Journal of Computer and Communications, 2014, 2, 220-231
Published Online March 2014 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2014.24029

Scientific Research

On-Line Privacy Behavior: Using User Interfaces for Salient Factors

Thomas Hughes-Roberts, Elahe Kani-Zabihi

Computing and Technology Department, Nottingham Trent University, Nottingham, UK
Email: Thomas.hughesroberts@ntu.ac.uk, elahe.kanizabihi@ntu.ac.uk

Received December 2013

Abstract

The problem of privacy in social networks is well documented within literature; users have privacy concerns however, they consistently disclose their sensitive information and leave it open to unintended third parties. While numerous causes of poor behaviour have been suggested by research the role of the User Interface (UI) and the system itself is underexplored. The field of Persuasive Technology would suggest that Social Network Systems persuade users to deviate from their normal or habitual behaviour. This paper makes the case that the UI can be used as the basis for user empowerment by informing them of their privacy at the point of interaction and reminding them of their privacy needs. The Theory of Planned Behaviour is introduced as a potential theoretical foundation for exploring the psychology behind privacy behaviour as it describes the salient factors that influence intention and action. Based on these factors of personal attitude, subjective norms and perceived control, a series of UIs are presented and implemented in controlled experiments examining their effect on personal information disclosure. This is combined with observations and interviews with the participants. Results from this initial, pilot experiment suggest groups with privacy salient information embedded exhibit less disclosure than the control group. This work reviews this approach as a method for exploring privacy behaviour and proposes further work required.

Keywords

On-Line Privacy, Social Networking Site, User Interface, Users' Behavior, Theory of Planned Behavior

1. Introduction

Privacy is a sensitive subject which matters to Internet users [1]-[4]. However, users of social network sites (SNS) such as Facebook routinely disclose highly personal information to the network, often to unintended and potentially unknown strangers [5]. Privacy as a concept is a complex social phenomena suffering from a variety of contextual definitions that shift from person to person [6] making it a difficult topic for research. This problem is exacerbated within social networks as data is persistently stored and dealt with granularly [7]. An individual data item may not be particular sensitive until taken into context with others visible within the network from various points in time leading to user struggling to manage their privacy. Previous studies in the field have

How to cite this paper: Hughes-Roberts, T. and Kani-Zabihi, E. (2014) On-Line Privacy Behavior: Using User Interfaces for Salient Factors. *Journal of Computer and Communications*, **2**, 220-231. http://dx.doi.org/10.4236/jcc.2014.24029

reported that young adults are more vulnerable to privacy threats and at risk when revealing personal information has become easier. SNS users disclose personal information more frequently without any indication of the possible consequences *i.e.* identity fraud [4]. Therefore, the focus of our preliminary study reported here is young adults' behavior in terms of disclosing personal information. A privacy paradox has been observed by research within social networks where a user's intention does not match their behavior online [8]. Therefore, there is a need to study users' behaviors to understand their deviation from the intention specially when users have raised privacy concerns. Given that behavior can be considered a reaction to environmental stimulus [9] and the User Interface (UI) is the environment interacted with, this paper seeks to present a method to exploring the role of the UI in contributing to, and potentially solving, damaging privacy behavior using social psychology. We studied users to understand users' behavior at the point of personal information disclosure. Specifically, the social psychology Theory of Planned Behavior (TPB) [10] is used to explore disclosure in a series of experiments, this is combined with informal interviews and observations to examine the cognition of behavior in relation to the UI. This has been identified as an area of need for research [11]. This paper examines the approach, presents the results of a preliminary study and proposes alterations to the method for future research.

2. Background

There have been numerous proposed causes of observable poor privacy behavior put forward by literature. Users may be insufficiently skilled at implementing their privacy preferences within a SNS [12] due to the added technical awareness required. They may be unaware of the impact of their actions within the context of privacy and the issues that may arise due to them [13]. They may also be unable to overcome the design of the network itself that encourages openness based on the business model of social networks [14]. Indeed, the HCI field of persuasive technology (PT) suggests that Facebook is designed to persuade users to act in opposition to how they would normally [15]. If a system can be designed to persuade for openness can the opposite also be achieved? These systems may have a lack of privacy salient information present within their UI so privacy information is not included within the thought process of resulting behavior [16]. Precisely what privacy salience is has not been clearly defined, a point that this paper seeks to clarify. It is also suggested that the psychology of the user plays an important role. Hyperbolic Discounting, for example, describes how users ignore long term risk in favor of short term gain [17].

In a user focused study conducted by Kani-Zabihi and Coles-Kemp [5], the result indicates that Internet users preferred to interact with UI to read privacy related information such as privacy policy statements or user/service agreements which are currently in text only format. The research also concluded, in addition to communicating the privacy policy contents, privacy risks also need to be communicated.

Exploring the concept of privacy as such allows for the granularity of interaction to be taken into account. Users are expected to deal with their information granularly in social networks [7] where they interact with an individual piece of data at a time. So, examining privacy in terms of the granular interactions allows each to be observed and manipulated by the treatments to be implemented. For example, behavioral consequences of disclosing ones date of birth can be isolated and addressed individually from other granules. Finally, in a qualitative study of Facebook postings it was found that causes of poor behavior include; not thinking of the consequences, misjudging social norms of peer groups and misunderstanding their level of control [18]. This paper proposes that the TPB [10] covers these areas well and has the potential to directly address them through the UI.

