Spring 3-27-2012

# A Cross-Disciplined Approach to Exploring the Privacy Paradox: Explaining Disclosure Behaviour Using the Theory of Planned Behaviour

Thomas Hughes Roberts
*University of Salford*, t.hughes-roberts@edu.salford.ac.uk

## Recommended Citation

Roberts, Thomas Hughes, "A Cross-Disciplined Approach to Exploring the Privacy Paradox: Explaining Disclosure Behaviour Using the Theory of Planned Behaviour" (2012). *UK Academy for Information Systems Conference Proceedings 2012*. 7.
http://aisel.aisnet.org/ukais2012/7

# A Cross-Disciplined Approach to Exploring the Privacy Paradox: Explaining Disclosure Behaviour Using the Theory of Planned Behaviour

## Introduction

The huge rise in the use of the Internet and in particular Social Networking sites, such as Facebook, has brought the issue of personal privacy to the forefront of concern. This privacy problem has been described as “inherently complex, ill-defined and seemingly insolvable” (Ackerman and Cranor 1999);  and due to this it has become “one of the most pressing concerns for research at the moment” (Fang and LeFevre 2010).

One way in which this complexity manifests itself is the privacy paradox which describes a disconnect between users’ stated concern and actual behaviour (Barnes 2006). Research has generally utilised survey instruments to observe this paradox comparing the results of surveys with actual privacy settings and action. This makes pinning a specific reason for the observed behaviour difficult and forces an assumption without any basis in theory or falsifiable evidence; even more so given that privacy is highly dependent upon context and changes over time (Masiello 2009). As such, there is a need for a deeper understanding of the privacy paradox in order to create usable solutions to it; thereby improving end-user security in social networks and other web services.

At the time of writing literature explaining the behaviour observed in the paradox is sparse; although several attempts to detail what the causes might be which shall be examined later. Indeed, there is a growing demand for research which uses formal experimental methods to study privacy on the web (Preibusch 2010) as technology has created privacy issues which fall beyond the bounds traditional analysis and a deeper understanding is now required to go forward (Paine, Reips et al. 2006). This is important as behaviour is a response to a certain stimulus and in order to understand how certain behaviours occur, that relationship needs to be understood by carefully controlling the stimulus and observing the resultant behaviour (McGuigan 1997). However, any experimental approach requires a proven theory from which the experiments can be controlled and effective conditions accurately modelled; as yet the field lacks a clear conceptualization which can be used to dynamically measure behaviour and the reasons for it.

This paper, then, proposes that the behaviour evident in web-based services can be modelled using psychological behavioural theory and, indeed, can provide an experimental basis for explaining why it happens. This model will be vital for designing and conducting experiments and also analysing pre-existing data in a more meaningful way; furthermore, it could provide the basis for designing User Interfaces which encourage pro-privacy behaviour as required (Ackerman and Mainwaring 2005). Therefore, the paper shall take the following structure, a short review of some related work to demonstrate the gap, a look at presumed causes of the privacy paradox in information systems literature, a review of psychology theory which could be applicable and finally, a proposed conceptual model of behaviour and what effects it, which can be applied to the privacy paradox and its uses in future research.

## Related Work

Several papers have made attempts to clarify what might be the cause of the privacy paradox but few have provided a theoretical basis for their assumptions. The closest attempt using theory is the IUIPC model which attempts to model the causes of concern (but not behaviour) (Malhotra, Kim et al. 2004). This used the theory of reasoned action (TRA), to look at what informs a person's level of concern and subsequent behaviour. However, the TRA assumes that behavioural intention is a good indicator of behaviour, but, as the paradox itself shows, this is not always the case. Furthermore, this was not created based on actual behaviour but through an interview process; the Hawthorne effect suggests that the results will be influenced by the participant being actively engaged with the subject matter, tailoring their answers to what they believe the interviewer wants. As such, this model is an interesting exploration of concern but is insufficient in providing a formal experimental method when exploring observable behaviour.

