On-line Privacy and Consent: A Dialogue, Not a Monologue

Lizzie Coles-Kemp
Royal Holloway University of London
Egham
United Kingdom
+44 (0)1784 443 084
Lizzie.Coles-Kemp@rhul.ac.uk

Elahe Kani-Zabihi
Royal Holloway University of London
Egham
United Kingdom
+44 (0)1784 276 517
Elahe.Kani@rhul.ac.uk

ABSTRACT
With the move to deliver services on-line, there is a reduction in opportunities for a service user to discuss and agree to the terms of the management of their personal data. As the focus is turned to on-line technologies, the design question becomes one of privacy protection not privacy negotiation and conflict resolution. However, the findings from a large privacy survey and the outputs of several follow-up focus groups reflect a need for privacy systems to also support different types of privacy and consent dialogues. These dialogues are used to support the resolution of privacy dilemmas through the selection of effective privacy protection practices. As the face to face contact between service user and service provider decreases, the potential for these types of dialogues to become increasingly important grows. The work presented in this paper forms the initial part of a study to learn more about the types of privacy dialogue and negotiation that should be deployed in on-line services. In this position paper we outline the types of privacy and consent dialogues that service providers and service users want to have. We also explore how a socio-technical approach should ideally form the basis of the design and implementation of any dialogue system.

Categories and Subject Descriptors
K.4.1 Computers and Society [Privacy].

General Terms
Design, Reliability, Experimentation, Security, Human Factors, Standardization, Theory, and Legal Aspects.

Keywords
Service Users; Service Providers; Privacy; Privacy statements; User agreements; Consent; Privacy and Consent Technology.

NSPW'10, September 21–23, 2010, Concord, Massachusetts, USA.

1. INTRODUCTION
In today's Internet culture where many service providers interact with their service users through on-line services, it is these organisations and their users which have become some of the key participants in the on-line privacy debate. Privacy is a subject which matters to the majority of Internet users [7, 13]. Internet users (service users) use on-line services provided by various organizations, including governments, academic institutions, commercial organizations or on-line social networking companies (service providers). Increasingly, for many service providers, the Internet is becoming the sole method of service delivery.

There are many definitions of privacy but, in the context of on-line services, perhaps privacy is most intuitively regarded as the ability a service user (or data 'subject') has to control the disclosure of personal information and the presentation of their on-line identity. This view of privacy refers to the privacy dimensions described in Westin's often-quoted definition of privacy: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [21]. When discussing the management of privacy [33], much is made of the management of personal data, along with a service provider's operational practices, processes and procedures for personal data handling. In this context, privacy management is often regarded as the processes for personal data handling. Privacy management approaches often regard privacy as a data handling issue. Privacy management can be predicated on the notion that service users have a constant view of privacy. In this view, the expectation is that privacy conflicts and dilemmas are resolved prior to the service user engaging with the on-line service and in the case of communal services rely on face to face dialogue for a resolution [6].

However, privacy is a multi-faceted and socially constructed concept, which researchers sometimes refer to as "elastic" [22]. This elasticity is influenced by cultural and social factors as well as technological factors [12]. This results in shifting requirements, an on-going need to express privacy concerns, conflicting interpretations of privacy, and the need to negotiate a joint privacy response by both service provider and service user. Such dilemmas can be resolved through dialogue and negotiation.

Today, where such privacy and consent dialogues take place, they take place off-line [6], often at the macro level within the community and at the societal level in general. However, our

exploratory research indicates that in an increasingly on-line delivery of services, there are points in a relationship between a service user and an on-line service provider where micro dialogues are necessary in order to help service users make decisions on privacy practices. As the resource to support communal services decreases, there becomes a greater reliance on on-line negotiation. From our study we can see that the design of on-line services does not allow for dialogue or negotiation within the on-line service itself; instead, each party is forced to present their stance as non-negotiable. This results in an unsatisfactory resolution of privacy dilemmas where on-line service users feel that they have to trade their privacy for the benefits of on-line services, and service providers are required to provide and support privacy functionality that has little value to the service user. This situation will only deteriorate as the shift towards the Internet as a sole method of delivery accelerates.

1.1 The Case for Privacy Dialogues

Privacy research has revealed privacy dilemmas for both service users and service providers. Research that has been used to measure and classify privacy concerns [7, 9, 10, 11, 12] often reflects privacy concern on the one hand but a willingness to disclose personal information and not engage in privacy protection practices on the other hand. As part of the Visualisation and Other Methods of Expression (VOME) project, an on-line survey [8] was conducted to gather information on users' perception of Internet and privacy issues.[1] The purpose of the survey was to contribute to the development of a baseline of privacy attitudes, beliefs and practices using tools traditionally used to measure on-line privacy. By using existing measurement scales, the findings from the VOME survey could be compared with previous surveys on this topic. 1048 respondents completed the survey. A number of results emerged from this survey which is sometimes termed "privacy paradox". Privacy paradoxes are discussed in the literature [26, 27, 30] and the following were identified through the VOME survey:

- Users are concerned about their privacy, but are unwilling to engage with privacy technologies. This is in line with the findings discussed in Buchanan et al.'s work [30].
- Users want autonomy over on-line privacy but are prepared to trade their privacy in return for some reward. This is in-line with the paradoxes discussed in Buchanan et al.'s work [27].

1.1.1 Concerned but Unwilling to Engage with Privacy Technologies

Coles-Kemp et al. [8] also analysed the privacy practice aspects of General Caution and Technical Protection, and then compared those practices with the privacy stances of the survey respondents. Buchanan et al. [30] developed and validated Internet-administered scales measuring privacy-related attitudes and behaviours. In the case of privacy-related practices, they identified two distinct groups of actions people may take to protect their on-line privacy. The first group is classified as General Caution and contains common sense steps that people take. The second group, known as Technical Protection of privacy, requires a specific level of technical competency and involves sophisticated use of hardware and software as tools for safeguarding privacy. While everyone can engage to some extent in General Caution to protect their on-line privacy, a higher level of technical knowledge is necessary for Technical Protection.