Examining the role of the UI is not without precedence. Work examining the effect of the presence of privacy seals found that disclosure was not lessened when they are visible but tailored privacy warnings did decrease disclosure [19]. This work used a real world e-commerce site to test the use of these seals. Furthermore, increased options of control was found to increase disclosure levels rather than lessen it as perhaps should be expected [20]. Here, a mock up social network was created for users to sign up to. The effect of various treatments on user behavior was measured. Each of these studies however, have lack a theoretical underpinning, a common criticism of HCI research [21]. Indeed, it has been noted that there is a need for behavior models to be introduced in order to further field [22].

Therefore, our research study used a behavior model examining theories of social psychology as tools for exploring privacy behavior in relation to the UI. Specifically, the TPB (**Figure 1**) chosen as an ideal fit to the problem area as it describes three salient factors that influence the intention to act and actual behavior [10]. These factors are:

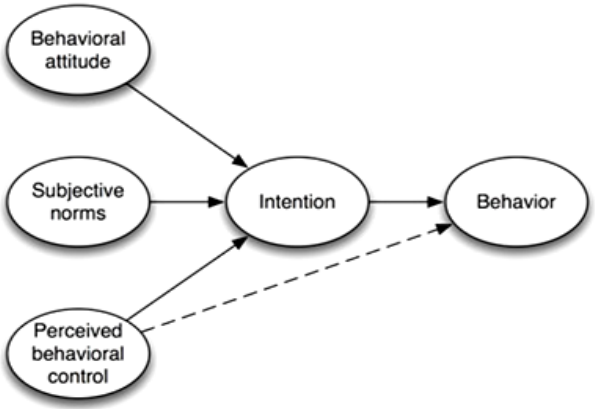

Figure 1. The theory of planned behaviour.

- Behavioral attitude (knowledge and perception of behavioral consequences): *The degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question.*
- Subjective norms (extent of the effect of social peers and experts): *It refers to the perceived social pressure to perform or not to perform the behavior.*
- Perceived control (perception of the ease of behavior): *It refers to perceived ease or difficulty of performing the behavior and it is assumed to reflect past experience as well as anticipated impediments and obstacles.*

Initially, the TPB seems a natural fit for not only classifying the privacy problems mentioned earlier but also for informing the design of experiments with multiple treatments framed by tested theory. For example, other work has made the proposal that increasing awareness can provide a solution to the privacy problems described [23]. The TPB provides the means of identifying what awareness to raise and provide a foundation for hypothesizing the effect this may have according to its framework.

This theory suggests that changing these influencing factors will have a bearing on an individual's intention to act and actual behavior. Hence, UI's that include elements designed around these salient properties should play an active role in affecting privacy behavior; for example, UI features that raise awareness of information disclosure consequence may play a part in changing the behavior of disclosure.

Hypotheses

This paper presents our results from a research study to test the following hypotheses:

(H1) users' privacy behavior can be studied by using UI to model salient factors in TPB.

(H2) Groups with salient properties embedded will exhibit stricter privacy habits than those without.

3. Design

The disclosure of users' personal information often happens at the point of registration for an online service. Consequently we used a registration process for a new social network site for students at University of Salford in UK. This process was designed to create personal profile for each user. **Figure 2** shows the first screen, Sign Up page. Note the similarity to Facebook in the design. This is to address the ecological validity of the experiments; where the design of the system should detract from the effect of the treatments applied [24]. This is also aimed at encouraging users to act as they would if a real SNS is asking for this information of them. However, these experiments will not cover behavior that is part of a goal conceived by the user which is out of scope. Instead, this work seeks to clarify what role the UI could play in influencing disclosure behavior within this set context.

The following sections describe each of the theoretical properties of salience and how they have been interpreted into a UI element aimed at influencing behavior.

3.1. Behavioural Attitude

The TPB defines behavioral attitude as the awareness and perception of behavioral consequences. It is impractical

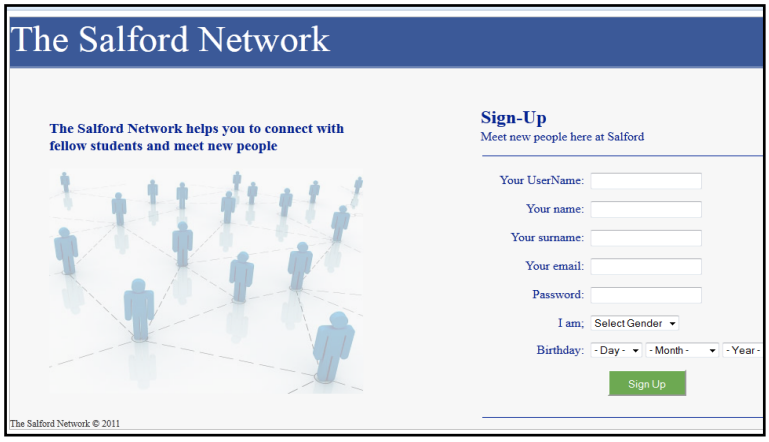

Figure 2. Control—sign-up page.

