Privacy as a Secondary Goal Problem: An Experiment Examining Control

T. Hughes-Roberts

School of Science and Technology, Nottingham Trent University, Nottingham, United Kingdom
e-mail : thomas.hughesroberts@ntu.ac.uk

Abstract

Privacy is a well-documented issue for research with end-users routinely disclosing large amounts of sensitive information about themselves. The privacy paradox, for example, suggests that users are concerned about their online privacy yet behave in opposition to such stated concern. One potential reason for this paradoxical behaviour is that privacy suffers from a secondary goal problem; that is, it is often not considered in conjunction with the primary motivation for using the system. Given that the User Interface (UI) provides the stimulus for interaction this paper proposes that it is ideally placed to remind users of their privacy and motivate them to consider their behaviour with more scrutiny. An experiment is implemented asking participants to sign-up to a social network by answering a series of questions to build their profiles. A treatment is designed based on the Theory of Planned Behaviour which posits that an individual's behaviour is influenced by their perception of how easy a particular action is to inform; hence, UI elements are designed aimed at aiding users in identifying sensitive information and motivating them to consider their privacy. Specifically, participants are given the opportunity to review their submitted information and make amendments; a privacy score is dynamically altered to make the goal of privacy protection more salient. Results from the treatment group are compared to a control. Findings suggest that participants within the treatment group disclosed less than those in the control with statistically significant results and there is evidence that user behaviour is influenced by a privacy goal oriented UI.

Keywords

Privacy, Social Networks, Experiment, Human Computer Interaction (HCI), Control

1. Introduction

End-users of social networks routinely disclose sensitive information about themselves despite stating a high level of concern for their privacy in such services; a phenomenon known as the privacy paradox (Acquisti and Gross 2006). Privacy has been described as a secondary goal problem (Bonneau, Anderson et al. 2009), that it is not considered during interaction where the focus is on achieving other goals which may well be in opposition to the idea of privacy. Users within social networks may therefore forget about the impact sharing information may have when they disclose it or fail to protect it using appropriate privacy settings when it is disclosed. For example, publish on a timeline without thought of the audience or apply default privacy settings. This paper proposes that reminding users of their privacy at the point of interaction through the User Interface (UI) could produce more privacy conscious behaviour.

The paper will introduce relevant related work to define what role user interface can play in informing behaviour by utilising theories of social psychology. An experiment and methodology is proposed with a treatment designed around the Theory of Planned Behaviour; specifically, the salient property it defines as "perceived control" (Ajzen 1991). This treatment aims to make the identification and control over sensitive information clearer, making privacy a more salient part of interaction; results are compared to control group to explore the effect of psychologically informed UI's.

2. Literature Review

Literature has proposed numerous potential causes of the privacy paradox, including low level of technical skill in users (Kolter and Pernul 2009), a lack of awareness of privacy issues (Miller, Salmona et al. 2011) and the design of the social network itself (Fogg and Iizawa 2008, Livingstone 2008). Indeed, privacy itself is a highly complex issue that differs from individual to individual (Rosenblum 2007). Given that users appear to desire a level of concern for the privacy and only they can be aware of their particular privacy context at any given time, an argument can be made that user must be empowered to enact their own privacy needs.

Privacy as a secondary goal for users has also been proposed as a potential cause of poor privacy behaviour (Bonneau, Anderson et al. 2009). That is, users do not consider their privacy at the point of interaction, perhaps as it conflicts with their personal reasons for using the system (or is simply not as important). The lack of privacy salience embedded into the design of the social network has been cited as a potential reason for the lack of privacy consideration shown by users (Houghton and Joinson 2010). If the act of disclosure is considered an emergent behaviour of privacy then theories of behavioural change could provide a means of exploring it. Social networks have been described as a persuasive technology, influencing and changing users habits through their use of the system (Fogg 2009). The Theory of Planned Behaviour (Figure 1) defines three aspects of salience that influence an individual's intention and behaviour (Ajzen 1991).