The survey results showed that, in terms of privacy concern, 49% (n=514) of people are somewhat concerned, with 'greater concern' shown by 27% (n=283) and less by 23% (n=242). These results are in line with the results of previous surveys. At the same time, in answering the question whether respondents use only on-line services that have a privacy policy: 41.2% responded "always", 73.1% said "most of the time", 48.4% said "sometimes", 10.6% said "hardly ever", and 5.9% said "never". Moreover the results showed that 13% (n=143) of respondents "hardly ever", and 5% (n=53) "never" read user agreements and privacy statements on-line before disclosing personal information. Analysis of the results also showed that the more experience a service user has in dealing with on-line services the less likely they are to engage with service agreements. This indicates a paradox: a concern about privacy that is not matched by the practice of using privacy statements and agreements. This type of practice is termed "general caution".

However, this paradox extended beyond the practice of general caution. The survey showed that numerous technical privacy practices were not used. For example, while females and the older service users were most concerned about on-line privacy, they were less likely to engage with methods of technical privacy protection to respond to a range of privacy risks. Technical privacy protection methods include clearing browsers, deploying spyware protection etc.

One interpretation is that this situation could be resolved by the development of more suitable protection controls. However, our pilot studies indicate that this is not so much a paradox, but a dilemma during the process of deciding the best approach to take. Further, our fieldwork shows that when faced with this indecision as to which privacy protection strategy to take, dialogue with service providers and other service users is an important method of achieving a resolution.

1.1.2 Want Autonomy but Prepared to Trade in Return for Reward

The majority of respondents agreed that "control and autonomy over the use of their data" is important and it appears that this view increases as a service user gains more experience. The survey showed that the more on-line experience a service user has the less in favour of personalized on-line services a service user becomes. In this case personalization was defined as: the adjustment and tailoring of web-services dependent on information that is collected automatically but does not identify the individual; on information that is given out voluntarily but does not identify the individual; and on information that one has given out voluntarily but does identify the individual.

[1] The purpose of the VOME project is to improve our understanding of how service users envisage and articulate privacy and consent concerns. It is hoped that an improved understanding will result in a specification for a tool box of interventions that enable richer dialogue about privacy and consent between the different stakeholders in on-line environments. With a richer dialogue, privacy and consent can be negotiated and re-negotiated as necessary.

The survey also indicated that a service user becomes more pragmatic about on-line privacy the more on-line experience a service user has. Similarly, the more on-line experience a service user has, the more a service user's trusting beliefs in the service provider decreases. These results indicate another paradox: the desire for autonomy conflicting with a sense of having to disclose personal data in order to be the recipient of the benefits of the on-line service. As with the first paradox, field work explored the trusting beliefs and the privacy practices to uncover the fact that these paradoxes are more usually the result of a dilemma as to which privacy protection strategy to choose.

1.2 Increasing Need to Resolve Dilemmas

The data gathered from the VOME survey [8] indicates that most of the respondents have used the Internet for transactional, administrative activities such as searching for information, travel reservations and on-line banking. Furthermore, 84% (n=880) of respondents said they use the Internet for purchasing. These transactional services are relatively straightforward in terms of the relationship between the service user and service provider. Yet, as the results of the survey demonstrate, even in this relatively simple relationship the service users do not use the mechanisms for privacy management and protection, while still wishing to retain control. To complicate matters still further, a new generation of services requiring much more complex privacy and consent decisions is emerging as the shift is made to deliver public services on-line [6].

In a case study conducted by Bogdanovic et al. [6], there was an exploration of the deployment of an on-line public service. Analysis of the project documentation and interviews with the service providers concluded that this type of on-line public service had a more complex consent negotiation process. This type of on-line public service also required more complex privacy and consent decisions to be made, resulting in dilemmas as to which privacy protection strategy the service users should use. It was identified that, to date, no tools have been developed so that this negotiation could be resolved using existing on-line technologies.

2. Current Research in on-line Privacy and Consent

Privacy regulations in the USA, the EU, Canada and Australia provide laws to protect privacy of personal information. For example, the Communication Act of 1934 in the USA mandated that customer proprietary information can only be used for the services requested by the customer [13]. A dialogue system between service users and service providers enables an understanding of privacy to be agreed upon and also to be adjusted as the context in which the service operates changes.

There are a number of research themes in privacy design functionality. The first theme is the increase in a service user's autonomy over the disclosure of their personal data. Church and Whitten [5] looked at security and user centred design and considered that users can be given more control over technology and information. They also suggested that users should be allowed to have more direct control over their information via end user programming. Moreover, Whitley [23] reviewed how notions of privacy and consent have been conceptualized in the literature. In this study, the author highlights the fact that very few service users read and understand the privacy statements and simply click through and accept them. Whitley believes that more control of personal data, in terms of giving and revoking consent, should be given to service users instead of service providers.

The second research theme is technologies related to the user control of their on-line identities. In order to protect users' privacy, researchers [1, 2, 3, 4] in system security are thinking about new techniques that secure and protect users' privacy from relevant attacks i.e. by producing reliable privacy statements and addressing identity systems. For example, in the field of cryptography, U-Prove technology [18] has achieved the means for providing privacy and autonomy in user authentication and data sharing systems. U-Prove technology can be used to merge multi-party security and privacy requirements in on-line communication and transaction systems. The privacy features of the U-Prove technology prevents service providers from knowing any more information than which can be inferred from the attributes that are revealed by service users.

In addition, the IDEMIX project by IBM [20] is working to protect users' privacy by allowing them to reveal their personal data in as minimal a way as possible. Hence the IDEMIX system uses an artificial name, a pseudonym, for users to choose and register with an on-line service. A user can obtain a credential from an issuing organization and then show the credential to a service provider. A credential is always issued to a pseudonym under which the user is registered with the issuing organization. A credential may have certain attributes. When showing a credential the user can choose which of the credential's attributes shall be revealed. The user would use the pseudonym to register and receive the corresponding credentials with an electronic signature. The pseudonym and credentials are given to a service provider only in an encrypted form. The user accesses the service by providing proof to the service provider that the corresponding digitally signed credentials are in their possession. Obtaining a credential from an issuing organization and showing it to a service provider works as follows. First, the user contacts the issuing organization and establishes a pseudonym. The issuing organization produces a credential by signing a statement containing an attribute and pseudonym. The issuing organization then sends the credential to the user. Finally, the user shows the credential to the service provider [32].

