Practice Makes Perfect

Motivating confident privacy protection practices

Lizzie Coles-Kemp

Information Security Group
Royal Holloway, University of London
Egham, United Kingdom
lizzie.coles-kemp@rhul.ac.uk

Elahe Kani-Zabihi

Information Security Group
Royal Holloway, University of London
Egham, United Kingdom
elahe.kani@rhul.ac.uk

Abstract— **The study presented in this paper shows that service users can have low confidence in a service provider's ability to protect their personal information even if those service users trust the overall brand. Today, on-line services are not specifically designed to promote a service user's confidence building. As a result, service users have to depend on off-line techniques to build confidence in their information practices. One implication of not having effective support for confidence building designed into the on-line service is that, despite costly investment in trust marks, security technologies and brand development, service users will continue to give false information, limit the extent of their engagement in on-line services and avoid registration with on-line services. In the era of on-line public services delivery, this pattern of privacy protection practice potentially has devastating consequences for public service delivery and the ability of the most vulnerable to receive the public service support that they need. The study also indicates that providing interaction possibilities through social computing as part of the service design is one way to help build service user confidence. This paper concludes with examples of social computing used for this purpose.**

Keywords - privacy; socio-technical; interaction; information practice; trust; confidence; privacy protection practice

I. INTRODUCTION

The delivery of public services in the UK has seen an expansion of the role of ICT and the deployment of the Internet, including social computing, in the delivery of public services [1]. Service providers are encouraged to create increasingly flexible, visible and collaborative value chains while directly engaging on-line users in the innovation process[2]. The expectation is that service users enter into this partnership confident with relationship building practices adapted for the on-line environment. Research indicates that this is not the case and a considerable amount of off-line support is often needed to implement on-line services across society [5]. As public service departments are required to cut budgets "digitizing" public services becomes an increasingly attractive means of reducing the costs of "face to face" communication. The result is that the "face to face" platform used to deliver public services reduces [21] and, with it, the loss of key trust building mechanisms and services used in the initiation and maintenance of service user to service provider relationships.

Sociologist Niklas Luhmann [19] differentiates between the concepts of trust, familiarity and confidence. In this sense "trust" is the decision to engage in the face of perceived risk, whereas "confidence" takes place where actions are executed under the assumption expectations will be met. This paper considers this interpretation of confidence and addresses the research question "How might on-line service design support confident decision making about when to disclose personal information to service providers?" The research presented in this paper indicates that an on-line service user must have both trust in a service provider and confidence in the technologies that a service provider uses to protect personal information and confidence in the processes and services they offer. The research also shows that typically such confidence is built off-line and as off-line opportunities for confidence building diminish, service users are faced with difficult choices as to how to protect their personal information. This paper concludes with a discussion as to how social computing may be designed into the delivery of on-line services to support this confidence building process. The problem of personal information disclosure is articulated as a privacy problem by Westin [2] "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". As the technology diversifies so too do privacy problems [3] and it is the position of this paper's authors that the delivery of services on-line adds an additional confidence problem. The work presented in this paper is part of a project entitled Visualisation and Other Methods of Expression (VOME) which uses qualitative social research [15] to ground the development of technology designed to support privacy and consent decision making. Examples of VOME technologies include a card trading game, participatory video and

---

[1] Cabinet Office (2005) Transformational Government: Enabled by Technology
www.epractice.eu/files/media/media_201.pdf

[2] http://spectrum.ieee.org/webinar/1703379

IEEE computer society

embedded on-line interaction tools, for example interactive information flow maps [3].

This paper has three main parts: a discussion of context and privacy protection research (sections II); a presentation of a user study (sections III and IV); and a discussion of confidence building technology design and conclusion (section V).

II. PREVIOUS RESEARCH IN PRIVACY PROTECTION

This section looks at the breadth of privacy protection research that has been undertaken. It identifies three main groups of privacy protection study: privacy technology, usability and accessibility studies and privacy protection practice research. Examples of such research are given below.

A. Privacy technology research

Technical protection measures include: personal data disclosure control; user management of personal privacy policies; and transparency functionality. Over the last ten years research has broadened to develop technologies that empower users to manage their personal data disclosures. This work falls into the areas of privacy policy management and transparency technologies.