to assume that specific consequences can be raised for disclosing a piece of information within any given context. As such, each piece of information is grouped according to a general level of impact and represented by the UI metaphor of traffic lights [25]; green for go (disclose), yellow for caution and red for stop (do not disclose). The aim of which is to remind users of their attitude or to inform their evaluation of disclosure consequences at the point of interaction. These can be seen in **Figure 3**. Note this is a portion of the UI presented to the user. The following groupings are therefore derived from the potential implication of disclosure that piece of data could have. A green light represents potentially embarrassing or socially oriented information, yellow is for breaches in policy (e.g. data which could prevent job offers or result in unemployment) and red indicates information that could cause legal problems (either breaches of law by the user or toward the user). Questions are assigned to sensitivity based on our interpretation of the potential consequences. For example, information of political or religious affiliations would not breach any laws but could lead the user not obtaining employment or being socially victimized (hence, the amber/yellow category). These are also present for the application of settings and follow a similar train of thought; red for the more invasive information grouping where a privacy setting can be applied. This UI element is presented to the user at the start of the experiment in a pop-up box introducing the treatment.

3.2. Subjective Norms

According to the TPB subjective norms represent the extent to which the attitude of others influences behavior. For example, a user could disclose information in order to strengthen social ties with their peers as per the Theory of Social Capital [26] or state a high level of concern due to increased media attention toward privacy. This is interpreted into an advice box providing the treatment for this group. This box offers a recommended action and a statement of what other users did when faced with the same questions as seen in **Figure 4**. The aim being to examine if one holds more sway over a user's decision to disclose.

This suggestion box becomes visible to the user upon interaction with the specific information field it relates to. Similar boxes are present advising on the optimum settings to be applied also.

3.3. Perceived Control

The final salient influence proposed by the TPB is that of perceived control which influences both intention and action according to the model and is closely tied with a user's self-efficacy; that is, their confidence in their own ability to perform a certain behavior [27]. A user may believe that identifying and suitably protecting their sensitive information is easy yet this belief is not reflected in reality leading to observable poor behavior. Similarly, a user may not be skilled technically (or have the belief they are not). This salient feature is designed to aid participants in identifying what information they *have* disclosed could be sensitive and make changes upon reflection. Immediately after each screen of questions and settings application is a review screen where the data is disclosed presented again but within a privacy oriented context. A "P-Score" dynamically alters based on changes to disclosed elements to make clear the impact of alterations to disclosed data.

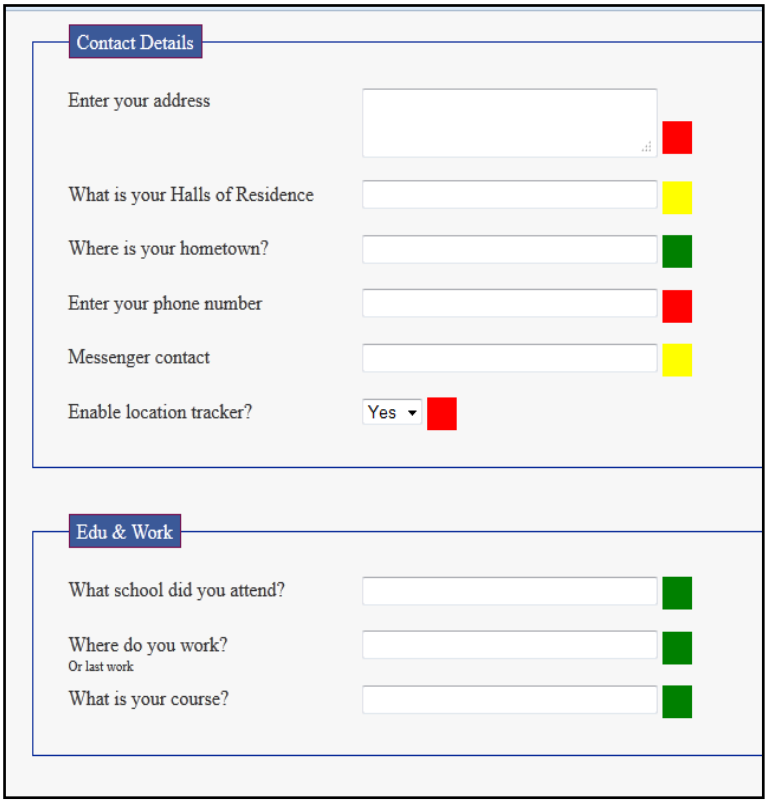

Figure 3. Traffic lights.

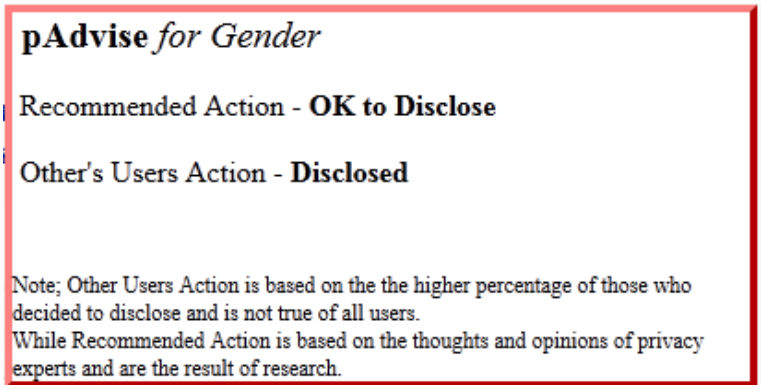

Figure 4. Subjective norm.