These protection technologies aim to build trust in a service by empowering users with an increased range of privacy protection options. These approaches focus on privacy protection, rather than support for privacy control selection and decision making. In order to support service users in making situated decisions about the deployment of privacy controls and exercising of privacy practices, there needs to be a dialogue between the service user and service provider which enables the service user to understand the implications of their privacy practices. As the Let's Go case study [6] shows, there are attempts to use human intermediaries to negotiate between service users and service providers but the diversity of intervention required and the cost of providing for intermediaries results in a significant cost overhead and introduces a constraint on the service's deployment.

There is some research in the area of privacy tracking and communication of privacy issues. For example, the Platform for Privacy Preferences Project (P3P), which enables service providers to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user

agents. The user agents provide an automated decision-making system. Thus, if a service user is using a web browser with P3P built in, it can automatically fetch the P3P policy for a service provider (with built in P3P policies). The web browser checks the service provider's policy against the preferences the user has given. If the policy is acceptable to the user the page will be displayed, otherwise a pop-up message will appear on the screen to inform the user that the privacy policy does not match her preferences. Hence, a service user need not read the privacy policies at every site they visit [14]. P3P is a good example of a dialogue system which attempts to avoid a breach of users' privacy. However, in this system users need to change their privacy settings each time they visit an on-line service with a policy which is incompatible with the user's privacy preferences. Therefore, there is no room for service users to contest privacy levels, to raise queries about the handling of their personal data, or to renegotiate the level of privacy. The lack of an informational interface and a lack of understanding as to where P3P relates to the privacy stance of service users have resulted in a low uptake of P3P functionality [17].

There is a third theme of privacy and consent research: the reporting and communication of privacy risks to the service user, and communication of the privacy stance of the service provider. This third stream of research moves us closer towards the notion of privacy dialogues. At the PrivacyOS conference in Oxford this year, the Privacy and Identity Management for Community Services (PICOS) project [16] introduced a tested and evaluated a mobile communication service prototype which uses a location identifier system. 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. One of the aims of the PICOS approach to trustworthy on-line community collaboration is to address this question: Which supporting services and infrastructures do the stakeholders need?

In the same vein, Clique is a privacy enhanced social networking site which was developed as part of the EU FP7 PrimeLife project and launched in February 2010. The creation or modification of any information on Clique results in the posting of information, and requires the user to press the "publish" button. Subsequently a 'save information dialogue' will be displayed on screen. This function prompts users to change the privacy settings and hence users can choose who can see this new information before it is published on the site [19].

Therefore, it can be seen that in current privacy research 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 support the forming of dialogues which enable both parties to respond to each other's concerns. The need for such dialogues has long been recognized in customer relationship management (CRM) as a way of building trust between service user and service provider, and enhancing customer satisfaction [24, 28]. While the privacy literature recognizes that privacy is often an important factor in customer satisfaction [29], privacy is treated more as a statement than a dialogue and negotiation. Hence, in order to enable service users to resolve privacy dilemmas and make effective choices in their deployment of privacy protection practices, a fuller privacy dialogue in line with CRM dialogue design principles is required.

3. PILOT STUDIES

In order to explore the potential decision making strategies for privacy control selections in more detail, we conducted two pilot studies to explore the need for dialogue from a service user perspective. We then conducted five interviews with different service providers in order to explore their perspective. In selecting an appropriate research approach, the following research assumptions were made:

- There is a need to elicit service providers' and service users' needs and requirements for dialogue systems in terms of privacy and consent.
- There is a need to understand how service users interact with current on-line services.
- Service user privacy practices and beliefs are influenced by a wide range of factors including: age, culture, education, use of the Internet, on-line experiences.
- There is a need to develop tools that enable the service user to gain greater control and autonomy over the selection of privacy controls and practices.
- Service users' perceptions and views will lead to the identification of issues/factors in current privacy and consent dialogues which need to be improved.
- In order to develop dialogues, the privacy communications that service providers want to make and receive need to identified.

We are using a mixed methods approach which compares with previous studies [8, 10, 12] where data was analysed using a solely quantitative approach. In our approach we used qualitative research methods to tease out the dialogue themes and understand their relationship to each other; quantitative methods to observe certain patterns of variables in on-line service privacy practice and perceptions. We used the following research methods in order to tease out where there is a need for privacy and consent between service users and service providers:

- Group interviews with service users who worked closely with on-line services on a daily basis.
- Interactive story in a public forum.
- Service provider interviews.

By using a combination of research methods we were able to draw out the different dimensions of privacy dialogues, the ways they are currently enacted today, and to understand the different roles such dialogues might play.

3.1 Service Users

3.1.1 First Pilot Study - CHYP Focus Group

The first pilot study was a focus group which ran with 8 participants (4 female and 4 male) and was hosted by on-line service developer Consult Hyperion (CHYP). The director of CHYP and his assistant (the moderator of our focus group discussion), who are our privacy specialists collaborating with this project, helped us to recruit these participants. The aim of this study was to learn more from a group of users who work closely with various service providers in their daily activities.

The topic of the discussion was "Privacy dialogue between Service Users and Service Providers." There was a short presentation given by the moderator followed by asking an open question on whether participants feel comfortable registering with on-line services. The group started their discussion by sharing their experiences with on-line registrations for various websites. The discussions were recorded and the researcher present in the room took notes. All the participants had registered their details with an on-line service provider for various reasons including on-line shopping and social networking. The group agreed that they hardly ever read on-line privacy statements. Moreover, on the topic of trust, one member of the group stated that the government cannot be trusted to legitimize reliable service providers. However, another participant disagreed and declared that he would trust recommended service providers from the government websites.

The outcome of the focus group was a list of possible interactions that might take place on-line between service users and service providers:

- The service provider should clearly specify with whom (which organizations) they share users' personal information and the relevance of that information sharing.
- Providing personal information should be optional for service users.
- There should be a grading system where users can decide how much information they want to reveal in order to get further service.
- The service provider should pay service users for obtaining their personal information. For example, they can offer sale discounts, or vouchers. The service users should be informed in advance that, by providing their personal information, they can receive gifts from the service provider.
- Little-known service providers should provide users' review (feedback) page to their new users. This page should give other users' opinions about the service provider in order to gain new users' trust.