Another attempt where the causes of the paradox are explored is presented by Acquisti *et al*, where a set of seven broad causes are presented; limited information, benefits and cost, bounded rationality, psychological distortions, ideology, market behaviour and attitude/behaviour dichotomy (Acquisti and Grossklags 2004). These provide a broad overview of the various potential causes of paradoxical behaviour, but it is unclear how these could be implemented into a formal method of experimentation. The paper also calls for experiments to examine the factors influencing behaviour claiming that there is a requirement for controlled conditions in order to identify behavioural changes accurately. From the causes presented here it is unclear how controlled factors could be defined.

Therefore, in order to perform the needed experiments called for by Preibusch (2010) and Acquisti (2004) there is a need for a grounded, robust framework which provides a formal method to experimentation and analysis of privacy behaviour, that identifies easily controlled and related variables. While work detailed here has contributed to theorising the constituent factors of observed behaviour they cannot be utilised in an experimental fashion as they are. What is required is a grounded theory which has been empirically tested and is capable of providing robust and accurate results. As such the following section shall show the trends in predicted causes from privacy research followed by a proposed model for implementing formal experimentation.

## Assumed Causes of the Privacy Paradox

The following literature review of privacy research shall show what the assumed causes are of the privacy paradox with the main aim being one of clarification in an attempt to bring some order to the research available at the time of writing.

First, from a technical point of view, web services themselves encourage through accident or design negative privacy behaviour. Acquisti and Gross, note that a social networks are engineered to promote network access from participants and accelerate market growth through increased social contact (Acquisti and Gross 2006). But how is this achieved? Users seem to have unprecedented control over their information down to individual data items, but it would seem that the resulting complexity is what promotes increased openness.

Indeed, complexity seems to be a significant factor surrounding the privacy problem in general. The complexity issues surrounding privacy and user interfaces make it difficult for users to navigate around them (John, Acquisti et al. 2009). It should be noted that a further paradox has been observed where the more control the user has, the more likely they are to publish and disclose sensitive information (Bandimarte, Acquisti et al. 2010). This complexity is also influenced through context; data items which are harmless may not be so when the context shifts. Users are required to be aware of this to be able to plan for it (Stutzman and Kramer-Duffield 2010).

Continuing with the theme of complexity; as mentioned earlier privacy itself suffers from a variety of meanings sowing confusion and complexity as to what privacy is to any one person (Paine, Reips et al. 2006). From this it be logical to assume that users know they should be worried about privacy but are unsure what this means in relation to themselves; this can be attributed to increased media attention (Norberg, Horne et al. 2007) creating a concern for privacy but little information on the solutions.

This brings us onto the second area of causes that contribute to the privacy paradox; the end-users and the socio-technical aspect of systems. The area of security research has long since identified users as the “weakest link” in the security chain (Sasse, Brostoff et al. 2001) where no matter the technological brilliance of the software the end-users will provide the fault in security. This problem can be said to be exacerbated in systems which are designed for openness (such as social network systems) and indeed as the antithesis to the idea of privacy (Livingstone 2008).

This, again, is a theme which runs throughout literature discussing privacy; Kolter, *et al*, blame inexperienced users for failing privacy (Kolter and Pernul 2009) as they do not know how to set privacy preferences which reflect what they desire. Several other sources agree with this pointing out that users do not know what action is available nor do they understand privacy mechanisms which are in place (Paine, Reips et al. 2006; Livingstone 2008).

These points come down to a general lack of awareness and understanding from end-users in social network systems which can lead to inappropriate disclosure and even material harm (Bonneau, Anderson et al. 2009). However, what is the psychology behind this? Why do users disclose information in an online system which they may not necessarily do on the street? Can a solution be found in theory which explains behaviour from a grounded psychological point of view?

