused specifically on the privacy features and the relationship between service users and service providers.

According to **Privacy-aware Secure Monitoring** (PRISM), network monitoring could become a threat to users' privacy by keeping individual communications under surveillance[4]. Therefore, to enhance the level of data protection, the aim of PRISM is to develop a traffic monitoring architecture which guarantees privacy preservation by

[2] http://www.encore-project.info/press.html
[3] www.pvnets.org
[4] www.fp7-prism.eu

avoiding disclosure of raw data even inside the controller domain itself. Despite the fact that PRISM identifies a technology solution to preserve the service users' privacy by avoiding disclosure of data, this is still not helping the fact that users themselves are not informed why their personal data should be given in the first place.

Privacy and Identity Management for Community Services (PICOS) project is testing and evaluating a mobile communication service prototype which uses a location identifier system[5]. A "privacy advisor" technology has been implemented in this system where users are informed about the privacy risk at each stage when users reveal their location to other service users. Our work in a different context is similar to the PICOS project by informing users about their on-line privacy risk in advance of personal data revelation.

PrimeLife[6] is based on the FP6 project **PRIME** (Privacy Identity Management) has demonstrated that privacy technologies can enable citizens execute their legal rights and control personal information in on-line transactions. PRIME was also a continuation project after the **PISA** (Privacy Incorporated Software Agent) project. PISA built a prototype and created a list of requirements necessary to develop software agents that safeguard users' privacy.

EU FP7 PrimeLife project launched (February 2010) Clique as a privacy enhanced social networking site. The privacy control functionality in Clique enables users to modify privacy settings in a way that users can choose who can see their new information before it is published on the site. PrimeLife also produced a privacy awareness tool called Privacy Dashboard[7]. The tool informs users of possible embedded browser-cookies. Service providers use those cookies to collect data about users' online behaviour. Our study focuses on the service provider explicitly informing the user about the use of their personal information. Hence, in our study, we implement online interactive tools that inform users beforehand of what will happen with their disclosed personal information after a registration process. Besides that, our work aims to include less-experienced users whereas Privacy Dashboard requires users to have a certain level of ICT skills.

In PICOS and PrimeLife (including finished projects: PISA and PRIME), the focus is on privacy protection, communication of privacy stances by either party, or the reporting of privacy status and risks. However, tools are not being developed to encourage interaction and create dialogues enabling both parties to respond to each other's concerns.

Many researchers [6, 7, 8, 15, 16, 17, 18 and 22] highlighted the 'relationship between privacy and technology' [18] and the importance of knowing what data is collected and stored by whom [6]. However, few studies have focused on a pioneer in privacy awareness using technology. A summary of related studies is reported in this section. In an article by [22], Web 2.0 users' privacy issues are discussed and classified into four categories: users' personal information; users' seeking behaviour privacy; threat from a third party and leaking of users' privacy documents. We are

[5] http://www.picos-project.eu
[6] www.primelife.eu
[7] http://www.primelife.eu/results/opensource/76-dashboard

inclined with their opinion of: "privacy protection should not only be approached as a technical concern but also as social consideration". Moreover, the authors introduced a list of privacy-enhancing measures. Relevant to our study is their Privacy Policy Statements measure, in which the authors state: users should be informed of the privacy of their sensitive data; how and when the data will be collected and processed; for which purposes it will be used and by whom. Interestingly, in compromising between privacy and trust, the author suggests: an effective collaboration between service providers and users is important in promoting privacy awareness (educating users on privacy and the risk of identity disclosure). Similarly, as the authors suggested, in our prototype a "synchronous interactive behaviour (chat)" [22] is provided as an option to increase users' privacy awareness. Therefore, the on-line chat option enables users to communicate with the service provider about their privacy concerns. With relation to privacy awareness, research indicates that privacy salience [1] or increase in awareness can increase people's worries about their privacy. With taking context into consideration and adopting customer relationship management principles (see next section), the provider is able to create a trustworthy (and trust building) environment. Hence, managing the relationship between the user and provider can create confidence and turn the negative effects of salience into a positive attitude towards the provider. Another study (in Web 2.0 users' privacy issues) by [15] conducted three user studies looking into three ethical issues: trust, privacy and etiquette in developing Web 2.0 applications. Hence the authors revealed a set of important user requirements of Web 2.0 applications of which one is in line with our study: privacy. The first study conducted in Norway with 200 participants (from various age groups) used a survey to collect the data. The study investigated the problem users experienced using social network sites (SNSs) and reported: users require control of their personal information. This relates to the control privacy mechanisms in different forms of intervened interaction designed to protect access to and publication of personal information. These privacy mechanisms should be user friendly. Otherwise the complexity of such settings will be ignored and avoided by users, despite the importance of privacy. Moreover, it was reported that students were careless in the revelation of personal information in SNSs; and finally, users have privacy concerns and want to know what happens to their data. Likewise, in designing our first version of the prototype (section 3), we considered that the OI privacy features should be accessible to different kinds of users and therefore complexity in the functionality needs to be reduced to a minimum. Furthermore, translucence maps (described in section 3.2) were used to explain users what will happen to their data when they submit their data to the service provider. The second study by [15] consists of 30 members of two on-line communities. The first group was a community of 50+ years old who had no ICT skills. The second group was a community of young men with good ICT skills and interested in photography. Participants from the first community were asked to answer questions on a blog on the on-line community site. The second community was asked to use provided diaries to report on a daily basis. Both groups were questioned on their on-line activities and the type of communication channels they used. The study revealed that the most important issue for all participants was privacy. When sharing information on-line, the younger adults used privacy options whereas the seniors used the more