It was noticeable that while this group talked from the perspective of a service user, privacy disclosure was in some senses being considered as a transaction which is a service provider perspective. However, there was also the recognition that, as a service user, you want to be able to make informed disclosure choices and be given a realistic choice in how much personal information you disclose. The conclusions of this focus group reflect the need for the following types of dialogue system: a) informational dialogue and b) raising privacy issues and queries. It is noticeable that the conclusions portray service users as being active users of a dialogue system and not simply passively receiving information.

3.1.2 Second Pilot Study - Festival of Social Science (FSS) in Sunderland

In order to explore further what we learned from the first pilot group, we aimed at a larger group in our second pilot study. This group was recruited through the Sunderland City Council's Citizen Panel. VOME was awarded a bursary to present its work in the Festival of Social Science (FSS) which is a nation-wide programme sponsored by the Economic and Social Science Research Council. The purpose of VOME's FSS event in Sunderland (UK) was to facilitate the general public in privacy and consent debate. 47 members of the public, representing a broad age range, showed their interest and participated in our discussion after a short performance (physical theatre)[2] on the topic, where they were asked to respond to the following questions:

Q1. Do you think you have enough options to negotiate the level of privacy in an on-line service that is right for you?

Q2. What do you think is the biggest risk in revealing your personal information on Internet?

Q3. How often do you read user agreements and privacy statements before disclosing your personal information for registration to use an on-line service?

Q4. In order to use an on-line service, do you think you should be able to negotiate the level of consent you give before registration?

Q5. Do you prefer to use a well-known high street brand when you purchase a product on-line?

Q6. Will you trust a little known service provider, with whom you have already engaged to protect you personal information?

These questions were developed to relate to the privacy dilemmas that emerged from the survey and in the previous pilot study. "Engagement" covers any form of service user on-line interaction with the service and includes registration, purchasing and browsing.

Figure 1 (in Appendix) shows the responses to questions Q1, Q4 and Q6, where not all participants responded. Hence, of those who did: 51% (n=24) of users disagreed that there are enough options to negotiate the level of privacy in on-line services (Q1). The same number of users said they should be able to negotiate the level of their consent before registering with any on-line services (Q4). Hence, there are a proportion of participants in favour of having a privacy dialogue system. Furthermore, only 46.5% (n=20) of respondents from this group said they would trust a little known service provider with their personal information (Q6). This also shows in their responses to Q5, where the majority of participants said that they preferred to use a well-known high street brand when they purchase a product on-line (Appendix, Figure 2). However, the open discussion that took place after the privacy theatre showed that regardless of the reliance on brand, service users still would like to raise privacy issues and seek further assurance.

On the same subject of trust, we wanted to know why users might hesitate registering with on-line services, or if they do, in their opinion what risk do they think that they might have taken. In responding to Q2, Figure 3 (Appendix) shows that from the three options given, 42.6% (n=20) of participants said the biggest risk

[2] The piece of theatre was developed from the results of the survey, privacy stories in the media and the results of qualitative fieldwork conducted by some of the VOME teams in the first year of the project.

in revealing their personal information on the Internet is identity theft; 29.8% (n=14) said bank theft and 21.3% (n=10) said breach of privacy. This may suggest users are concerned about their identity being stolen when disclosing their personal information and therefore they would feel uncomfortable using little-known service providers. This indicates that different types of privacy concerns arise when using service providers with different brand statuses. In some instances, providing further clarification and support for the selection of privacy practices, in the form of a dialogue system, might resolve some of these concerns.

Moreover, similar to the previous group, the majority of respondents (n=21) which is shown in Figure 4 (Appendix), said they 'hardly ever' read user agreements and privacy statements (Q3). This again indicates that there is a need for a dialogue system relating specifically to consent and it is necessary to change the way privacy and consent is negotiated between service users and service providers.

After a break, 21 of the 47 participants elected to continue in the study. They responded to the following questions:

Q7. What do you think is the best way for the service provider to communicate with you to gain your trust?

Q8. Why do you trust a well-known brand with your personal information?

Q9. How do you want to communicate with an on-line service provider to give them your consent?

Q10. Do you think reading service providers' user agreements and privacy statements on-line is enough for you to trust them with your personal information?

85.7% (n=18) of participants chose from the four options (Q7) in order to indicate which is the best way for the service provider to communicate with them (Appendix, Figure 5). As the results show, there was an almost even spread of preferred communication methods. Hence, providing a means of communicating with service representatives on-line; providing a privacy policy that guarantees the security of their personal information; and providing contact details (telephone and address) were almost equally acceptable to this group.

Furthermore, 57.1% (n=12) of participants would prefer to speak to a representative on the phone to give them their consent (Q9). However, 19.1% (n=4) chose sending their consent via email and only 14.3% (n=3) said they would read the user agreement and privacy statements on-line (Appendix, Figure 6). This again confirms the fact that users often do not engage with on-line user agreements and privacy statements. This result also indicates that users are more comfortable giving their consent when there is a dialogue between them and the service provider. Figure 7 (Appendix) shows that when 57.1% (n=12) of participants disagreed that reading service providers' user agreements and privacy statements on-line is enough for them to trust service providers with their personal information (Q10). They believe service providers should provide more services to assure them that their personal information is safe.

Surprisingly, although we learned that participants have more faith in well-known brands (Appendix, Figures 1 and 2), 33% (n=7) of this group declared they 'don't trust them' with their personal information (Q8). 38% (n=8) would trust them because 'they are professional and therefore will not breach their privacy' and smaller number (19.05%, n=4) of participants declared their trust is based on other peoples' experience in the past (Appendix, Figure 8).

The findings from this study show that information systems and dialogue systems that can be used to raise issues and concerns are both systems that service users would like to use. It could also be argued that where service users are not sufficiently assured, a system for contesting the service provider's privacy stance needs to be provided. These results also indicate that a range of configurable dialogues is needed, depending on the privacy stance, Internet experience, and privacy perceptions of the service user. Some service users would like feedback and recommendations from other service users, some service users would like to contest the privacy stance of the service provider, and some service users would like further information from the service provider.

3.2 Service Providers

As a first step to understanding what sorts of privacy negotiation and privacy dialogues service providers might need, semi-structured interviews were used to explore the organizational processes deployed for managing privacy.