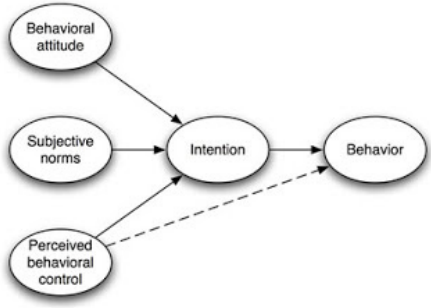

Figure 1: Theory of Planned Behaviour (Ajzen, 1991)

Each of these aspects of salience could provide a basis for altering the UI such that privacy becomes part of the behavioural intention and action and is therefore part of the goal rather than a secondary goal. Indeed, this paper proposes that the UI is ideally suited to empower users to protect their privacy by adding privacy salient information and mechanisms to it and it has been suggested that there lacks critical focus on the role of the UI (Masiello 2009). Furthermore, behavioural psychology suggests that behaviour is a reaction environmental stimulus (Breakwell 2006) and the UI in a social network is the environment with which users react and interact with. Wider research has found that the way in which information is presented to users and the control options surrounding can influence the amount of disclosure users exhibit (Brandimarte, Acquisti et al. 2012).

From the TPB, Behavioural Attitude suggests that behaviour is influenced by our knowledge and perception of the consequences associated with certain acts. Hence, the UI could provide prompts to remind users of the risks of information disclosure. Indeed, an element of persuasion has been defined as suggestion (Fogg 2003) where interventions are set to appear "at the right time" with the right information thus raising awareness of privacy issues. Subjective Norms suggests that behaviour is influenced by the thoughts and actions of those around us. The Theory of Social Capital (Portes 1998) for example, would see disclosure as the act of strengthening social ties with peers. The UI could also be used to deliver advice and guidance either from peers or expert users to aid in the decision making process of privacy behaviour. Finally, the Perceived Control aspect deals with the perception of how easy a behaviour is to perform and how easy it actually is to enact. The design of technology may make it easy to disclose private information and not so easy to protect it. Similarly, users may feel that the identification and protection of private information is simple yet this perception may not relate to reality (and hence paradox). Indeed, tunnelling has been proposed as another persuasion strategy where goal driven design is concerned to reduce uncertainty by leading users through interaction (Fogg 2003).

An experiment has been designed to test each of these salient aspects. This paper presents the findings from the Perceived Control treatment in comparison to a control group and is described in the following section.

3. Methodology

Based on the Perceived Control element of the Theory of Planned Behaviour an experimental treatment is designed to explore the following hypotheses:

H1. A User Interface that aids users in identifying and controlling sensitive information will influence user behaviour and decrease the amount of sensitive information they give.

This experiment asks users to "sign-up" to a new social network created for Nottingham Trent University Students and create their profiles on it. The experiment is designed to mimic Facebook in appearance in order to promote the ecological

validity of the experiment (Lew, Nguyen et al. 2011) and place it in a clear context; see example in Figure 2. Notice the red asterisks to illustrate that the other questions asked of participants are optional and that they do not have to answer.

Figure 2: Experiment home page

This account creation process asks participants a series of questions that range in their potential sensitivity and privacy invasiveness similar to work by Brandimarte *et al* (2012).

In total 33 questions are asked of participants during this account creation process; the total amount of questions answered is used to test H1 by comparing the results in the treatment group to a control. These questions have a variety of input types including text boxes, drop down menus and yes/no checkboxes (e.g. have you ever pirated media?). Participants are informed that the questions are intended to populate their profile with information and create a network of like-minded individuals and the more they disclose the more accurate their resulting network will be.

The control group in total traverses three screens, the introductory screen as shown in figure 1, the question bank that "builds" their profile (see figure 3) and finally a screen to apply privacy settings to their new accounts (the purpose of this paper is to focus on the questions answered rather than the settings applied).

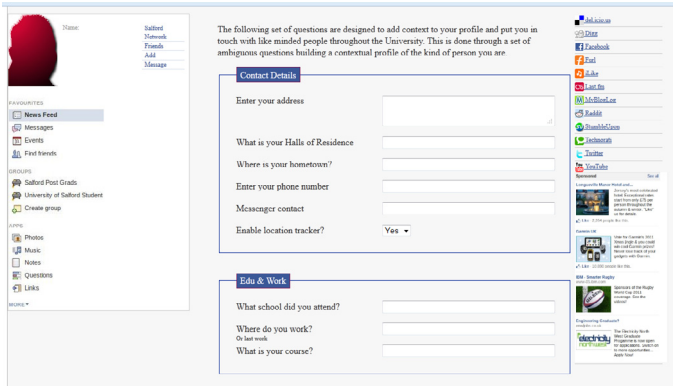

Figure 3: Profile builder page

The treatment adds a series of review screens after each from submission from the participants. This review screen is intended to provide an opportunity to examine what data they have entered outside of the context of the social network, identify potentially sensitive information they have inputted and modify where they feel is necessary. As such, two levels of disclosure were recorded for the treatment group participants: one prior to salient review and one after.