traditional way of privacy practice by avoiding disclosure of personal information. Similar to [15], in choosing our participants for the user study, both ICT skilled users and inexperienced users were recruited. However, as opposed to [15], the same research methodology was used for both groups. This is described in section 4. Finally, [15] conducted another study in Belgium with two communities: the first an unstructured group of 85 families with children and the second a structured group of 50 gay males (40 to 50 years old). The participants were given access to an on-line community platform and provided with a digital camera to generate and share contents. Their activities were observed, monitored and logged. The participants were interviewed and various focus groups were organised to collect data. On the subject of privacy, the authors reported that the website's restricted access gained users confidence to share more personal information. Furthermore, users found it important to have control of how and with whom they shared their personal information. On the subject of transparency, the authors concluded that the on-line community site should be transparent implying that messages or comments on the website should be presented clearly. Moreover, messages should indicate whether they are viewable for everyone or only to specific persons. Likewise, in our prototype (section 3.2), the inspiration of transparency (translucence maps) is considered to be one of the more important OI privacy features in the design.

Correspondingly, on the same subject of transparency, the work presented by [10] introduces a privacy policy visualization model where users are able to better capture the designed privacy policies. The proposed theoretical visualization model facilitates understanding the privacy policy in place and avoids users reading the entire statement. Hence both service users and providers will be able to understand the policies without the need of reading the entire privacy policy statement. In designing our prototype, we have taken an approach contrary to [10]. Rather than just focusing on privacy policy statements, the focal point was more on presenting what happens to service users' data and providing a communication channel where users can raise their privacy concerns.

Finally, [19] introduces a user-centric privacy architecture that enables the provider-independent protection of personal data. The prototype designed for an on-line privacy community, facilitates the open exchange among users of privacy-related information about service providers. As opposed to the 'provider-independent' approach taken by [19], we believe that it is beneficial to users when service providers are involved in both privacy protection and privacy awareness processes.

3 Design Principles

In designing an on-line service with embedded OI privacy features, we adopted HCI usability design guidelines and principles by Nielsen [25] and Raymond [21]. These are important principles that designers should consider when developing usable and accessible systems. Table 2 shows a list of system requirements for an on-line service with embedded OI privacy features using the HCI usability design principles.

Table 2. System requirements using HCI principles

No.	HCI design principles	System requirements for an on-line service with embedded OI privacy features
SR1	Match between system and the real world	The communication channel provided, should feel similar to off-line dialogue when users freely discuss their privacy concerns.
SR2	Recognition rather than recall	Links to privacy policy statements and service's term and conditions should be clearly visible and familiar to all users.
SR3	Aesthetic and minimalist design	The system should avoid using information that is irrelevant or rarely needed.
SR4	Visibility of system status	The system should inform the user about what is going on by providing appropriate feedback within reasonable time.
SR5	Rule of confirmation	The system should provide a contract (an agreement between the user and the provider) stating that the user's personal information will be safe and confidential.

Table 3. System requirements using CRM principles

No.	CRM principles	System requirements for online service with embedded OI privacy features
SR6	*Initiating behaviour:* Service provider pro-actively initiates efforts to better understand a user's needs and requirements	Informing a user about services and particularly making users more aware (in advance) about privacy.
SR7	*Signalling behaviour:* Service provider provides advance information about intended changes in its marketing programs	HCI components that allow interaction between user and provider about intended changes.
SR8	*Disclosing behaviour:* Service provider is perceived to provide *sensitive* information about itself.	The service provider is disclosing sensitive information (working practises, relationships with third parties).
SR9	*Interaction frequency:* The inverse of the average time elapsed between consecutive user and service provider interactions.	When interactions take place more often, mutual trust in a relationship gets a chance to increase.
SR10	*Richness*: The richer the channel, the more complex messages can be transferred.	Richness can vary on a scale from high to low: video conference, voice chat, text chat, and email.