Five interviews were conducted. Each interviewee was an employee selected from a different organisation. Each of the five interviewees was responsible for managing an on-line service and, as part of that role, responsible for managing an aspect of customer privacy. The organizations from which the interviewees were selected all had the following general characteristics:

- The on-line services provided contained a combination of transactional services, used for purchasing, and services for making contacts and developing relationships (for example messaging services or blogging services)
- Multiple on-line services with different privacy requirements delivered from one technological architecture (in order to explore how organizations supported the different privacy requirements and adjusted their management processes accordingly)
- All on-line services delivered to UK (not overseas) communities

The service providers came from two distinct groups:

- Service providers who deliver traditional on-line transactional e-business services. These providers are in the private sector. (2)
- Service providers who are beginning the process of delivering on-line public services. These providers are in the public sector. (3)

3.2.1 Methodology

As stated above, five interviewees volunteered from five different organizations. The interviewees were responsible both for the delivery of the on-line service and the management of service user privacy. The interviews were semi-structured. The structured questions were as follows:

- Please briefly explain the role of the Internet in delivering your organization's business services.

- Please briefly outline who are the users of any on-line services.
- Please briefly outline the aspects of customer privacy that you address in your on-line services.
- As a policy, are on-line service users' privacy requirements gathered when developing an on-line service?
- As a policy, when one of your on-line services collects personal data, is the on-line service user given a choice as to whether or not they disclose it to you?
- Do you receive on-line service user queries and complaints about the kind of personal data you ask them for? (If so, what mechanism is used for raising and responding to queries and complaints? Can you give examples of the types of queries or complaints that arise?)

The open, discursive questions were as follows:

- What mechanisms do you use to protect your service users' privacy?
- Do your service users raise privacy concerns? If so, what types of concerns are raised?

The latter two questions were more discursive in the sense that the researcher raised neutral responses to the answers given in order to promote reflection and deeper answers.

The same questions were asked of each interviewee, but each was also allowed to expand on the areas of interest. At the end of each session, conclusions and reflections were discussed and agreed. At each interview, two researchers were present.

3.2.2 Results

Two aspects to privacy management emerged: regulatory compliance and a dimension to the customer relationship management process. The customer relationship management process emerged in the responses to questions about queries and raising complaints, and also in the reflective responses regarding privacy concerns. CRM literature [28, 29] cites privacy as a determinant in customer satisfaction but does not present the need for privacy dialogues, more the need for privacy protection. However, the results from these interviews indicate that as privacy concerns arise, service users wish to communicate with service providers about these issues. Also, service providers show a willingness to modify service content in order to reduce the likelihood of privacy complaints.

3.2.2.1 Regulation

When asked how privacy requirements are generated, all service providers cited privacy legislation (in particular the Data Protection Act 1988) as a key input into privacy policy and procedures. For all the service providers interviewed, the UK data loss incidents reported in the media were cited as motivation for developing privacy management, and as a cause of service user privacy concerns and queries. The regulatory response took the form of revisiting data handling policies, revisiting audit schedules, review of roles and responsibilities for personal data handling, and revising how the regulatory messages were communicated. There was also an increased level of interaction with assurance bodies, and a greater level of regulation.

Therefore, for the service providers the emphasis was on revisiting regulation and strengthening the communication of the regulatory messages, making privacy very firmly a regulatory and compliance issue. Only one service provider considered cultural change as a significant response.

3.2.2.2 Customer Relationship Management

The results show that, in privacy management, there is a very specific strand of business input which was continuously emphasized in all the interviews, namely service user expectations and the management of their personal information. All interviewees cited service user expectations but did so in different ways. The public sector organizations were more inclined to use their knowledge of the communities they represented to form their view of customer expectation. In each case, assumptions were made about personal information disclosure and the rights of access, rather than using a process of dialogue for understanding service users' expectations in this area.

The commercial service providers based their view of customer expectation on the privacy concerns and queries that were raised. In all cases, the process for requirements gathering did not include direct engagement with the service users. These service providers talked about customer feedback and service-user expectations in terms of privacy services such as anonymity and link-ability. However, they also considered service user privacy expectations in terms of the amount and type of marketing contact the service users experienced. There was also awareness with both commercial service providers that service user privacy expectations change. There was no on-going communication about expectations; instead, expectations were understood from complaints and concerns about quality of service. This latter point is surprising.

The literature cites that privacy is an important determinant for satisfaction in on-line services [29] and customer dialogue is an important factor in obtaining high customer satisfaction [28]. Yet mechanisms for privacy dialogue as part of the on-line service do not yet exist. Instead, the focus is primarily on privacy protection and notification of good practice. This implies that design principles for privacy dialogue systems need to recognize general CRM dialogue design principles such as: frequency, initiation, signalling, service provider disclosure and richness [25]. It also implies that privacy-specific issues should also be included in the dialogue design principles. Privacy-specific principles include: transparency, service user disclosure and agreement on privacy norms and rules.

The individuality of the service user's pattern of privacy beliefs and practices did not emerge as part of the interviews with the public service providers. One possible reason for this is that the on-line public services were deployed using a large amount of off-line engagement, and the personalization of privacy preferences took place as part of this off-line engagement.

4. DISCUSSION AND CONCLUSION

4.1 Key Findings

In our study we were able to find what various groups of service users thought with regards to current privacy and consent functionality provided by on-line service providers. Comments given by service users in our studies have underlined the importance of understanding the shifting nature of users' privacy perceptions when designing privacy and consent technologies that users will engage with. Users from all groups confirmed that they avoid reading privacy statements and user agreements. Worryingly, privacy statements and user agreements are the only

current option for privacy and consent dialogue that exists in most on-line services.

Another key finding has to do with the importance of informing users of how their details are used. The service users who participated in our study suggested that a privacy dialogue system must include a range of methods for communicating with service representatives; for providing feedback on the implications of a privacy policy, and for communicating the methods of protection for contact details (telephone and address). Participants showed a strong desire to have more information on why their personal information is needed and to be able to contest that need.