Signal Detection Theory [28] suggests that increased environmental noise decreases a person's ability to make correct judgments impacting on an individual's self-efficacy. Hence, the "noise" of the social network and its specific goals are removed and replaces with a privacy focus. So, a participant will go through the questions twice, once as they are asked by the "vanilla" interface and again by reviewing and altering their responses. This review screen is presented in **Figure 5**.

4. Methodology

We recruited participants from undergraduate level students at University of Salford in UK. This is not considered to be a representative sample of users of a SNS but is consistent with the age group that most exhibits paradoxical privacy behavior [29]. Participants are to be approached prior to lab sessions within their courses and asked to take part should they wish to join a new social network. They were asked to create their profiles in a

new social network specifically for the university. In the creation of this profile they are asked a variety of questions to populate their profile with information about themselves. These questions will vary in sensitivity, asking questions from favorite films to drug use, and are grouped into separate sections generally described in **Table 1** with a total of 30 questions for participants to respond to. Furthermore, questions have variety of interactive inputs, ranging from text boxes to binary responses in the form of check boxes. These questions can also be grouped according to the sensitivity prescribed to them in the behavioral attitude group: red (highly sensitive), yellow (moderately sensitive) and green (little sensitivity) with 10 questions in each category.

The settings that can be applied are to be split into sections as they are grouped within the SNS Facebook and are generally described in **Table 2**.

Each treatment is applied to one experimental group and each treatment group compared to a control (**Figure 1**) with no privacy salient features present. All participants in each experiment are asked the same series of questions in the same order with the only difference being the treatment applied to the UI; the way in which these questions are presented can be seen in **Figure 6**. Following the questions will be the application of settings with the connection settings appearing as a separate link as in Facebook (requiring the participant to navigate to it if they wish to make changes). Results from these experiments are combined with observations made during their conduction and with post-experiment informal interviews aimed at adding to the data richness.

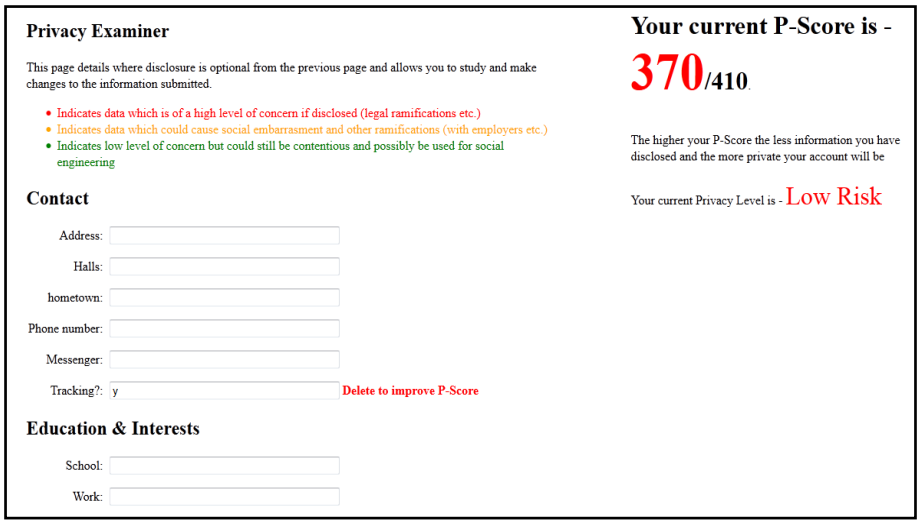

Figure 5. Perceived control.

Table 1. Question groupings.

Group	*No of questions (optional)*	*Detail*
Sign Up	2	The first page of the experiment contains basic sign-up information and is not particularly sensitive.
Contact Information	5	The user is asked for contact information; such as address, phone, email etc.
Education & Interests	8	The user is asked for educational background information and personal interests.
Contextual Information	12	This section contained a variety of questions dealing with the personal context of the user. Questions ranging from relationship status to drinking habits were.
Marketing Data	3	This section asked the user about shopping habits; favorite stores, items usually bought etc.

Table 2. Settings.

Settings	*Detail*
General Settings	These were explicitly presented to the user during the profile creation process and covered areas such as photos, education, interests etc.
Connection Settings	These settings required extra exploration by the user (although the link was presented to them during the process). These covered the general settings of who can contact them and how visible they are.