1) Reducing personal data disclosure

Ardagna et. al. [4] proposed an approach to enable privacy-preserving and credential-based access control, which supports users in authenticating without revealing any personal information. U-Prove project by Microsoft [4] is an anonymous credential system for use in authentication and data sharing systems. In a similar vein, Identity Mixing (IDEMIX) project by IBM [10] is working to protect users' privacy by allowing them to reveal the minimal personal data through the use of a credential, which works as an identifier to introduce users to service providers. Another example is the Privacy-aware Secure Monitoring (PRISM) [5] project whose aim is to develop a traffic monitoring architecture that guarantees privacy preservation by avoiding disclosure of raw data even inside the controller domain itself.

2) Privacy policy management

Platform for Privacy Preferences (P3P) enables the expression of privacy preferences. It has been an influential project, despite usability issues resulting in a low uptake of P3P functionality [14]. In a development of the P3P philosophy, EU FP7 PrimeLife [6] project launched Clique, which 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[7]. Server Privacy Architecture and Capability Enablement (SPARCLE) [7] has developed the P3P philosophy in another way and enables the service

provider to identify if their policies are being enforced by service providers.

3) Transparency

Transparency technologies are designed to communicate how personal data is processed both in terms of information flows and in terms of the decision logic used. One example is the Privacy and Identity Management for Community Services (PICOS)[8] which has developed a "privacy advisor" technology used to inform users about the privacy risk at each stage when users reveal their location to other service users.

B. Accessibility and usability

It has been established in research such as [18] that technical protection measures are challenging for many users. For example, McDonald & Cranor [18] showed that many technology users have poor understanding of third party cookies and believe that their actions on-line are anonymous unless they are logged into a website. As a result, usability and accessibility has become a specific focus for some privacy research communities. It is particularly recognised that much of the language used to articulate privacy concerns and issues are rooted in legal and technical language and this language is difficult for service users to engage with. Bonneau & Preibusch [6] conducted an analysis of the market for privacy practices and policies in on-line social networks. In terms of user interfaces to technological privacy controls, they found many cases of confusing settings, ambiguous wording, and inconsistent use of terminology between sections of the same site's privacy settings. Hence, they introduced a privacy communication game to make privacy control available while hiding the privacy control interfaces. In a further development to on-line privacy communication, Cornwell et. al. [12] proposed technologies to support users with managing their security and privacy by designing simple user interfaces and visualisations for specifying and understanding policies.

C. Privacy protection practices research

Privacy protection practices are a complex set of actions that are a response to perceived privacy issues in a given situation. Dourish and Anderson [1] write about the concept of communities of information practice and how practices inform an individual's understanding of the world which, to be understood, require situated research [13]. Numerous social researchers who explore the nature of practice in ICT mediated communication concur that patterns of practice is influenced by many social factors [1, 13]. In an attempt to quantify these factors, Buchanan et. al. [9] developed and validated Internet-administered scales measuring privacy-related attitudes and behaviours, including privacy protection practices. In the case of privacy-related protection 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 to use 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. Significantly less research has taken place in general caution approaches to privacy protection than into the area of technical protection and their practices. The majority of this research is related to the use of privacy policies [6, 12].

III. USER STUDY

As the focus of both privacy technology and protection practice research shows, research into strategies for improving privacy protection practices have focused on: communication to raise awareness, simplification of the complexity of the privacy problem and usable privacy design in order to make technical protection privacy practices easier to adopt.

Despite these approaches to improving practice, the uptake of privacy protection practices is still inconsistent [9]. As a result, there have been calls for further information practice research [1, 13]. It is clear from social research [1] that there are many reasons for seemingly inconsistent practice. VOME's initial pilot studies indicated that part of the reason for inconsistent privacy practices is confusion as to which privacy issue to focus on and which privacy protection practice to select [11]. In order to explore further the nature of inconsistent practice, a user study was setup to explore privacy protection practices in a particular context. It was designed so that users could articulate the decision logic they use to carry out privacy protection in this specific context. The user study is described below.