Service users are clear that they want feedback on the privacy and consent management of on-line services from a variety of sources: from a third party, from the service provider themselves and from other service users. The service users also demonstrated that they did not want a system that treated them as passive actors in the management of privacy and consent in on-line transactions. The service users clearly articulated the need for dialogue as opposed to a service provider monologue. As a result, service users showed a strong desire for three types of dialogue system: 1) a system to request information, 2) a system to query and raise issues and to seek assurances and 3) a dialogue system to contest the professed privacy stance of service providers.

Furthermore, from the service providers' interviews, three types of dialogue also emerge:

1. A dialogue to understand a service user's privacy patterns and behaviours, along with the associated personalization requirements. Rather than on-going requirement gathering, this is more a question of identifying privacy expectations as they emerge. Today, the results of our interviews indicate that this is handled as part of customer relationship management as exceptions. This has the potential to lead to dissatisfied service users and an inefficient resolution process.
2. A dialogue to understand service users' privacy concerns and respond to them. Again, today this is handled in an inefficient manner outside of the on-line service delivery.
3. In the more complex services, a dialogue is needed to determine the appropriate level of service user autonomy. These services also require dialogue to decide when the control over privacy and consent lies with the service user, and when the service provider needs to intervene and override the privacy and consent levels. This is a need that emerges with the rise of on-line public service delivery.

It was noticeable that in the regulatory view of privacy, none of the service providers interviewed felt a need to negotiate privacy levels with service users. The perception was that this dialogue happens through the legislative process. Instead, the need for dialogues emerged as part of the customer relationship management process.

The difference in nature between the commercial services and public services were clearly reflected in the service provider dialogue needs. Public services are often more complex. The more complex and multi-faceted the service, the more negotiation was necessary. Complexity increases when services are delivered for multiple purposes. Multiple purposes include when a combination of transactional and discursive communications are used to deliver the on-line services. Complexity is increased when the off-line version of the service has a lengthy process for establishing trust and confidence.

Currently, we are recruiting participants to further understand the types of privacy practices that are used and the requirements needed to develop tools to facilitate more effective selection of privacy practices.

4.2 Implications for Privacy and Consent Functionality Design

These findings deepen our understanding of general caution behaviour and the role that dialogues might play in supporting a service user's selection of privacy protection practices. From both the pilot studies with service users and the interviews with service providers, it is clear that, where privacy dialogues take place, they primarily take place off-line. Results from both the work with service providers and service users indicate that on-line privacy is part of the relationship (both on and off-line) that service users have with service providers. This is in-line with Solove's [31] view of privacy as a dimension of relationships. By working with service users in a variety of settings, it became clear that privacy and consent management is not segregated into on- and off-line worlds. It also became clear that service providers manage privacy as a technological issue. Although they are aware of the relationship between privacy and customer relationship management, they do not design on-line systems to include privacy and consent dialogue tools and neither do they design off-line CRM processes to facilitate privacy and consent dialogue.

Giving consideration to the building of privacy dialogues at the service user –to- service provider relationship level, as well as at the technological (hardware and software) levels, requires the development of privacy dialogue design principles. The focus on the relationship building results in a socio-technical design which recognizes that all technology design can be analysed, and therefore constructed, from a social perspective [24], and which recognizes that privacy is not a separate off-line or on-line concept but an integral part of relationship building. As a result, a socio-technical design for privacy management should consider the design of privacy dialogues as part of the design of on-line services. Such a system of dialogue contains elements in the on-line and off-line worlds, including: a) configurable options for dialogues; b) a tighter integration of on-line services and the organizational processes that support them; c) the design of supporting organizational processes as part of the on-line service design.

As part of the design, consideration needs to be given to how privacy and consent issues can be raised and responded to. As part of the response, the frequency of privacy messages and the richness of privacy messages need to be identified. Furthermore, the norms relating to service users and service providers when they contest each other's privacy stance needs definition. In addition, the mechanisms for communicating and responding to contestations need to be designed.

However, providing such a dialogue system has potentially negative side-effects for privacy and consent management. If service users and service providers know more about each others' privacy stance and behaviours, it is possible that this knowledge may be used to manipulate behaviours. For example, knowing

that a service user has a particular stance may result in certain inferences being made about their political or social values. It may also make it possible to co-ordinate service user feedback on the privacy and consent functionality of a service, resulting in a service provider's ability to manipulate service user privacy perceptions en-masse; or from the service user side to conduct "mobbing" type activities against a service provider. These are all examples of possible "revenge" or unpredictable side-effects of privacy dialogue systems. As a result the "patching" of a socio-technical system for privacy management may also include defences against behavioural attacks as well as technological attacks.

Designing such socio-technical systems would also require an adaptation of existing system modelling techniques, so that assessments can be carried out on how adjustments to the system in changes to expected privacy and consent behaviours. Such modelling might indicate if it is possible in a socio-technical system to adjust technological privacy practices by adjusting some of the social elements in the system.

A socio-technical perspective on privacy and consent management allows for a much richer set of responses to privacy dilemmas. At the same time it offers a better means of integration between the technological and social elements of a privacy management system, and a more effective means of resolving the privacy dilemmas faced by both service users and service providers.

5. ACKNOWLEDGMENTS

We are grateful to all 58 participants who took part in this study.

Many thanks must go to Robin Wilton for his contribution to the references for Privacy-enhancing Technologies.

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].

6. REFERENCES

[1] Probst, C.W and Hansen, R. R. 2009. Fluid Information Systems. In Proceedings of New Security Paradigms Workshop. http://www.nspw.org/proceedings/2009

[2] Laurie, B. and Singer, A. 2009. Choose the Red Pill and the Blue Pill. In Proceedings of New Security Paradigms Workshop. http://www.nspw.org/proceedings/2009

[3] Turpe, S., 2009. What is the Shape of Your Security Policy? Security as a Classification Problem. In Proceedings of New Security Paradigms Workshop. http://www.nspw.org/proceedings/2009

[4] Shirley, J. and Evans, D. 2009. The User is Not the Enemy: Fighting Malware by Tracking User Intentions. In Proceedings of New Security Paradigms Workshop. http://www.nspw.org/proceedings/2009

[5] Church, L. and Whitten, A. 2009. Generative Usability: Security and User Centered Design beyond the Appliance. In Proceedings of New Security Paradigms Workshop. http://www.nspw.org/proceedings/2009

[6] Bogdanovic, D. Crawford, C. and Coles-Kemp, L. 2009. The need for enhanced privacy and consent dialogues. Information Security Technical Report, 14(3), p (167-172).