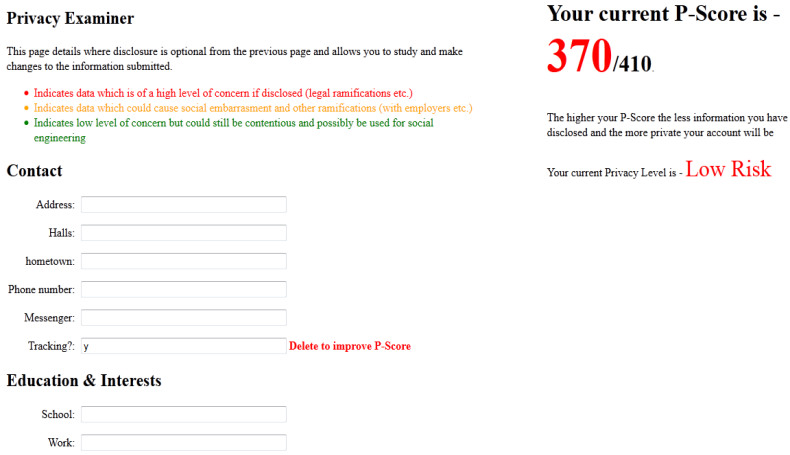

Figure 4: Salient review treatment

This screen aids in the identification of potentially sensitive information that has been submitted through a variety of dynamic UI elements. Each piece of data has a rating that is hidden if the field is blank ("Delete to improve P-Score"), should a participant remove information this rating dynamically turns off in order to emphasise the impact of the interaction and to demonstrate the tangible results of control (making risk management more obvious). This rating of sensitivity categorises the requested data into three brackets: low risk (green), medium risk

(yellow) and high risk (red) (Knijnenburg, Kobsa et al. 2013). Green category data items carry little privacy risk and include such questions dealing with favourite films, music etc. Yellow data items have more potential impact and include questions dealing with political ideology, religion etc. Finally, the Red questions deal with potentially highly sensitive data items including address, drinking habits etc. It is important to note that these categorisations are not clear cut definitions of privacy invasiveness but instead are intended to provide a general guide for participants to use to inform their decisions when considering *their* privacy.

A live "P-Score" is provided to assess the level of privacy risk there potentially is based on how questions have been filled in. These dynamic elements aim to not only aid participants in identifying their sensitive information but also to promote increased control over it through a demonstration of the impact of interaction. Furthermore, the goal of privacy is made the centre of interaction to determine the degree to which participants may be affected when considering extra information during their account creation. As participants will interact with two screens in this treatment group, two measures of answered questions are provided: before and after review of information.

Following the experiment participants in the treatment group have access to an exit-survey and took part in a focus group to assess their perceptions of the treatment. This exit-survey aims to explore the degree to which participants felt the treatment was useful and specifically provides a number of statements for participants to state their level of agreement:

1. I found the privacy information helpful.

2. The privacy information helped to select what to fill in.

3. I believe the privacy information would be beneficial in the long run.

4. I acted differently due to its presence.

Participants were sampled from Nottingham Trent University's Information Systems course (convenience sampling) and were approached in scheduled lab sessions. They were asked if they would like to sign-up to a new social network specifically for the University. They were then randomly assigned to either the control or a treatment group. In total 20 (16 male and 4 female) participants were gained for the control group and 21 (17 male and 4 female) for the Perceived Control treatment group. It is noted that the participants were predominantly male as a result of the sampling technique used and as such may not be considered representative of a social network systems population as a whole.

4. Results

Table 1 provides an overview of the results from the experiment in terms of the total amount of disclosure (% of questions answered) exhibited in the experiment groups (PC1 and 2 represent the Perceived Control group before and after data review).