The waters are still muddied in terms of research in privacy from a purely information security perspective. The range of causes provided in literature is varied and the above is an effort to bring them together to clarify the research field in some way. The general theme behind them seems to be one of awareness on behalf of the user and encouraging user interfaces from the system. Both of these may be true but is there a theoretical foundation explaining this paradox within psychological behavioural theory? For example, the control paradox, where users give out more information based on increased control, cannot so easily be explained through a lack of awareness alone as it is not clear what awareness is being referred to; solutions or issues or both. While either can be said to be true this is unsatisfactory in providing a clear cut reason for such behaviour.

Furthermore, if solutions are to be found we do not simply need to know the potential causes of the paradox but to explicitly know the effect of these causes on each other, and in relation to behaviour i.e. how can we influence privacy behaviour positively through tackling those causes? The only way to answer this question is to examine behavioural theory for potential reasons behind the privacy paradox to better understand *precisely* why users make the decisions they make. The following then, shows the proposed theories to be introduced to the field in an effort to tackle the problems outlined thus far in the paper and to provide an already robust and tested method to experiment design and analysis.

## Behavioural Theory

Mentioned earlier in reference to the IUIPC model was the Theory of Reasoned Action (Ajzen and Fishbein 1980). This theory seems well-suited to explaining behaviour in social networks at first glance; that a combination of attitude and social expectation leads to intention and ultimately behaviour. However, criticisms of the theory directly relate to the privacy paradox and, indeed, highlight a possible problem with approaches to studying the paradox so far. The most prominent of these is the implicit assumption that concern and behavioural intention are valid indicators of actual behaviour, while the presence of choice can also significantly affect the outcome (Sheppard, Hartwick et al. 1988).

### Theory of Planned Behaviour

In response to these criticisms the TRA was expanded to the Theory of Planned Behaviour (TPB) to take into account control beliefs about the facilitation of performing certain behaviour (*fig. 2*) (Ajzen 1991).

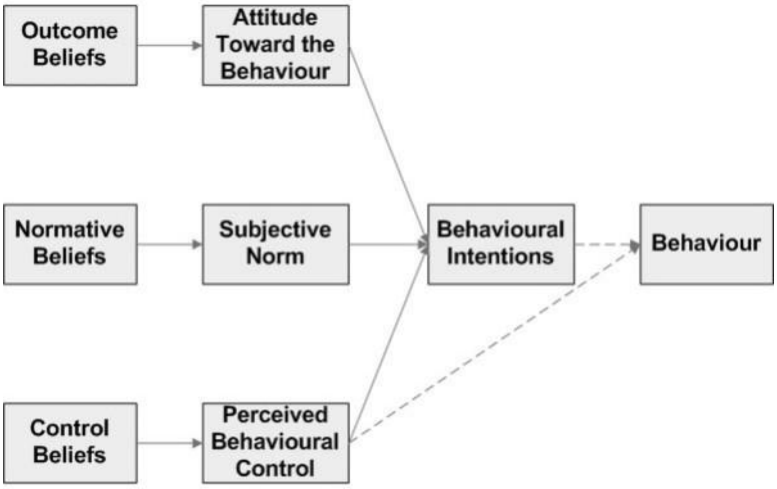


*Fig 1 - Theory of Planned Behaviour* (Ajzen 1991)

These control beliefs pertain to factors which may aid or hinder the ability to perform action and is closely related to the idea of self-efficacy; that is, a person's own conviction about the knowledge they possess in accomplishing a certain task. This is now combined with subjective norms and personal beliefs as in the TRA, while control beliefs inform intention, how easy the subject believes an action to be and behaviour directly if that does or does not turn out to be the case. It is this, the model proposes, that creates a behavioural disconnect from intention or personal attitude/concern; the perceived control over performing that action. Marketing campaigns, for example, that focus only on the information dissemination alone typically have less success than those which promote the ease of controls and improve attitudes (Martiskainen 2007).