In order to understand the user better, the service provider needs to invest in building relationships with its users or customers. Customer Relation Management (CRM) theory [3] is a strategy that can be adopted for managing service provider's interactions. Hence, when applied properly, CRM can have a significant impact on customer satisfaction and create a closer relationship between service provider and user. Therefore, in designing the prototype, we considered CRM design principles to be as important as HCI design principles. Table 3 shows the list of possible CRM principles and the requirements for an on-line service.

3.1 The Prototype

The disclosure of users' personal information often happens at the point of registration for an online service. Registration processes are often used when a relationship is needed for the longer term in order to deliver a service. In the following sections we exemplify our proposal with screenshots taken from the prototype. Consequently, we embedded OI privacy features during an on-line service registration. The prototype represents a mock-up council, Your Local Council (YLC), which offers an on-line smartcard registration service. The smartcard is used by the council to combine several services: a Library service, a Local Shops discount scheme and Local Transport, as part of one card. Figure 1 shows the first web page (Services) displayed after users selected the "Register me" link on the Home page.

For the purpose of this user study, all participants were asked to select 'Smartcard Services' from the list and move to the next page by clicking on the 'Next' button. All users are first directed to four pages before the registration page:

1. Introduction to smartcard services and selection of services

This page is shown in Figure 1. The user will start the registration process by selecting their services. This is an opportunity for the user to be in control of the type of services they register for. This procedure meets the following requirements: CRM principle: Initiating behaviour (SR6, Table 3) and User Requirements: 8 and 16 (Table 1);

2. About us

The service provider will display information about the nature of the organisation and other useful information for the user: description; contact details; and information about their partners (CRM principles: SR6 and SR8 (Table 3) and Users' requirements: 1 (Table 1));

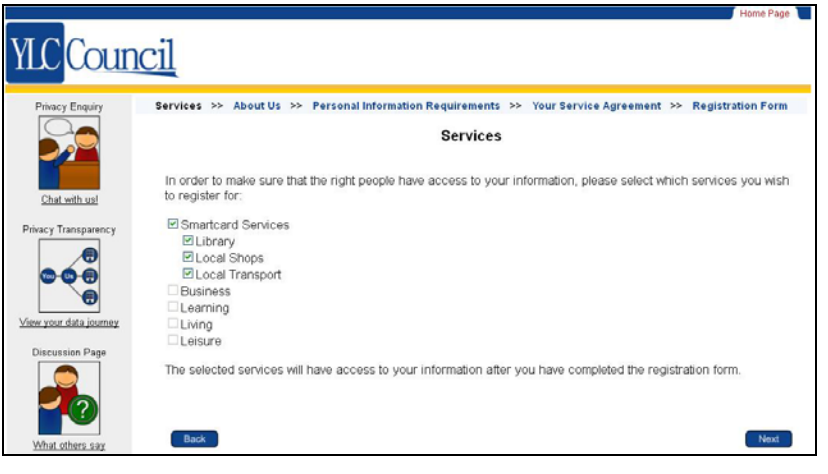

Fig. 1. Smartcard services offered by YLC Council

3. Personal Information Requirements

Displayed in Figure 6 (Appendix). The service provider informs the user that certain personal information is required to use the service, what will happen to the data as well as the reason for collecting it. This information will be communicated to the user with help of an interactive dataflow map that displays who has access to what type of personal information (CRM principle: SR8 (Table 3) and User Requirements: 3 and 17 (Table 1));

4. Service Agreement

The service provider gives a contract of their agreement for the user to keep as a reference. An overview of selected services, privacy policy and terms & conditions (User Requirement: 6 (Table 1));

5. Registration form

Displayed in Figure 7 (Appendix). The final step of the process displays a registration form where the user discloses the necessary personal information for getting the selected service(s). During the registration process, the user is able to get help and access the three OI privacy features (left panel in Figure 1). The next section elaborates this further.

3.2 On-Line Interactive Privacy Features

The OI privacy features are designed with usability and (social) interaction / sociability in mind. Usability and sociability in design are important when interaction between user(s) and provider takes place, especially when interaction needs to be (partly) controlled by bringing in social policies [20].