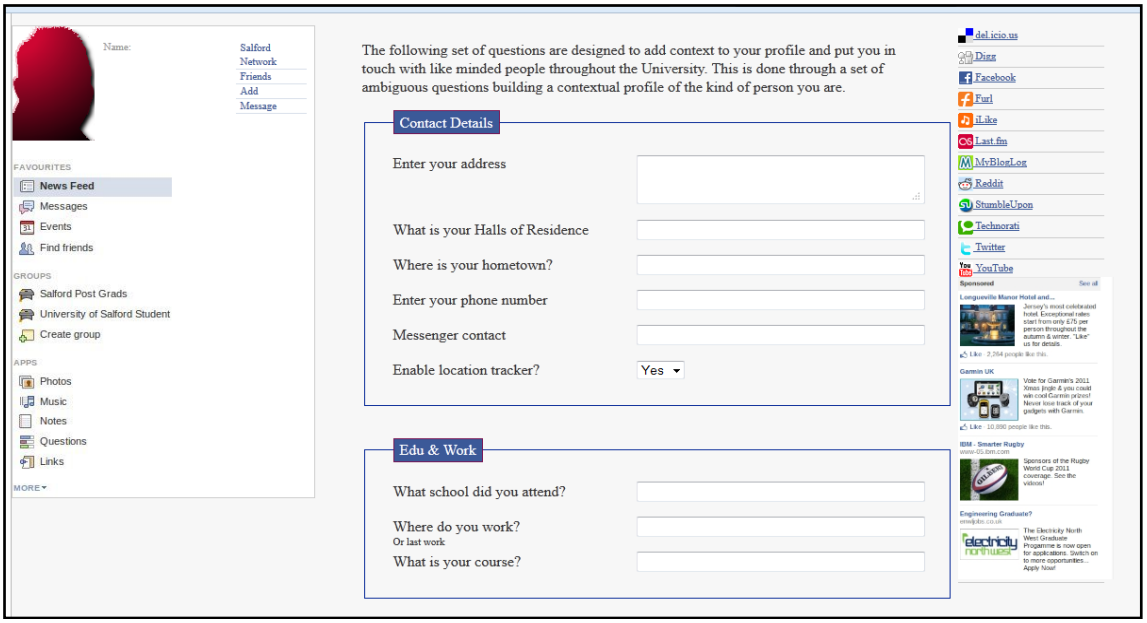

Figure 6. UI overview.

5. Results

In total, 45 participants took part in the study and were split randomly into the groups described; all participants were users of SNSs, were predominantly male and where within the 18 - 21 age range. Informal interviews were conducted immediately after the experiments with 3 participants from each group. Participants are asked what they disclosed, why and what they thought of the UI elements present. Observations were made during the experiments and anything of interest noted down including, but not limited to, anything participants said and how they interacted with the system in front of them; these will be used during the discussion of the results presented here.

Table 3 details the average level of non-disclosure per participant in each of the groups along with average setting score gained split into the two settings groupings described earlier. This score is calculate out of a total of 200 (maximum settings applied) and decreases as more lax options are chosen (0 for “Everyone”, 10 for “Friend of a Friend” and 20 for “Friends Only”). There are two rows for Perceived Control for the information given before the review screen and after.

The spread across information groupings is detailed in **Table 4**; note, that two statistics are given, one for the amount of questions answered and one where only yes responses are considered for binary questions.

Due to the non-normal distribution of the data, nonparametric statistical tests were ran on the data set using the statistical software package SPSS. Specifically, the Mann Whitney U test is ran on each group to compare to the control where a probability value of 0.05 is required to reject the null hypothesis that TPB salience did not affect disclosure; the results of these are detailed in **Table 5**. Two tests are ran levels of disclosure: one on the amount of questions answered (*i.e.* the number of interactions) and one where only yes answers to binary questions are counted as disclosure.

Similar tests ran on the settings differences between the treatments and control did not produce statistically significant results and will be addressed in the discussion.

The presence of salient UI elements resulted in differing (reduced) levels of disclosure from participants in answering the same questions in a controlled context when compared to the control group. Settings held an increase in averages for the personal attitude group and the perceived control. However, the subjective norms groups decreased when compared to the control although without statistical significance.

6. Discussion

The following discussion deals with each group in turn to examine if the statistical changes in behavior are due

Table 3. Averages across groups.

Group	*Users*	*Total amount answered questions*	*Average per participant*	*Settings*	*Connection*
Control	10	84%	3.70	108	0
PA	11	61%	9.73	145.5	0
SN	12	60%	12.17	72.5	5
PC1	12	53%	18.58	172	15
PC2	12	35%	10.17	185	94.2

Table 4. Averages across questions groupings.

Group	*"Green" questions answered*	*"Yellow" questions answered* (*only yes responses*)	*"Red" questions answered* (*only yes responses*)
Control	72%	90.3% (65%)	90% (67%)
Attitude	49%	67% (41%)	67% (32%)
PC1	44%	57% (39.8%)	57.5% (32.5%)
PC2	34.1%	38.5% (29.5%)	32.5% (18.3%)
Subjective	54.1%	68.6% (47.1%)	57.5% (33.3%)

Table 5. Statistical results.

Group	*Statistical Test*	*Disclosure P-Value*	*Disregarding No answers*
Personal Attitude	Mann Whitney U	P = 0.029	P = 0.005
Perceive Control (Pre-Salient Review)	Mann Whitney U	P = 0.003	P = 0.002
Perceived Control (Post Salient Review)	Mann Whitney U	P < 0.0001	P < 0.0001
Subjective Norms	Mann Whitney U	P = 0.025	P = 0.043

to the intended influences of the model or due to other reasons that the treatments may have introduced to the UI.