[7] Langheinrich, M. 2002. A Privacy Awareness System for Ubiquitous Computing Environments. Ubiquitous Computing , 315-320, Springer.

[8] Coles-Kemp, L. Lai, Y. Ford, M. 2009. Privacy: Contemporary Developments in Users' Attitudes and Behaviours. http://www.vome.org.uk/index.php/publications/

[9] Teltzrow, M. and Kobsa, A. 2004. Impacts of User Privacy Preferences on Personalised Systems. Designing personalised user experiences in eCommerce. Springer, p (315-332).

[10] Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., Carter, C. 2000. Trust and Privacy Online: Why Americans Wants to Rewrite the Rules. The Pew Internet & American Life Project. http://www.pewinternet.org

[11] Bennett, L. 2009. Reflections on Privacy, Identity and Consent in Online Services. Information Security Technical Report, 14(3), p (119-123).

[12] Smith, H., Milberg, S., Bruke, S. 1996. Information Privacy: Measuring individuals' concerns about organisational practices. MIS Quart. 20(2), p (167-196).

[13] Malik, N.A. and Tomlinson, A. 2009. Privacy and Consent in Pervasive Networks. Information Security Technical Report, 14(3), p (138-142).

[14] W3C. 2010. Platform for Privacy Preferences, Technology and Society domain. http://www.w3.org/P3P

[15] PrivacyOS Conference, 12th and 13th April 2010, Oxford, UK. https://www.privacyos.eu/

[16] Privacy and Identity Management for Community Services. http://www.picos-project.eu

[17] Jensen, C. Potts, C. Jensen, C. Privacy practices of Internet Users: Self-reports Versus Observed Behaviour. 2005. International Journal of Human-Computer Studies. 63(1-2), p (203-227).

[18] Brands, S. 2010. U-Prove Technology Overview. Microsoft Corporation. https://connect.microsoft.com

[19] Clique.2010.Privacy. http://clique.primelife.eu/pg/expages/read/Privacy

[20] IDEMIX. http://www.zurich.ibm.com/pri/projects/idemix.html

[21] Westin, A.F. 1967. Privacy and Freedom. New York, Atheneum, p (xvi).

[22] Allen, A.L. 1988. Uneasy access: Privacy for women in a free society. Totowa, NJ: Rowman & Littlefield.

[23] Whitley, E.A. 2009. Informational Privacy, Consent and the "Control" of Personal Data. Information Security Technical Report, 14(3), p (154-159).

[24] Barley, S.R. 1988. Technology, power, and the social organization of work: Towards a paradigmatic theory of skilling and deskilling. Research in the Sociology of Organizations, 6, p (33-60).

[25] Leuthersser, l., Kohli, A, K. 1995. Relational Behaviour in Business Markets – Implications for Relationship Management, Journal of Business Research 34, pp. 221-233

[26] Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users'perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536.

[27] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs,41*(1), 100-126.

[28] Bruhn M., Grund M. (2000) Theory, Development and Implementation of National Customer Satisfaction Indices: the Swiss Index of Customer Satisfaction (SWICS) *Total Quality Management, Volume 11, Number 7*

[29] Horn D., Feinberg R., Salvendy, G.(2005) Determinant Elements of Customer Relationshjp Management in e-Business. Behaviour and Information Technology Volume 24, Number 2

[30] Buchanan, Tom, Ulf-Dietrich Reips, Carina Paine and Adam N. Joinson, (2007) "Development of measures of on-line privacy concern and protection for use on the Internet." Journal of the American Society for Information Science and Technology, Vol. 58, Issue 2, pp. 157 – 165

[31] Solove, D.J., 2008. Understanding Privacy. Harvard.

[32] Camenisch, J. & Van Herreweghen, E., 2002, Design and implementation of the idemix anonymous credential system, Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, pp. 30.

[33] Information Commissioner's Office (2008) "Privacy by Design" available from: http://www.ico.gov.uk/upload/documents/pdb_report_html/index.html (last accessed 5th August 2010)