Immediately, this model is much more relatable to the behaviour observed in social networks systems regarding privacy. Users hold their own attitudes formed from knowledge of behavioural consequences, influence from the media and those around them and finally, the knowledge of how to perform that behaviour. Furthermore, the TPB has a solid and tested background in psychological experimentation as it robustly identifies the determinant factors of behaviour and shows how they relate to each other (Tonglet, Phillips et al. 2004). This then is a good place to start exploring the behaviour observed in the privacy paradox with a view to developing controlled experiments and analytical tools.

In order to re-enforce the point of control as an important and necessary factor, Signal Detection Theory is another behavioural theory which demonstrates that the noisier an environment is (more complex) then the less likely people are to make a correctly informed decision (Tanner, Wilson et al. 1954). For example, the increased amount of variables and complex nature of a social network make it difficult to know exactly who is going to see what, when and how. SDT's component parts include information acquisition (more knowledge), criterion (judging against what), internal and external noise and internal response (Heeger 1998). Again this gives a partial explanation to the privacy control paradox mentioned earlier.

This shows that increased complexity hinders the ability to make correct decisions and environments which are inherently noisy can increase the amount of incorrect judgements being made. It has already been stated that privacy is complex and combined with a system designed to be open in order to facilitate all the complexities of real world social relationships (Lipford, Besmer et al. 2008) it is immediately obvious that there is the potential for signal noise to be very high. Thus both these theories seem to point to the complexity of the environment combined with certain other factors as being causes of differences between intention and actual behaviour.

## Concept Map for Experimentation

From these two theories and the review of literature performed identifying the assumed causes of the paradox, a final model which satisfies the needs of both an experimental basis and analytical tool can be produced. Thus, by combining the above points together the following theoretical model can be inferred;

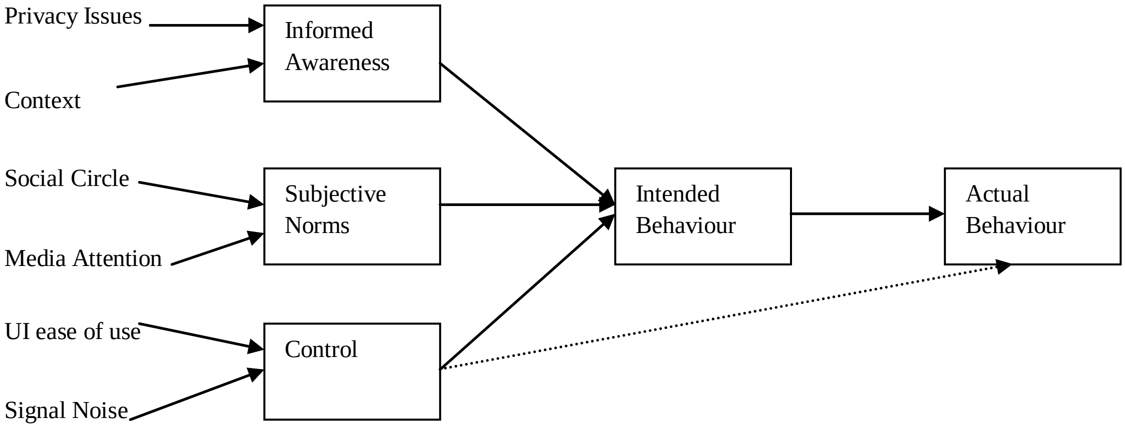


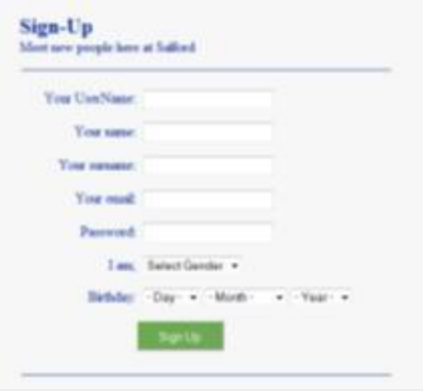
*Fig. 2* – The privacy paradox determinant factors