1. Privacy Enquiry: Fulfilling CRM principles (SR9 and SR10, Table 3) and also meeting the needs of users for a private and synchronous communication channel calls for an on-line chat tool. Users can instantly communicate with a service provider regarding their privacy concerns. In order to meet CRM *signaling* principle (SR7, Table 3) and Users Requirements 10 and 11 (Table 1), the chat tool informs users of a secure private channel of communication by displaying three icons: a 'live' icon assuring the user that there is a person on the other side ready to listen, a 'padlock' icon indicating the communication channel is secure, and a '1:1': icon showing the user that the communication is a one-to-one conversation. This is shown in Figure 2. The disadvantages of chats, besides not seeing the other person, are that they do not give much time to reflect or correct faults which can lead to chaotic interaction. However, people who are regular users are enthusiastic and do not have such complaints [20]. A final aspect to consider is whether the privacy enquiry gives the user enough comfort to discuss concerns that are sensitive and personal.

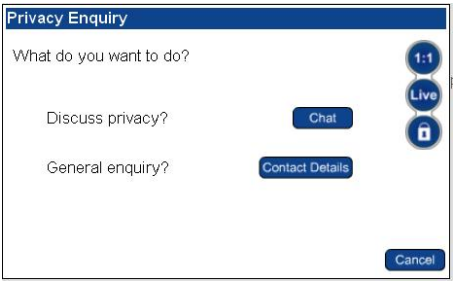

Fig. 2. Initiating on-line privacy communication

2. Privacy Transparency[8]: One of the aspects of privacy is personal information and the need for more transparency. Whereas privacy is difficult to describe and is perceived differently depending upon cultural background, personal information is an easier way to address many common problems concerning privacy. Besides that, because of interaction and location, personal information (or its perceived meaning) is situated and part of the perceived inner context as well as the perceived outer context. Concerning context and interaction, we adopt the notion of context as an interactional problem [4], which states that context is a relational, dynamic and occasioned property and arises from activity and is produced and maintained by that activity. Concerning (semi) transparency, we adopt *social translucence* [5] which makes users aware of the presence of other groups or activities, but does not (necessarily) reveal their identity. Figures 3 and 4 both depict a user interacting with the translucence map and shows what data is needed when eventually the user registers for a particular service. Figure 3 shows that *gender* information is only given to the Council, consultancy company 'CardSmart' and 'Local Shops', and not to parties whose access is blocked by a cross. Figure 4 shows which information is accessed by 'Local Shops'.

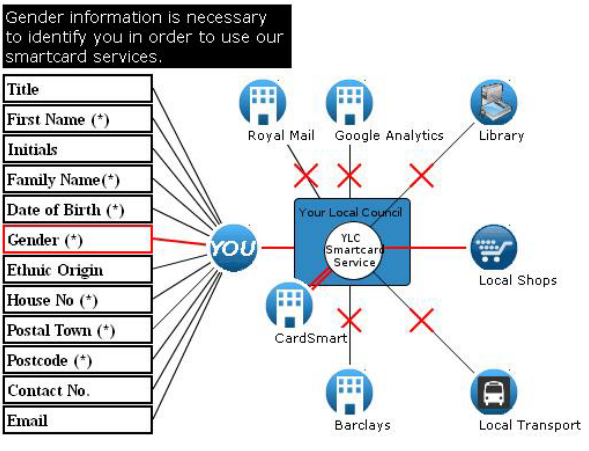

Fig. 3. Translucence Map (1)—User moves mouse over Gender field

[8] In the prototype we use the term Privacy Transparency because transparency is understandable language (User Requirement 5 (Table 1)) whereas 'Translucence' could puzzle the user.

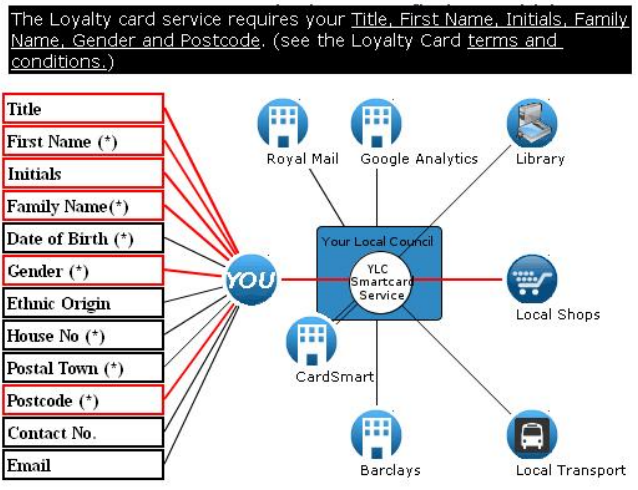

Fig. 4. Translucence Map (2)—User moves mouse over Local Shops icon

3. Discussion Page: The discussion forum (Figure 5) is designed as a knowledgebase for users to find answers to the concerns they have. The knowledge base contains previous users' privacy enquiries and answers from the service provider. The policy of the discussion forum is to allow users to submit comments and let the provider moderate those comments. Hence, the user sends a comment and receives feedback that response will follow the next working day. Registration is not needed and therefore the forum is open to comments from everyone. However, moderating the comments assures the knowledge base to present reliable answers of the provider but also represent the questions and views of the users.