Researchers agree that privacy is a culturally and socially situated concept [1]. We situated our user study in the context of registering for an on-line service. This context was selected because it is a scenario that many on-line service users encounter. It also placed the focus of the study on the relationship between service user and service provider. Finally, the on-line registration process is a context common to many forms of public service delivery. Research with public service providers showed that registration through social computing platforms is becoming the preferred way of delivering services. In selecting an appropriate research method, we specified six research objectives:

1. Identify points at which users reach out for support in privacy practice selection;
2. Identify users' views, expectations and desire for interaction;
3. Observe users' practices in a situated environment including privacy practices;
4. Hear their privacy practices and their views of privacy concerns;
5. Quantify their privacy practices and privacy concerns so that they can be compared;
6. Gather users' demographic information.

These objectives are not achievable with one common research method. This type of study blends research into attitudes with research of practice and requires a mixed-method approach [15]. Therefore, we combined the following research methods: structured interviews, observation, think-out-loud and questionnaire techniques. This combination enabled us to observe and hear users' privacy practices and concerns during their interaction with the on-line services. Rather than base our results on surveys which is a common method of studying users' on-line privacy concerns and practices [9], our qualitative data gathering techniques (interview, observation and think-out-loud) give participants an opportunity to reflect with researchers on the outcomes and reach an agreed interpretation of their privacy protection practices.

A. Study structure

We recruited participants from six UK online centres[9] (an organization focusing on IT training and supporting the digital inclusion of the UK public). All participants (Internet users at the centre) were recruited by the Centre Manger and were offered a shopping voucher as a reward for their contribution to the research. We were interested in a wide range of Internet users. Accordingly 56 users (36 Female and 20 Male) with a diverse range of Internet experience backgrounds participated in our study. The study was composed of three parts:

1. An on-line registration (both observed and think-out-loud);
2. The completion of a questionnaire in order to place users on the digital literacy spectrum and quantify their privacy concerns;
3. Structured interview.

For each participant the study started with a registration task, which entailed a user selecting one of five services to register with. This task was observed and using think-out-loud methods participants were encouraged to comment on their privacy protection practices as they worked through the registration process. Following the registration task, each participant completed a questionnaire. We administered a questionnaire soliciting both qualitative and quantitative data, via the use of both closed and open-ended questions. The aim of these questions was to find out how users felt about revealing their personal information; giving their consent; and whether they were satisfied with the current information given by the service provider with regards to their privacy. These questions were developed from previous studies in these areas [9, 11] and were trialled in three pilot studies [11]. Finally, the participants underwent a structured interview.

The aim of the interview questions was to explore users' views and obtain a deeper understanding of users' privacy practices. A further aim was to identify where interventions might be used to support privacy practice selection and use and what form these interventions might take.

---

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

The results of the different parts of the study were analysed and then triangulated to form a cohesive picture of: different types of privacy protection practices in use during an on-line service registration process; and where interventions might be used in the support of use.

IV. STUDY RESULTS

In analysing the data, we realised user's privacy practices[10] were affected to some extent by their privacy concerns[11]. The qualitative research in this study indicates that privacy concerns and practices are enmeshed in real life but users do not clearly link one with the other and often practices are not a clear result of concerns. In the study it was possible to identify confidence-building general caution practices and distrusting general caution practices. Each participant showed a complex pattern of practice that potentially has implications for the delivery of public services on-line. Complexity manifested itself in an intricate interplay between trust in a service provider's brand, levels of confidence in the on-line technologies and confidence in the service provider's ability to protection their personal information.

A. Confidence and trust

The results of the study show that whilst service users may have sufficient trust in a service provider's brand that despite their concerns they are willing to engage in their on-line service, they do not necessarily have confidence in the service provider's ability to protect their personal information. In an open-ended question we asked users whether they trusted the service providers with their personal information. 32 of the participants stated that they trusted the service providers they had registered with in the tasks. Common reasons given were: the service provider is a well-known organization; they had a privacy policy which was promising; and reasonable personal information was requested. Trust was partly based on the confidence that service providers would keep the service user's personal data safe. Users commented service providers should:

- Provide a secure system;
- Keep users' personal information safe, confidential and avoid sharing them with third parties without users' consent.