Group	Number of Participants	Total % of questions answered
Control	20	82%
PC1	21	74%
PC2	21	48%

Table 1: Total Disclosure in Groups

An initial review of these results shows that there is a percentage decrease when compared to the control for PC2 (after data review). Indeed, this is a statistically significant result with a Mann Whitney U $p<0.0001$. The reduction for PC1 however, is not statistically significant ($p=.244$); this would suggest that the treatment influenced participants to review and amend their submitted data. If a participant is considering their privacy then it is reasonable to assume that disclosure will be the least in more sensitive data categories as the treatment should aid in identifying which these are (a breakdown of which is in Table 2).

Group	% of "Green questions answered	% of "Yellow" questions answered	% of "Red" questions answered
Control	83%	82%	81%
PC1	77%	73%	73%
PC2	65%	41%	37%

Table 2: Spread of disclosure across suggested sensitivities

It would appear here that upon review of their data participants did disclose less in the more sensitive data categories with statistical significance compare to the control (Table 3).

Group	Test	Green	Yellow	Red
PC1	Mann Whitney	=.242	=.192	=.175
PC2	Mann Whitney	=.027	<.0001	<.0001

Table 3: Statistical tests comparing each sensitivity category to the control group

Again, this table would suggest that the greatest effect of the treatment appeared in the more sensitive data categories; although, the green category was also reduced with statistical significance. H1, therefore, would appear to be true based on these results. However, further exploration is required to examine if participants are enacting their own privacy desires or those that they feel are persuaded by the system. Literature has noted that user do tend to forsake sub-goals in pursuit of a

perceived main goal provided by the system (Jacko and Sears 2003). It could that participants are being persuaded to be more private than they desire to be.

Statement	Agreed	Neutral	Disagreed
I found the privacy information helpful	58%	32%	10%
The privacy information helped me answer	63%	32%	5%
I believe the privacy information would be beneficial in the long-run	42%	47%	12%
I acted differently due to the privacy information	42%	37%	21%

Table 4: Exit survey results summary

5. Discussion

The literature review identified that privacy can suffer from a secondary goal problem and hence is not considered during the implementation of other pre-defined goals. In this experiment, the goal was to create an account on a new social network and this is achieved through the completion of the smaller sub-goals of answering a series of questions. Certainly, disclosure within the control group seems to be fairly high with an even spread across the sensitivity categories defined in the treatment. This would suggest that their privacy is not being considered during the completion of the task set before them. Indeed, when asked post experiment about why they behaved in such a way the response was: *I don't really know, I just answered the questions* and *I didn't think, now I would have left some questions out*. These responses are similar to wider work (Strater and Lipford 2008) and are indicative of a lack of privacy thought during the interaction. Some participants described themselves as "completionists" and wanted to answer each question they could; indeed, wider research suggests that disclosing information about the self is intrinsically rewarding and potentially addictive (Tamir and Mitchell 2012).

The decreases in the more sensitive information categories in the treatment group would suggest that participants were making a selection of what to disclose based on the potential privacy invasiveness of the information asked of them. However, the question remains as to whether or not participants are enacting *their* privacy preferences or are responding the potentially persuasive goal of the treatment (that places the interaction squarely within a privacy context). From the exit-survey, the majority of participants agreed with the statements that the treatment was useful in aiding their selection. However, only 42% believed that they acted differently due to its presence; this is despite the change in disclosure when the treatment is introduced to the group (i.e. there is strong evidence that they were effected). Participants may be unwilling to admit the extent to which they were influenced by the treatment should it be persuasive in convincing them to act in accordance with strong privacy recommendations. Indeed, there is evidence in the literature that users tend to downplay the effect of perceived counterintuitive behaviour on themselves but do perceive it to be persuasive to others (Debatin, Lovejoy et al. 2009).

Interestingly, post experiment, participant's responses suggested that the dynamic "Privacy Score" was the most influential in convincing them to remove submitted information: *I wanted to get a low score, it was like a game*. Also, when asked if they changed response: *yes, it seemed to want me to*. The score would therefore seem to provide participants with a real-time reaction to their interaction that gave them something to aim for with a real and tangible goal. However, the main reason for removing information may be attributed to gaining a low score and not as a result of thinking about their own privacy needs; although, disclosure was lessened in the more sensitive categories. Privacy would therefore seem to be a more prevalent goal of the interaction where the treatment is present. However, the treatment may have made privacy the *primary* goal of interaction and therefore was persuasive in the same vein as a social network may be with gathering participant information.