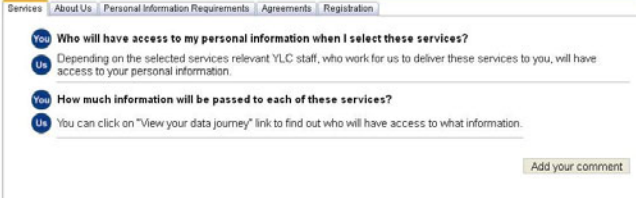

Fig. 5. Discussion forum

4 User Study

In order to evaluate the usability of the OI privacy features, there is a need to elicit on-line service users' opinions and observe their behaviour during interaction with the prototype. We were interested in a wide range of Internet users. In addition to Internet users with more than five years experience we recruited 'non-users' as well. In HCI non-users are regarded as potential users who might in the future engage with the system but are currently inactive users. The current state of technology has not the

right answer to gain their confidence and reduce their privacy concerns. We suggest that designers should consider non-users' opinions in cases where OI privacy features are adopted for the development of on-line services. When non-users feel comfortable and have their needs fulfilled, they possibly return and eventually can become future on-line service users [23].

4.1 Participants

We recruited participants from nine UK online centres[9]. All participants were recruited by the Centre Manager and were offered a shopping voucher as a reward for their contribution to the research. Following the result reported by [15] (students have less privacy concerns), we recruited 10 students from Royal Holloway University of London (undergraduate and postgraduate levels) to study their behaviours towards and opinions of OI privacy features. Correspondingly, 100 users (65 Female and 35 Male) between 16 to 60 years old participated in our user study. Participants were questioned about their Internet experience. Hence, it is reported that 64 of them had more than five years; 21 between one to five years; and 15 less than one year experience with Internet as source of information. Participants were also questioned about their IT literacy. Using the IT literacy questionnaire [12], 41 were categorized as novice, 36 as intermediate and 23 as advanced users. Categorising participants based on their IT literacy helped us in usability evaluation of the OI privacy features and also to better understand different types of users' attitudes towards these features. We also were interested into two groups of *Experienced* and *Less-experienced* users. Therefore, participants were questioned with respect to their experience with on-line services as "have you registered with any on-line services in the past?". Accordingly, based on their Internet usage, IT literacy and also their experience with on-line services, 100 users were equally distributed between the Experienced and Less-experienced groups.

4.2 Research Methodology

The research methodology conducted was a mixed-method research [14] which is a combination of qualitative and quantitative methods with flexible and fixed questions. Therefore, data were collected using interview, observation, think-out-loud and questionnaire techniques. The study started with a questionnaire about general demographics including the computer expertise and the privacy attitudes about websites mostly focused on personal information. Following the questionnaire, users were introduced to the prototype as: "a website that projects the portal of a council, *Your Local Council (YLC)*". Each user was asked to take the role of a citizen and imagine the council to be his/her 'real' council. Then, the user was introduced to a *smartcard* service provided by the council. After the introduction, the user was asked to interact with the website and try to register with the council. Users were given approximately five

[9] The UK online centres network was set up by UK government to provide public access to computers in year 2000. http://www.ukonlinecentres.com

minutes to register. In an unsuccessful attempt to register, users were then given support by one of the researchers present in the field. Users who had successfully registered with the website were asked to interact further with the prototype to accomplish their tasks. The aim of these tasks was to make sure users interact with OI privacy features. While giving support, users were questioned to comment on what they would have expected to see in order to achieve the task. We applied think aloud protocol [9, 2] that helped us analyzing the interaction of the user with the website while thinking out loud. Simultaneously, we asked users to rank the usability of each task using an on-line questionnaire. Upon completion of all the tasks, users were asked to reply to a list of questions eliciting their privacy concerns with regards to the YLC council. The complete analysis of the data will be presented in a separate paper. Finally, we conducted a fifteen minutes interview to explore users' views and obtain a deeper understanding of users' requirements with respect to the embedded OI privacy features. Moreover, this was an opportunity to discuss users' behaviours during the interaction and their opinions about the features.