6.1. Control Group

Participants within the control group demonstrated a willingness to disclose much of the information asked of them and when asked after why, responded: "I thought I had to give everything".

The Milgram Effect would suggest that participants acted according to how they were instructed as opposed to what their conscience tells them [30]. From the persuasive technology perspective, users may answer the questions asked of them in order to achieve a perceived system goal *i.e*. the system asks for it to sign up, so it must be needed. This would be in line with assertion that users of social networks are goal-driven [31] and privacy is a secondary goal of using the system [32]. These assertions will be kept in mind when examining the treatment groups. However, it may be that participants were not completely aware that disclosure was optional, highlighting a potential design flaw in the experiment that should be corrected in future iterations of it.

6.2. Behavioral Attitude Group

The behavioral attitude treatment aimed to increase awareness of the consequences of disclosing particular pieces of information and examine the effect of that potentially increased awareness. It is a reasonable assumption to make that the questions dealing with higher degrees of sensitivity are less likely to be answered by participants when they are informed of the potentially serious consequences involved. This group did disclose significantly less than the control and, if we consider only yes answers (see **Table 4**), participants disclosed the

least in the red grouping of questions. However, disclosure also decreased in the green section of questions which tended to hold more long-winded question interactions. It could be that the option of disclosing information was made clear through the treatment. Indeed, Persuasive Technology suggests that options are not made clear by SNS's [15], while HCI also has shown that users are more likely to opt for easy interactions when they are unskilled at system use [33]. However, it may also be a result the amount of effort required to answer questions. The green category, for example, held more questions with text field input and questions that may not be applicable to all participants. The yellow and red categories, on the other hand, held more binary response questions with simple yes, no checkboxes. Hence, the reduction in the green category may be due to unwillingness to interact with questions requiring more effort. Although, post-experiment one participant did note: *the lights did make me think about my privacy*, *particularly things like my address*. There is some evidence then, that participants are considering their privacy. However, due to the types of questions asked the extent of the effect of the treatment in terms of informing awareness is unclear.

So, while the salient treatment did decrease disclosure within the group, it could be for reasons outside the remit of the TPB model. Instead, the treatment made users aware of the option of disclosure and they seemed to exercise that choice when faced with the more complex interactive elements.

6.3. Subjective Norm Group

The Subjective Norms treatment aimed to examine the effect of salient advice offered to the user on their behavior. Again, levels of disclosure were significantly decreased from the control group and, looking at only the "yes" answers in **Table 4**, participants disclosed less in the yellow and red categories than the green. Although, one participant commented post-experiment: "I answered those questions but I shouldn't have, I answered the easy ones"; a similar comment as reported in [18]. Again, suggesting that the ease of interaction plays a persuasive role in encouraging disclosure.

Returning to the intended effect of the treatment, participants within this group did not appear to favor one form of information over the other from the salient property. Indeed, the pop-up nature seemed to disconcert users where they were observed questioning what they did wrong to make a "warning box" appear. This could go some way to explaining the drop in settings scores applied for the group as a whole. The salient feature added more information to the UI and in a way that seemed to alarm users; as such, the self-efficacy of participants may have been affected so they were not confident to make changes to the system. Specifically, the treatment added two sources of information that could potentially confuse participants and make it unclear which advice, if any, they are following. Similarly, the control paradox [20] found that increased control over information increased disclosure. Despite these points disclosure was less than the control and it would seem this is due to the points mentioned previously. Specifically, the UI elements made it clearer that disclosure was not mandatory. Indeed, when asked what they thought of the elements added, a participant in the Personal Attitude group noted that they *made it clear what that they did not have to fill everything in, like the red dots on other web forms*.

Future iterations of the experiment should explore the potential effect of this treatment by providing a single piece of advice rather than two in the same pop-up box. Perhaps two separate treatments could be utilized to explore each type of advice to examine if one has a greater effect.

6.4. Perceived Control Group

The goal of the perceived control group was to make it easier to identify and protect potentially sensitive information and, indeed, disclosure was significantly less than the control and any other treatment group in these experiments. However, that decrease occurred across all question groupings as the goal of interaction for the users seemed to shift to one of privacy protection; although, the red grouping did contain the least amount of disclosure (see **Table 4**, PC2). Particular focus was paid to the dynamic "P-Score" with one participant mentioning: "I'll delete this to get my P-Score down". Interestingly within this group, one participant stated that the treatment applied did not inform his decision to disclose a piece of information over another. However, disclosure was decreased upon review from this participant showing the property did have an apparently sub-conscious effect. Such an observation could fit in well with the concepts of unconscious motivation and psychic determinants from psychology [34]. These suggest that the actions of an individual are subconsciously derived and informed by factors that are not immediately obvious to them. Hence, the question is raised: can the personal attitude of an individual be overtly informed such that it alters their conscious processing of a behavior? That is,

can UI elements alter the perceptions of individuals such that they report the specific reasons (with probable consequences) behind the performance of granular behavior?