One user commented:

"[When using the services] I would expect to see the 'secure padlock sign' and some assurance that my personal information [is not passed] to any third party. I would prefer to see a [visible] tick box to choose whether or not I would agree with their terms and conditions".

---

[10] Example of privacy Practices: reading privacy statements; giving false personal information; trusting the service provider and any statement of data protection controls.

[11] Privacy concerns on: disclosure of personal information to third party; identity theft; revealing unnecessary sensitive data to use the service; and data being compromised by hackers.

The interview results suggest that users have confidence in security technologies and feel safer if on-line service providers are seen to be using these technologies. However, the results from the questionnaire also showed that some of those who had claimed trust in the service provider still would not disclose accurate personal data. In the interviews some participants admitted to giving false information as a means of protecting their privacy. Table I illustrates some of the unease participants feel. This reasoning was collected as part of the think-out-loud activity and triangulated with the responses to interview questions.

TABLE I.   USERS' COMMENTS FOR REVEALING PERSONAL INFORMATION IN THE INTERVIEW

User A: *"…We give them our information because otherwise we are not going to register with them. It would have been nice if didn't have to…"*
User B: *"…I don't want to give out my details but I have no choice and I get frustrated…"*
User C: *"I think [my] personal information is now held [by] all sorts of services, and I have no control over who looks at it… I was unhappy about the fact that [the service provider] required my date of birth. [My] identity is made up of several different 'pieces' of information. I might withhold my date of birth, as it is one of the least 'required' pieces and very personal, though I did not do so during this experiment".*

Therefore, confidence in the technology and trust in the brand is not always enough. Results from the interview showed that service users also have to be confident that the personal information is necessary and that the service provider will continue to protect the personal information. When there is uncertainty in either of these respects, it was observed in the study that users adopt one of several strategies:

- Give false information;
- Discontinue with registration;
- Continue with registration, give accurate information but reduce the degree of on-going service engagement.

These strategies can be interpreted as actions to reduce the relationship with the service provider. In the case of the first two actions, these strategies are executed when service users feel they have no choice but to engage with the service.

Service design comment: From a design perspective simply providing clearer information on how personal data is to be managed and why it is to be collected is unlikely to be enough. It is noticeable that participants who were unconfident about service provider practices indicated a greater desire for interaction with service providers. These participants gave examples of how they would interact with service providers outside of the service using the telephone or send the service provider emails in order to build their confidence in personal information disclosure practices. The participants made it clear in interviews that it was the act of interaction that contributed to the confidence building, not merely the acquisition of knowledge. The participants also indicated that interaction with other service users, in particular those from their social and family circles, was critical to building confidence in on-line personal

information disclosure. Responses in the interviews indicated that family and peer support often takes place at the point of service use while the service user is engaged with the service. The explanations users gave during the think-out-loud activity also reflected confusion and lack of understanding as to what would happen to their personal information. This is despite those participants undergoing various Internet safety education programmes. Support at the point of service use is therefore seemingly an important aspect to the design of confidence building technologies.

B. The role of privacy statements

In the majority of on-line services, service providers communicate their privacy stance through privacy statements. Research [6, 14] has shown that users ignore on-line privacy statements. While observing this behaviour we also asked our participants to give us their feedback using a think-out-loud method so that we could develop a deeper understanding of their privacy behaviours (Table II).

TABLE II.   USERS' COMMENTS ABOUT CURRENT PRIVACY STATEMENTS

Time consuming	23 of users think the privacy statements are "too long" to read and it is time consuming: *"…they make it too long winded…"* *"…We are in a very fast modern world now and people want things to be done in a flash…"*
Legal jargon	5 users claimed the statements are ambiguous and contains legal jargon which makes it difficult to understand: *"… I would say a fraction of the population can really understand what it says…"*
Small font	18 users were annoyed by the small font used in the statements and said the "small print/letters" has discouraged them to read it: *"…With these small letters people's eyes get tired and you can't even finish reading it…"*
Awareness of the same contents	4 users claimed to have the knowledge of the contents and therefore will always skip reading privacy statements. They believe all privacy statements are the same: *"…It's almost the same…you are accepting you are above 18…"* *"…I didn't read it because they all look the same…"*
Invisible link	10 users were unable to notice the link to the privacy statements on the screen and hence one users said: *"…I realized I didn't read the terms and conditions and also the privacy policy…it didn't come out first before I actually registered…I thought there would be somewhere I could read it before actually registering…"*