4.3 Results

In this section, we report the outcome of the prototype as a whole concerning privacy attitude and awareness and the results regarding the usability of the OI privacy features. Although the experiment was not conducted in a laboratory setting, we can conclude that in general many users mentioned that the prototype helped them understand what happened to their information. Users were asked about their general attitude in advance of the experiment and asked similar questions concerning their attitude concerning the prototype. Regarding users' privacy concern, we saw a reduction of 34% in users stating that they have concerns and a 33% increase in users that have no concern when comparing the YLC prototype with their general privacy attitude. Concerning disclosure and the way YLC collects processes and uses data, users were less concerned (35%). Finally, users commented that the YLC website helped them to be aware of how their personal information will be used in comparison to other websites they used in the past. The result shows an increase of 40% and only 14% disagree that YLC makes them aware. In general, the prototype with embedded OI privacy features seems to be very promising, but for a better understanding, we need to look at the usability of the OI privacy features. The usability study involved participants with different age and varying Internet experiences. Almost all users (93%) felt the registration process was easy to do. However 43% of users indicated they needed help in order to complete the task. The data gathered from think-out-loud and observation methods explain that less-experienced users had difficulties with finding the relevant links to proceed to 'Registration Form'. Therefore, non-users who had no experience with on-line services represent a further design challenge. Even though this type was concerned about their privacy, the OI privacy features were still insufficient to facilitate them in understanding the privacy information. Some of these users stopped interacting at the "Personal Information Requirements" page believing that they reached the registration page and hence completed the registration task without studying the 'translucence map'. During the interview session we learned that

once users were directed to the right direction, they were able to interact with the interface. One user commented that his lack of IT experience was the only barrier for him but once he was given guidance, he found the prototype very easy to use. Surprisingly, we noted that most users failed to notice the OI privacy features on the left hand side of the screen. One user commented: "I usually ignore this section as it belongs to advertisement". We will consider in the next development stage whether using the left hand side panel as part of the design needs to be avoided. The feedback from all participants was optimistic with regards to the translucence maps (Figure 4 & 5). Users were more in favour of receiving information given in figures and diagrams rather than reading them in text i.e. privacy statements. 89% of users said it was easy to use the map and 52% of them said no help was required. However, we learned in the interview that the 'red cross sign' on the map indicating that there is no flow of data, confused users. Moreover, the guiding text box on the top of the diagram was invisible to most users. The black background colour with white texts was not readable. As opposed to experienced users who found the diagram very easy to understand, the less-experienced users commented they were unsure about the functionality of the maps as there was too much information on the screen. This made them confused about what the purpose of the map was. 68% of users felt the service provider is trustworthy at this stage whereas only 17% said otherwise and 18% stayed neutral. The 'Privacy Enquiry' option was the least favourable OI privacy feature. The idea of chatting on-line only via text raised a privacy concern by itself. Users prefer to see or hear the other person when they have a dialogue with the service provider discussing their privacy concerns. Nevertheless, this option was necessary according to some experienced users who have prior experience with on-line chat channels. One user said that the availability of this option gives him a feeling of security and more confidence as there will be always someone to help. Therefore in the next version of the prototype, this communication channel should be developed further to not only a text chat but possibly include voice as well. Furthermore, by using this option, 70% of users felt they can rely on the service provider at this stage. Similarly, the 'Privacy Discussion' was mainly favourable by those who previously had experience with Frequently Asked Questions (FAQ). The importance of having this option available was highlighted by users. In the interview, users suggested that it was beneficial to read this information. However, it was unclear to them who raised these privacy concerns. Therefore, the next version of the prototype should be designed to make this information more transparent to users by clearly indicating who the users are that actually raise those privacy concerns.

5 Conclusion and Future Work

Previous researches [7, 9 &13] as well as our current study have shown that in general users are concerned when they are asked to disclose personal information. Whether this is caused by a lack of information received or inexperience, there is clearly a need