6. Conclusions and Further Work

This paper has presented the results of an experiment based on the Perceived Control aspect of the Theory of Planned Behaviour and explored a means of including the idea of privacy as part of the interaction with social networks. This treatment aimed to introduce privacy into the goal of interaction in attempt to provide a solution to privacy as a secondary goal problem by making the identification of sensitive information more salient and the impact of control over that information more obvious. Participants in the treatment group did disclose less than the control and this disclosure was specifically reduced in the more sensitive categories of questions. Such a dynamic score could be added to real social networks through browser extensions or the use of API's to aid users in the use of such systems. However, the extent to which participant enacted their privacy preferences is unclear due to the potential persuasion the treatment may have introduced; that is, privacy may have become the *primary* goal of interaction and other goals may have suffered.

This experiment does show that one form of salience can be particularly effective in persuading users at the point of interaction through dynamic UI elements that instantly show the tangible effect of an interaction. However, the experiments took place in a controlled context and as such do not model the real world setting of privacy and social network behaviour. Hence, participants may have acted according to the perceived aim of the experiment explaining the extensive reduction in the more sensitive data categories. In order to verify the results here the UI elements should be placed in a real world setting to examine the potential effects in an actual context. For example, in Facebook, participants may disclose due their own pre-defined goals rather than goals defined by the system (account creation, reduce Privacy Score etc.). Would such UI elements influence these more personal goals?

Ultimately, this experiment has examined if privacy can be made a salient goal of interaction in an attempt to tackle the potential secondary goal problem it has. The treatment designed here placed privacy squarely into the interactive experience of the participant and made it a clear, tangible goal of system use. UI elements described demonstrate how privacy goals can be made to be a more persuasive part of end-user needs.

7. References

Acquisti, A. and R. Gross (2006). "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Proceedings of the 6th Workshop on Privacy Enhancing Technologies.

Ajzen, I. (1991). "The Theory of Planned Behaviour." Organizational Behaviour and Human Decision Processes 50: 179-211.

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

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

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

Debatin, B., J. P. Lovejoy, A. K. Horn and B. N. Hughes (2009). "Facebook and online privacy: Attitudes, behaviors, and unintended consequences." Journal of Computer-Mediated Communication 15(1): 83-108.

Fogg, B. J. (2003). Persuasive Technology: Using Computers to Change what We Think and Do. San Francisco, Morgan Kaufmann.

Fogg, B. J. (2009). The Behaviour Grid: 35 Ways Behaviour Can Change. PERSUASIVE. Clairemont, California.

Fogg, B. J. and D. Iizawa (2008). Online Persuasion in Facebook and Mixi: A Cross-Cultural Comparison. PERSUASIVE. O.-K. *e. al*. Berlin: 35-46.

Houghton, D. J. and A. Joinson (2010). "Privacy, Social Network Sites, and Social Relations." Journal of Technology in Human Services 28(1-2): 74-94.

Jacko, J. A. and A. Sears (2003). The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications Mahwah, NJ, USA, Lawrence Erlbaum and Associates.

Knijnenburg, B. P., A. Kobsa and H. Jin (2013). "Dimensionality of information disclosure behavior." International Journal of Human-Computer Studies 71(12): 1144-1162.

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

Lew, L., T. Nguyen, S. Messing and S. Westwood (2011). "Of Course I Wouldn't Do That in Real Life: Advancing the Arguments for Increasing Realism in HCI Experiments." Computer Human Interaction.

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(3): 393-411.

Masiello, B. (2009). "Deconstructing the Privacy Experience." IEEE Security and Privacy 7(4): 68-70.

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

Portes, A. (1998). "Social Capital: Its Origins and Applications in Modern Sociology." Annu. Rev. Sociol. 24: 1-24.

Rosenblum, D. (2007). "What Anyone Can Know: The Privacy Risks of Social Networking." IEEE Security and Privacy 5(3): 40-49.

Strater, K. and H. R. Lipford (2008). Strategies and Struggles with Privacy in an Online Social Networking Community. Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, British Computing Society.

Tamir, D. I. and J. P. Mitchell (2012). "Disclosing information about the self is intrinsically rewarding." Proceedings of the National Academy of Sciences 109(21): 8038-8043.