Unsurprisingly, when registering with the websites, the observer noted that 54 participants avoided reading privacy statements. This amount was significantly higher than those who admitted in the questionnaire to not reading such statements. Users were questioned (in the interview) as to why they avoid reading privacy statements and their comments can be categorised into five groups: Time consuming; Legal jargon; Small font; Awareness of the same contents; Invisible link. Table III shows a few examples of

their interview comments combined with results from the questionnaire and think-out-loud. 49 of users said they accepted the statements, whereas 7 users rejected them. Using think-out-loud and interviews it was possible to elicit the reasons for rejecting the reading of privacy process as a privacy protection practice. The existence of the privacy statement contributed to the willingness of a participant to engage with the registration service but the privacy statement did not affect feelings of confidence when disclosing personal information.

Service Design Comment: The feedback from participants shows that if interaction is to be designed, communication techniques must be deployed in a way that is accessible and inclusive. In particular, language used must be grounded in the everyday language of the service user. Communication must also be accessible for users with differing levels of literacy and cognitive abilities. The interaction mechanisms must be designed in such a way that they are fore-grounded for the service users who want to use them but also designed in such a way that users are not inconvenienced or forced to read copious text. The observations and the responses to the interview questions also show that four of the participants felt they were aware of the privacy issues and yet their responses and tasks behaviours do not reflect this. This is not unusual for users with more extensive Internet experience. Therefore, confidence building interventions also need to introduce critical engagement by encouraging reflection on practices and the challenging of privacy risk assumptions.

V. DISCUSSION AND CONCLUSION

A. Implications of the Current Practice Picture

Our research shows that a service user expects a reliable service provider to understand their users' privacy concerns and explain their institutional privacy stance. Our results also show that this communication must be accessible and inclusive. The implications of not including such communication is that, despite costly investment in trust marks, security technologies and brand development, service users will continue to give false information, limit the extent of their engagement in on-line services and avoid registration with on-line services. In the era of delivering public services on-line, this potentially has devastating consequences for public service delivery and the ability of the most vulnerable to receive the public service support that they need. This study shows that current on-line service design assumes that confidence building will take place off-line. Participants indicated support at the point of use was desired in addition to off-line education and support.

B. Where to build confidence

Some socio-technical systems research includes a layer of system design which enables users to resolve issues of mistrust, unfairness and unjustness [20]. Social computing is situated at this layer and focuses on the relationship building processes. From a socio-technical perspective, a system can be conceptualized as having the following layers [17]: physical layer, informational layer, personal layer and the

communal layer. The personal layer relates to an individual's use of the system, whereas the communal layer relates to a group or institutional use of the system. From a privacy perspective: the physical layer and the information layer are the layers typically addressed by the privacy protection techniques described in Section II. The personal layer is responsible for exchanges of meaning and utilizes HCI design techniques and has been extended by the usable privacy community's research as also described in Section II. However, explicit design of the communal layer has not been explored in technical privacy research. This is the layer that is necessary for confidence building in the service user-service provider relationship because, as the participants' responses indicate, the issues are ones of mistrust and feelings of unfairness and unjustness.

C. Instantiations of confidence building technologies

Traditionally, the socio-technical layer has been implemented in face-to-face communication [5] and not using digital techniques. Social computing platforms and techniques [8] offer the potential to digitise this layer. Public service providers are increasingly delivering public services on existing social computing platforms for this reason. Gathering design requirements from four user studies and service provider studies, VOME has prototyped and is trialling two instantiations of confidence building technologies which use a social computing platform. The need to visualise the relationship between a user's information disclosure action and the journey of their personal information after disclosure was a requirement common to all participants. In response to this, an interactive map was designed using social translucence techniques, which enables users to visualise, question and challenge the disclosure path that their personal information will take. Challenging and query raising uses embedded messaging technology common to social computing platforms [8].

In order to support service user queries at the point of use, an interactive forum was embedded into service design that enables both service users and service providers within a community to respond and raise privacy related queries. This forum is being developed to include technologies that enable the critical evaluation of specific privacy stances by the service users themselves and to include pre-programmed utterances to support a spectrum of literacy capabilities.