Finally, the "connection settings", which required navigating through an optional link, remained largely untouched by all participants except for the Perceived Control group post-review who were the only participants to have these settings explicitly presented to them as part of the interactive flow. Again, this could be explained through goal driven behavior (not presented, not necessary) or through self-efficacy (not confident enough to explore). Not only do participants require knowledge of specific risks as they relate to them and their context, it would appear they also require a level of comfort in using the system that enables them to manage those risks and utilize the system appropriately.

7. Reviewing the Method and Lessons Learned

This paper has presented the social psychology TPB as a tool for exploring privacy behavior in controlled experiments and a method for implementing it as such. This provided a useful framework for specifying varying treatments with a theoretical foundation, enabling a greater degree of data triangulation to produce the conclusions presented here. Hence, too revisit our hypothesis H1 there is promise in such an approach given that the behaviour of privacy can be compared between groups of participants. This initial, pilot study has demonstrated that the UI can be used to influence and provided avenues of research when employing such an approach in the future.

In terms of H2, initial results show that such an approach can influence the behavior of users at the point of interaction. However due to the limitations faced in this study, it is unclear if the changes in users' privacy behavior are a result of an increase in privacy awareness. Future iterations of the experiment should seek to correct these and would benefit from a control that makes the option of disclosure clear and a subjective norms treatment that contains a singular piece of direction. Furthermore, the questions asked must be equally distributed across the sensitivity categories in terms of the effort required to answer them and their applicability to participants in order to increase the chance they are answered in relation to each other.

The work focused on a subset of social network users on a specific undergraduate course and so is not representative of a broader SNS population. However, the role of the work was to examine the potential for the UI to play a role and, given that it did seem to within this subset; the method can now be carried into further work with a broader sample.

These experiments deal only with information asked of users within the context of the experiment and as such a beneficial avenue for further work would be to examine the effect of these features within a "real" setting where users derive the goals of the system. For example, users within a SNS will post information that is not specifically asked for and instead is a behavior conducted for reasons that they define. Would features such as these be enough to persuade users to think about their privacy under their own context?

8. Conclusions and Further Work

This work has introduced a method of exploring privacy behavior within a controlled experimental environment aiming to examine what role the UI could play in influencing behavior during a sign-up process. To that end the Theory of Planned Behavior is introduced as a novel means of classifying and informing privacy salient User Interface elements. Results from these experiments found that levels of disclosure were reduced when compared to a control sample with no privacy salient properties present.

Participants within these experiments seemed to disclose based on a perceived system goal rather than in their own interests. Salient features subverted this goal to one of privacy leading to decreased disclosure; however, this was across all data groupings including the non-sensitive questions, so, whether this is representative of their own intention or simply a response to persuasion is debatable. Furthermore, it would appear that users would require specific awareness of the risks associated with the granular disclosure of individual data items within the context of that disclosure as well as a level of comfort and skill within the system in order to implement appropriate privacy behavior.

Further work should expand the salient features defined into real world applications; say as browser extensions that retroactively apply them to UI's. The effect of which can be measured by recording data before and after their application. The work would also benefit from a second experiment that addresses the issues outlined here and that has an exit-survey measure in order to assess how the treatments have affected perceived cognition.

The use of the TPB in informing surveys is well documented and is readily available for implementation. Furthermore, post interviews would benefit from a formal, focus group approach with the same set of questions directed at each group allowing for comparisons to be made using qualitative enquiry as well as quantitative. Finally, as user behavior appeared to be influenced through minimal engagement with the system (sub-conscious processing) then a pre-survey based on the TPB could be implemented. This would give an idea of predisposed participants are prior to experiments to disclosure and enable some predictions to be made.

Ultimately, this work has shown that when a specific sample of participants are asked the same questions in a controlled environment, the level of disclosure they exhibit is dependent on the User Interface elements interacted with.

Acknowledgments

My thanks to staff and colleagues at the University of Salford in recruiting participants to take part in this research

References

[1] OFCOM Media Literacy Matters (2010) Online Trust and Privacy: People's Attitude and Behaviour.

[2] US Federal Trade Commission (2000) Privacy Online: Fair information Practices in the Electronic Marketplace: A Report to Congress. FTC, Washington DC.

[3] Karahasanovic, A., Brandtzæg, P.B., Vanattenhoven, J., Lievens, B., Nielsen, K.T. and Pierson, J. (2009) Ensuring Trust, Privacy, and Etiquette in Web 2.0 Applications. *Computer*, **42**, 42-49. http://dx.doi.org/10.1109/MC.2009.186

[4] Kani-Zabihi, E. and Helmhout, M. (2011) Increasing Service Users' Privacy Awareness by Introducing On-line Interactive Privacy Features. In: *Pre-Proceedings of Nordsec* 2011 16*th Nordic Conference on Secure IT-Systems*, Talinn, 26-28 October 2011, 287-306.

[5] Gross, R. and Acquisti, A. (2005) Information Revelation and Privacy in Online Social Networks (The Facebook Case). *ACM Workshop on Privacy in the Electronic Society*, Virginia.

[6] Palen, L. and Dourish, P. (2003) Unpacking "Privacy" for a Networked World. *Proceeding of the SIGCHI Conference on Human Factors in Computer Systems*.