Here then, we have three beliefs which influence a user's decision to disclose information about themselves. The first of these, informed awareness, details the attitude of the user and knowledge of consequences i.e. are they concerned about privacy and how skilled/knowledgeable are the with regards to it. The second, subjective norms, is concerned with the influence other have over disclosure behaviour, e.g. the media has made us concerned (Norberg, Horne et al. 2007) or our social circles disclose a lot of information which makes it acceptable. Finally, control, applies to how easy it is to identify sensitive information within the context of the system. Social Network Systems (SNS's) are designed to be open and to gather data which can make it difficult to decide what information to give it and how to protect that information. Users may believe this to be extremely easy yet their behaviour would show this to not be the case. Furthermore, SDT demonstrates that increased complexity and choice hinders our ability to identify the correct decisions to make; as observed by Bandimarte (2010) more options can lead to increased disclosure. This research proposes this model to explain why this phenomenon occurs.

**Using the Model for Experimentation**

The above identified beliefs have been labelled salient beliefs (Ajzen 1991) where these form the basis for any behavioural action and are required to be embedded into the environment in which the behaviour is taking place in order to effectively inform it. Recent research and articles from privacy commentators have suggested a lack of salient beliefs as being a cause of unintended privacy disclosure (Schneier 2009) (Tsai 2009). Yet these articles do not mention what these salient beliefs are, indeed, to the best of knowledge these beliefs have been clearly outlined or defined and introduced to the research field. As such this paper presents a model in which these beliefs are clarified and introduced.

With this model now described experiments can be designed to effectively guide the testing of the effects of salience directly on disclosure in a sound falsifiable manner. This research proposes to examine the effect of the properties using four experiments in total; one for each of the salient beliefs and one control group (*fig.3*). Users shall follow a sign-up process to a new social network system which asks a variety of questions in order to build a profile. The level of disclosure shall be measured between groups where it is hypothesised that groups with salient factors shall exhibit less disclosure than the control.

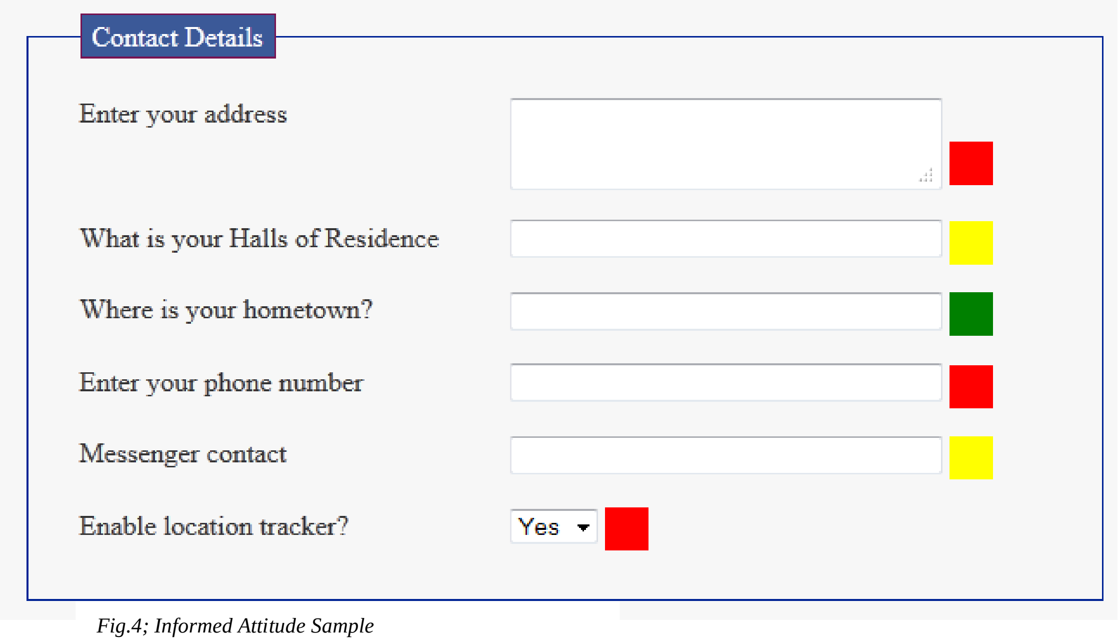


Sign-Up
Meet new people here at Salford

Your UserName:
Your name:
Your surname:
Your email:
Password:
I am: Select Gender
Birthday: - Day - - Month - - Year -