7. APPENDIX

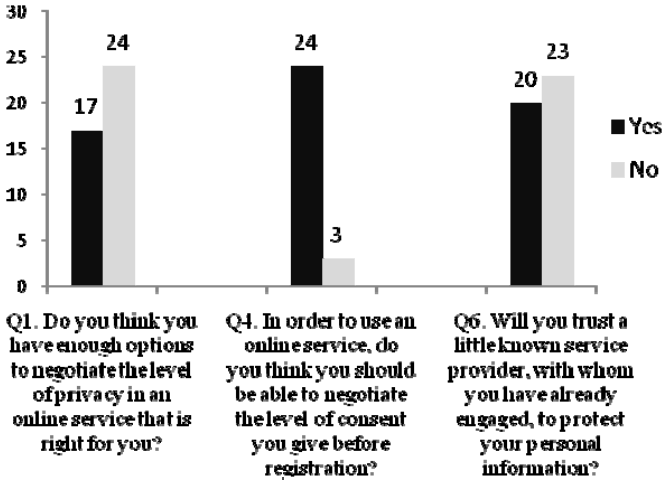

Figure 1. Responses to FSS questions Q1, Q4, and Q6

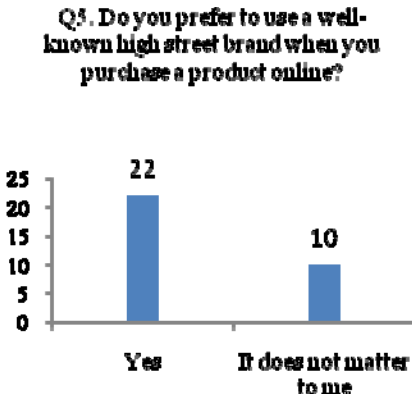

Figure 2. Responses to FSS question Q5

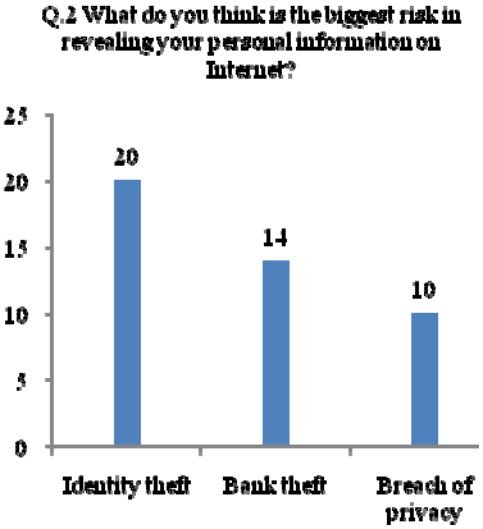

Figure 3. Responses to FSS question Q2

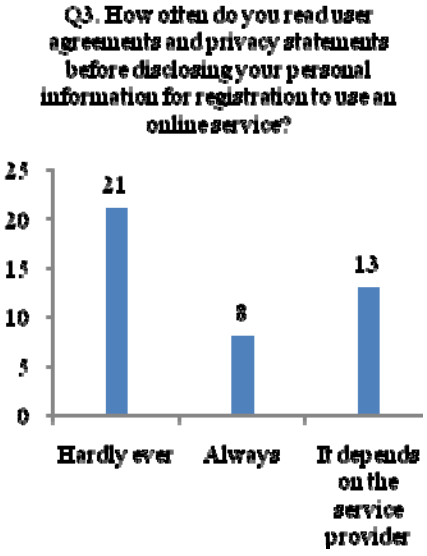

Figure 4. Responses to FSS question Q3

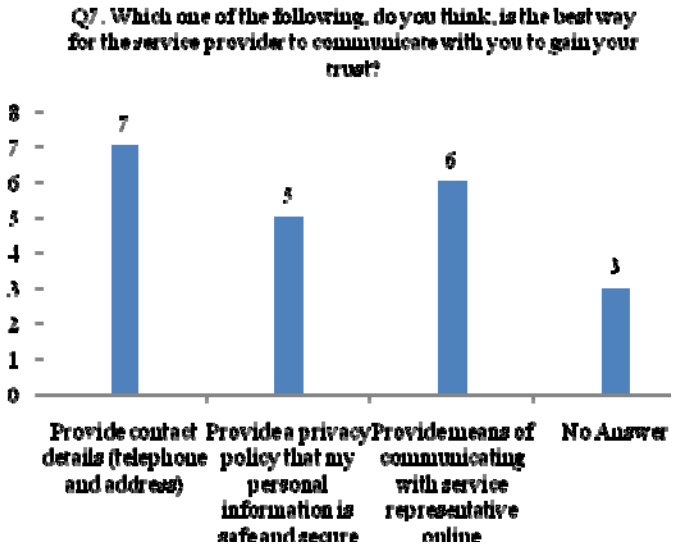

Figure 5. Responses to FSS question Q7

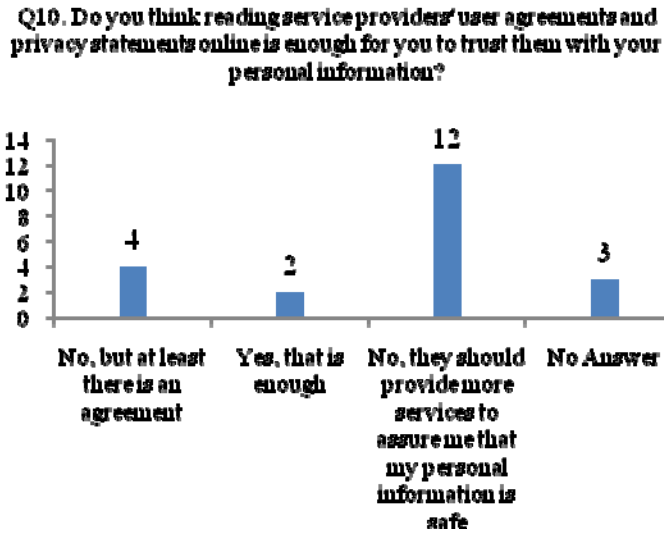

Figure 7. Responses to FSS question Q10

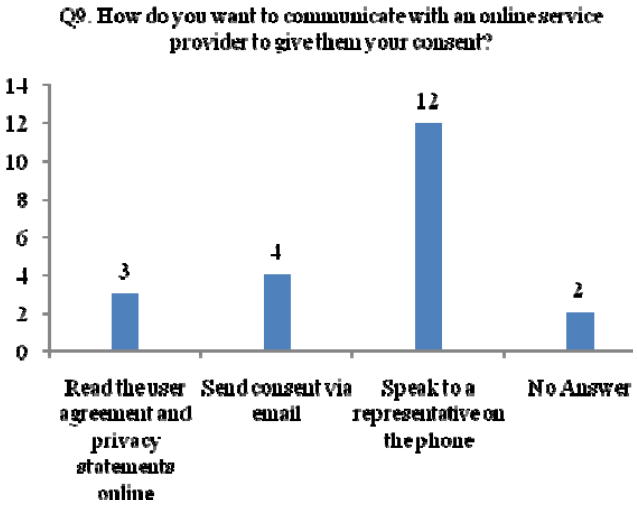

Figure 6. Responses to FSS question Q9

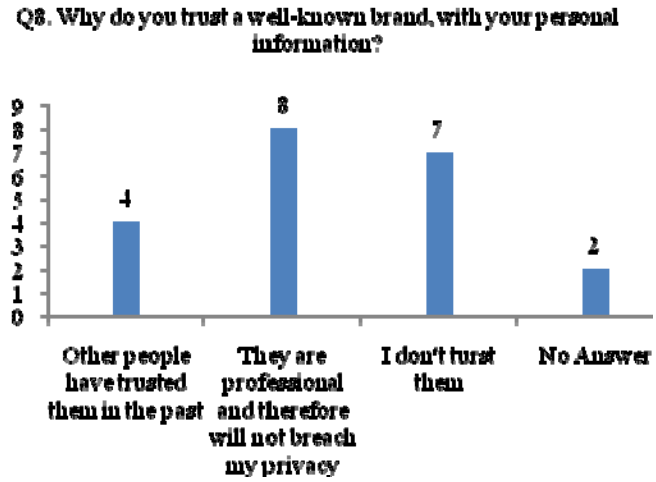

Figure 8. Responses to FSS question Q8