Technologies that support confidence building in information practices are an essential aspect of usable privacy management design if service design is to be truly inclusive.

ACKNOWLEDGMENT

REFERENCES

[1] P. Dourish, and K. Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena", HCI, Lawrence Erlbaum Assoc., 2006.

[2] A. F. Westin, "Privacy and freedom", London, Vol.97, 1967.

[3] D.J. Solove, "Understanding privacy", Harvard university press, 2008.

[4] C. A. Ardagna, S. D. C. Di Vimercati, G. Neven, S. Paraboschi, F. S. Preiss, P. Samarati and M. Verdicchio, "Enabling Privacy-Preserving Credential-Based Access Control with XACML and SAML", 10th IEEE International Conference on Computer and Information Technology,. IEEE Computer Society, Bradford. 2010. pp. 1090.

[5] D. Bogdanovic, C. Crawford and L. Coles-Kemp, "The need for enhanced privacy and consent dialogues, Information Security Technical Report, Vol.14, No.3, 2009, pp. 167-172.

[6] J. Bonneau and S. Preibusch, "The privacy jungle: On the market for data protection in social networks", Economics of Information Security and Privacy, 2010, pp. 121-167.

[7] C. A. Brodie, C. M. Karat and J. Karat, "An empirical study of natural language parsing of privacy policy rules using the SPARCLE policy workbench", Proceedings of the second symposium on Usable privacy and security, ACM, 2006, pp. 8.

[8] M. Parameswaran, A. B. Whinston, "Social Computing: An Overview", Communications of the Association for Information Systems , Vol.19, No.37, 2007, pp. 762-780.

[9] T. Buchanan, U-D. Reips, C. Paine and A. N. Joinson, "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, No.2, , 2007, pp. 157 – 165.

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

[11] L. Coles-Kemp, E. Kani-Zabihi, "On-line privacy and consent: a dialogue not a monologue", In proceeding of NSPW 2010, 21-23rd September, ACM Press, USA, 2010.

[12] J. Cornwell, , I. Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor and J. Hong 2007, "User-controllable security and privacy for pervasive computing", Mobile Computing Systems and Applications, HotMobile 2007. Eighth IEEE Workshop, 2007, pp. 14.

[13] P. Dourish, B. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the wild: user strategies for managing security as an everyday practical problem", Personal and Ubiquitous Computing, Vol.8, No.6, 2004, pp. 391-401, DOI: 10.1007/s00779-004-0308-5.

[14] C. Jensen, C. Potts, C. Jensen, "Privacy practices of Internet Users: Self-reports Versus Observed Behaviour", International Journal of Human-Computer Studies, Vol.63, 2005, No.1-2, pp. 203-227.

[15] E. Kani-Zabihi, G. Ghinea, and S. Y. Chen, "Experiences with developing a user-centered digital library", International Journal of Digital Library Systems, Vol.1, No.1, 2010, pp.1-23.

[16] P. Kumaraguru and L. F. Cranor, "Privacy Indexes: A survey of Westin's Studies", Carnegie Mellon University, Pittsburgh, 2005.

[17] K. Kuutti, "Activity Theory as a Potential Framework for Human Computer Interaction Research", in Context and Consciousness, eds. B. A. Nardi, 1996, pp.17-44.

[18] A. M. McDonald and L. F. Cranor, "An Empirical Study of How People Perceive Online Behavioral Advertising", CyLab, 2009, pp. 2.

[19] N. Luhmann, "Familiarity, Confidence, Trust: Problems and alternatives", in Diego,G (ed) Trust: Making and Breaking Cooperative Relations, University of Oxford, Oxford, 2000.

[20] B. Whitworth, "The Social Requirements of Technical Systems, Socio-technical Design and Social Networking Systems" eds. Whitworth, B. And de Moor A , 2009, pp.1-22.

[21] J. R. Cordoba, L. Coles-Kemp, J. Ahwere-Bafo, "(Re)-conceptualising E-government: Studying and Using Patterns of Practice". Submitted to OR52 (Operational Research Society Annual Conference) Paper to appear in proceedings.