[7] Stutzman, F. (2006) An Evaluation of Identity-Sharing Behavior in Social Network Communities. *iDMAa Journal*, **3**.

[8] Acquisti, A. and Gross, R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Proceedings of the* 6*th Workshop on Privacy Enhancing Technologies*. http://dx.doi.org/10.1007/11957454_3

[9] Breakwell, G.M. (2006) Research Methods in Psychology. Sage Publications Ltd, Oxford.

[10] Ajzen, I. (1991) The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes*, **50**, 179-211. http://dx.doi.org/10.1016/0749-5978(91)90020-T

[11] Masiello, B. (2009) Deconstructing the Privacy Experience. *IEEE Security and Privacy*, **7**, 68-70. http://dx.doi.org/10.1109/MSP.2009.88

[12] Kolter, J. and Pernul, G. (2009) Generating User-Understandable Privacy Preferences. *International Conference on Availability, Reliability and Security*, 299-306.

[13] Miller, R.E., Salmona, M. and Melton, J. (2011) Students and Social Networking Site: A Model of Inappropriate Posting. *Proceedings of the Southern Association for Information Systems Conference*, Atlanta.

[14] Livingstone, S. (2008) Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression. *New Media and Society*, **10**, 393-411. http://dx.doi.org/10.1177/1461444808089415

[15] Fogg, B.J. and Iizawa, D. (2008) Online Persuasion in Facebook and Mixi: A Cross-Cultural Comparison. In *Persuasive*, Berlin, 35-46.

[16] Houghton, D.J. and Joinson, A. (2010) Privacy, Social Network Sites, and Social Relations. *Journal of Technology in Human Services*, **28**, 74-94. http://dx.doi.org/10.1080/15228831003770775

[17] Acquisti, A. and Grossklags, J. (2004) Privacy Attitudes and Privacy Behaviour: Losses, Gains and Hyperbolic Discounting. In: Camp, L.J. and Lewis, R., Eds., *The Economics of Information Security*, Klewer.

[18] Wang, Y., *et al*. (2011) I Regretted the Minute I Pressed Share: A Qualitative Study of Regrets on Facebook. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ACM. http://dx.doi.org/10.1145/2078827.2078841

[19] LaRose, R. and Rifon, N. (2007) Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behaviour. *The Journal of Consumer Affairs*, **41**, 127-149. http://dx.doi.org/10.1111/j.1745-6606.2006.00071.x

[20] Brandimarte, M., Acquisti, A. and Loewenstien, G. (2012) Misplaced Confidences: Privacy and the Control Paradox. In: *Workshop on the Economics of Information Security*, Harvard.

[21] Galletta, D.F. and Zhang, P. (2006) Human-Computer Interaction and Management Information Systems: Applications. Vol. 6, ME Sharpe.

[22] Lyytined, K. (2010) HCI Research: Future Directions That Matter. *AIS Transactions on Human-Computer Interaction*, **2**, 22-25.

[23] Pötzsch, S. (2009) Privacy Awareness: A Means to Solve the Privacy Paradox. The Future of Identity, 226-236.

[24] Lew, L., *et al*. (2011) Of Course I Wouldn't Do That in Real Life: Advancing the Arguments for Increasing Realism in HCI Experiments. Computer Human Interaction.

[25] Marcus, A. (1998) Metaphor Design in User Interfaces. *Journal of Computer Documentation*, **22**, 43-57.

[26] Portes, A. (1998) Social Capital: Its Origins and Applications in Modern Sociology. *Annual Review of Sociology*, **24**, 1-24. http://dx.doi.org/10.1146/annurev.soc.24.1.1

[27] Bandura, A. (1977) Self-Efficacy: Toward a Unifying Theory of Behavioural Change. *Psychological Review*, **84**, 191-215. http://dx.doi.org/10.1037/0033-295X.84.2.191

[28] Macmillan, N.A. (2002) Signal Detection Theory. In: Wixted, J., Ed., *Stevens' Handbook of Experimental Psychology*, John Wiley & Sons, New York. http://dx.doi.org/10.1002/0471214426.pas0402

[29] Barnes, S.B. (2006) A Privacy Paradox: Social Networking in the United States. *First Monday*, **11**. http://dx.doi.org/10.5210/fm.v11i9.1394

[30] Milgra m, S. and Fleissner, R. (1974) Das Milgram-Experiment. Rowohlt.

[31] Bishop, J. (2007) Increasing Participation in Online Communities: A Framework for Human-Computer Interaction. *Computers in Human Behavior*, **23**, 1881-1893. http://dx.doi.org/10.1016/j.chb.2005.11.004

[32] Bonneau, J., Anderson, J. and Church, L. (2009) Privacy Suites: Shared Privacy for Social Networks. 5*th Symposium on Usable Privacy and Security*.

[33] Chiasson, S., *et al*. (2008) Influencing Users towards Better Passwords: Persuasive Cued Click-Points. In: *Proceedings of the* 22*nd British HCI Group Annual Conference on People and Computers*: *Culture*, *Creativity*, *Interaction*, Swinton, 121-130.

[34] Fancher, R.E. (1973) Psychoanalytic Psychology: The Development of Freud's Thought. WW Norton.