*Fig. 3; First screen of experiments*

These salient properties can be introduced in the following was; for informed awareness, where the goal is to inform of consequences, a “traffic light” systems shall be used to categorise data into groups of consequences if they are disclosed. These categories would include legal (a breach of the law); policy (negative impact on work of school) and social (directed marketing and other annoyances). As seen in *fig. 4;*

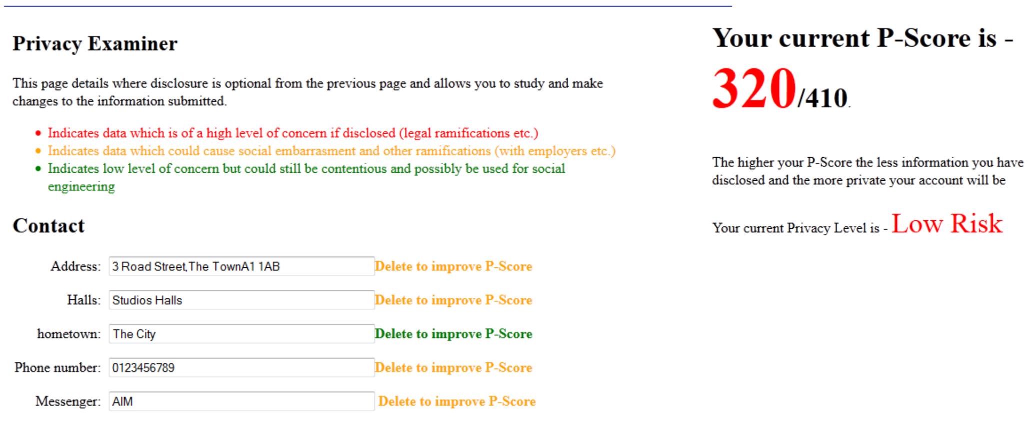


Contact Details

| | | |
|---|---|---|
| Enter your address | | 🟥 |
| What is your Halls of Residence | | 🟨 |
| Where is your hometown? | | 🟩 |
| Enter your phone number | | 🟥 |
| Messenger contact | | 🟨 |
| Enable location tracker? | Yes | 🟥 |

*Fig.4; Informed Attitude Sample*

For perceived control; the difficulty lies not in the act of disclosing data, but in choosing what data to disclose, i.e. users believe that identifying sensitive information is easy but this may not be the case. As such this group will have the ability to review their data, out of the context of the social network and make changes; see *fig.5;*



**Privacy Examiner**

This page details where disclosure is optional from the previous page and allows you to study and make changes to the information submitted.

- Indicates data which is of a high level of concern if disclosed (legal ramifications etc.)
- Indicates data which could cause social embarrasment and other ramifications (with employers etc.)
- Indicates low level of concern but could still be contentious and possibly be used for social engineering

**Contact**

| | | |
|---|---|---|
| Address: | 3 Road Street,The TownA1 1AB | Delete to improve P-Score |
| Halls: | Studios Halls | Delete to improve P-Score |
| hometown: | The City | Delete to improve P-Score |
| Phone number: | 0123456789 | Delete to improve P-Score |
| Messenger: | AIM | Delete to improve P-Score |