to reduce uncertainty and increase the interaction between service user and provider. The user study and the prototype with embedded OI privacy features, in particular the social translucence maps, demonstrate that users by interacting with the user interface are encouraged to explore and gather information. Moreover, users are also more aware about what to expect and what the consequences are regarding privacy when they register for a certain service. The prototype was designed according to a combination of user requirements, HCI and CRM principles. Together, they act as a guideline to design an interface that makes user and provider as well as the designer more aware of privacy issues. The HCI principle encourages the design of a usable and accessible system. The CRM principles put the emphasis on sociability and building a relationship between the user and service provider. The combination of requirements and principles led to the three components we implemented in our prototype: Privacy Enquiry, Privacy Transparency and Discussion Page. Although the participants in the study were aware of our research and the mock-up council website, the application of mixed-methodology allowed us to get a deeper understanding about how the user perceives and understands the interface. The 'think aloud protocol' gave us a better understanding about what needs to be improved about the prototype and specifically the features. The qualitative interview gave us more insight about how comfortable or confident a user feels. From the gathered results, we can conclude that our first prototype is a good step in the right direction. The feedback received from the participants makes clear that more research is necessary. The result from the user study also indicates that users are in favour of the interactive data flow map (translucence) and prefer to be informed of their personal information privacy. However, further work needs to be done on privacy communication channels and in this case the on-line chat tool was the least favourable privacy feature. Another part of further research is to involve the service provider in the design process and to investigate how much a service provider is willing to disclose sensitive information. Considering the needs and limits of a service provider can influence a design as well as contribute to the implementation of new features. Gathering information about the dialogue between a service provider and its users is crucial for a successful implementation of privacy features. In our future research, we will embed our privacy features in an existing website and gather feedback from 'real' online-service providers and users. Finally, as part of further research is a controlled HCI lab-experiment to measure differences in the relationship between privacy awareness, attitudes and how different groups respond to privacy features. The outcome of the experiment can help adjusting the privacy features towards groups with different needs.

Acknowledgements. We are grateful to all 100 participants who took part in this study. We also like to thank Consult Hyperion (www.chyp.com) for their contribution in implementing the web interface. This work was supported by the Technology Strategy Board; the Engineering and Physical Sciences Research Council and the Economic and Social Research Council [grant number EP/G00255/X].

References

[1] John, L.K., Acquisti, A., Loewenstein, G.: The Best of Strangers: Context Dependent Willingness to Divulge Personal Information (2009), SSRN http://ssrn.com/abstract=1430482
[2] Constantine, L.L., Lockwood, L.A.D.: Software for Use: A practical guide to the models and methods of usage-centred design. Addison Wesley (2000)
[3] Leuthesser, L., Kohli, A.K.: Relational Behavior in Business Markets: Implications for Relationship Management. Journal of Business Research 34, 221–223 (1995)
[4] Dourish, P.: What we talk about when we talk about the context. Personal and Ubiquitous Computing 8(1), 19–30 (2004)
[5] Erickson, T., Kellogg, W.A.: Social translucence: an approach to designing systems that support social processes. ACM Transactions on Computer-Human Interaction 7(1), 59–83 (2000)
[6] Breznitz, D., Murphree, M., Goodman, S.: Ubiquitous Data Collection: Rethinking Privacy Debates. Computer 44, 100–102 (2011)
[7] Coles-Kemp, L., Kani-Zabihi, E.: On-line privacy and consent: A dialogue not a monologue, September 21-23, pp. 1–15. ACM Press (2010)
[8] Hiok, C.Y., Khoo, V.K.T.: Education Services Mashup: Examining the Impact of Web Design Features on User Trust. In Second International Conference on Computer Research and Development, pp. 349–353. IEEE (2010)
[9] Coles-Kemp, L., Kani-Zabihi, E.: Practice Makes Perfect- Motivating confident on-line privacy protection practices. In: IEEE International Conference on Social Computing (forthcoming, 2011)
[10] Ghazinour, K., Majedi, M., Barker, K.: A model for privacy policy visualization. In: 33rd Annual IEEE International Computer Software and Applications Conference, pp. 335–340 (2009)
[11] Jensen, C., Potts, C., Jensen, C.: Privacy practices of Internet users: self-reports versus observed behaviour. International Journal of Human-Computer Studies 63, 203–227 (2005)
[12] Kani-Zabihi, E., Ghinea, G., Chen, S.Y.: Digital libraries: what do users want? Online Information Review 30, 395–412 (2006)
[13] Kani-Zabihi, E., Coles-Kemp, L.: Service users' requirements for tools to support effective on-line privacy and consent practices. In: The 15th Nordic Conference in Secure IT Systems (NordSec 2010), October 24-30. LNCS, pp. 106–120. ACM Press (2010)
[14] Kani-Zabihi, E., Ghinea, G., Chen, S.Y.: Experiences with Developing a User-Centered Digital Library. International Journal of Digital Library Systems 1, 1–23 (2010)
[15] Karahasanovic, A., Brandtzæg, P.B., Vanattenhoven, J., Lievens, B., Nielsen, K.T., Pierson, J.: Ensuring Trust, Privacy, and Etiquette in Web 2.0 Applications. Computer 42, 42–49 (2009)
[16] Karat, C.M., Brodie, C., Karat, J.: Usable privacy and security for personal information management. Communications of the ACM 49, 56–57 (2006)
[17] Information Commissioner's Office "Privacy by Design", http://www.ico.gov.uk/upload/documents/pdb_report_html/index.html (last accessed August 5, 2010)

[18] Palen, L., Dourish, P.: Unpacking privacy for a networke d world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 129–136. ACM (2003)
[19] Pernul, G., Kolter, J., Kernchen, T.: Collaborative Privacy Management. Computers & Security 29, 580–591 (2010)
[20] Preece, J.: Online Communities; Usability, Sociability, Theory and Methods. In: Earnshaw, R., Guedj, R., van Dam, A., Vince, T. (eds.) Frontiers of Human-Centred Computing, Online Communities and Virtual Environments, pp. 263–277. Springer, Amsterdam (2001)
[21] Preece, J., Rogers, Y., Sharp, H.: Interaction design: beyond human-computer interaction. John Wiley (2009)
[22] Xiaozhao, D., Jianhai, R.: Users' Privacy Issues with E-learning in Library 2.0. In: International Conference on Multimedia Information Networking and Security, pp. 90–92. IEEE (2009)
[23] Satchell, C., Dourish, P.: Beyond the user: use and non-use in HCI. In: Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7, pp. 9–16. ACM (2009)
[24] Spiekermann, S., Cranor, L.F.: Engineering privacy. IEEE Transactions on Software Engineering 35, 67–82 (2009)
[25] Nielsen, J.: Usability Engineering. Academic Press, Boston (1993)

Appendix

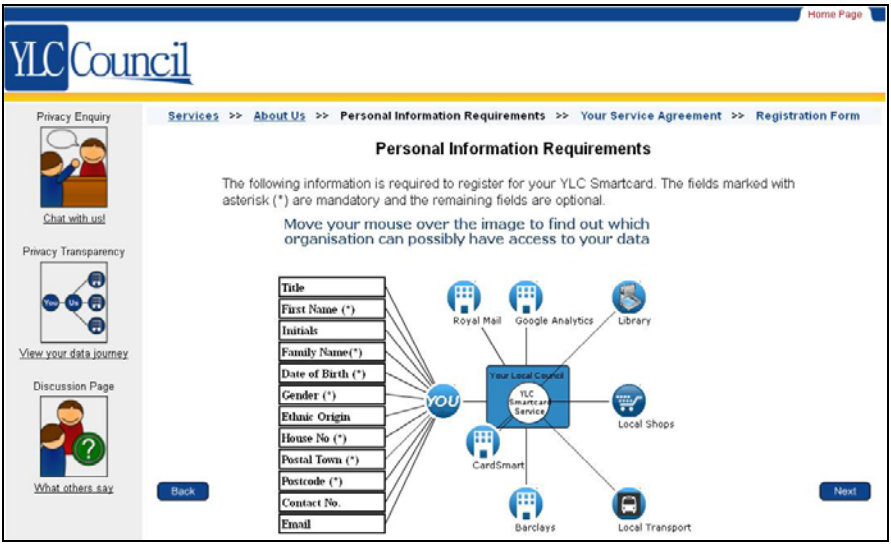

Fig. 6. Personal Information Requirements page

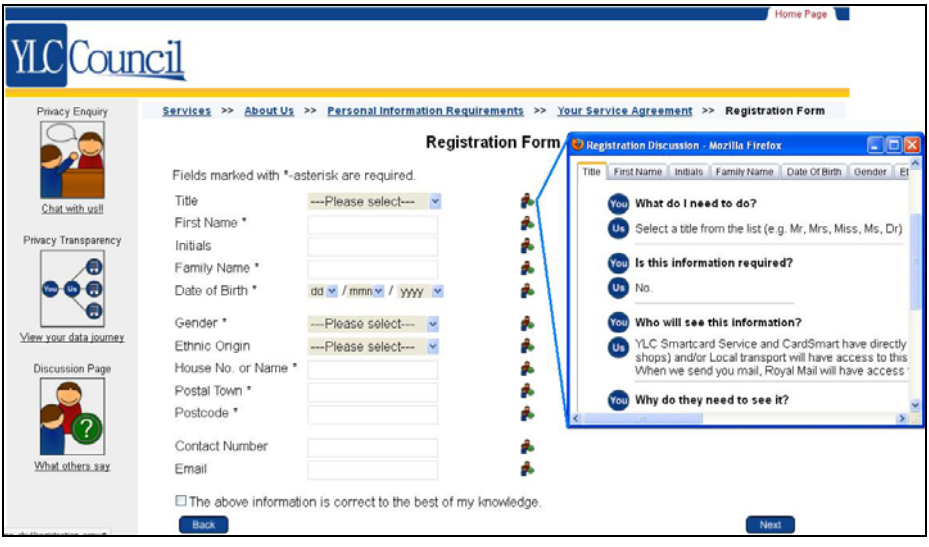

Fig. 7. Registration Form page