**Your current P-Score is -**

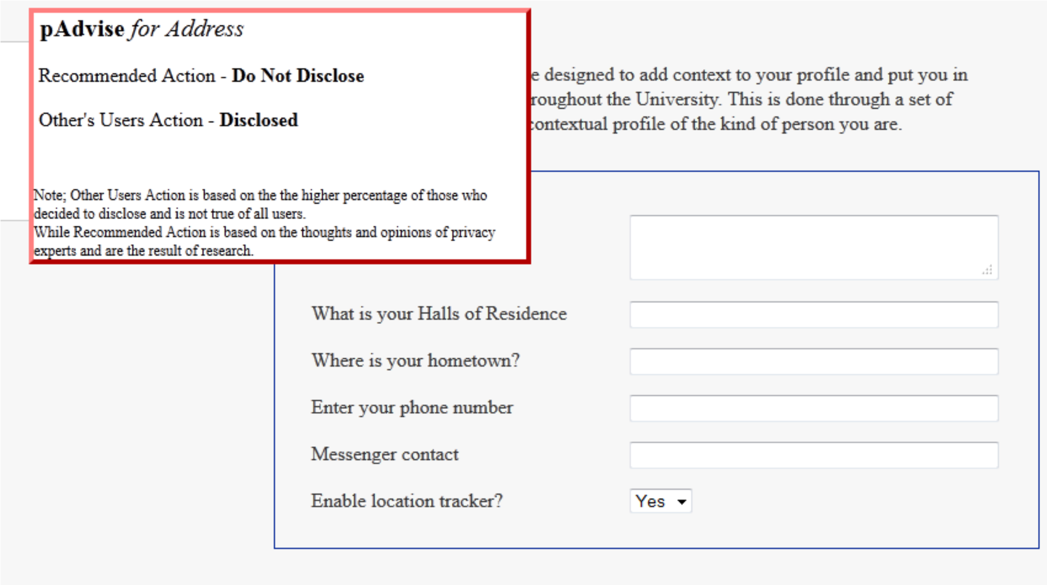
**320/410**.

The higher your P-Score the less information you have disclosed and the more private your account will be

Your current Privacy Level is - Low Risk

*Fig.5; Greater degree of control in isolating sensitive data*

Finally, the subjective norms groups shall have a tutoring system embedded which offers advice based on an expert opinion and the general consensus from the user base, i.e. two sets of advice; one from an expert and one from what the majority of other people do. The experiment could then measure what is more influential in disclosing information; see *fig.6;*



**pAdvise** *for Address*

Recommended Action - **Do Not Disclose**

Other's Users Action - **Disclosed**

Note; Other Users Action is based on the the higher percentage of those who decided to disclose and is not true of all users.
While Recommended Action is based on the thoughts and opinions of privacy experts and are the result of research.

e designed to add context to your profile and put you in
roughout the University. This is done through a set of
contextual profile of the kind of person you are.

What is your Halls of Residence

Where is your hometown?

Enter your phone number

Messenger contact

Enable location tracker? Yes

*Fig.6; Subjective advice offered.*

## Hypotheses

The following sets of hypotheses describe specifically what the experiments shall test;

1. That each group with embedded beliefs will exhibit less disclosure than the control.
2. That each group will exhibit stricter privacy controls over their information from the control group.
3. The Perceived control shall exhibit the most significant difference from the control and other groups as the data is being taken completely out of the context of the social network.

As well as these hypotheses, this method of exploring disclosure behaviour (through an informed model) shall allow research to closely study the effect of salient information on behaviour and have falsifiable evidence of the extent of the effect.

## Conclusion and Future Work

Literature has shown that the complexity of privacy is one which causes paradoxical behaviour when translated into an online environment. In order to understand this behaviour research has identified the need for formal methods of experimentation in order to reliable understand that behaviour in relation to its stimulus. In order to accomplish this, a theoretical basis is required which will guide the design and analysis of the experiments. This paper has proposed that the Theory of Planned Behaviour can be tailored to provide just such a model and is particularly effective due to its relevance and robust implementations in producing falsifiable experiments.

Future work shall include conducting these experiments. Through this research, not only will a greater understanding of the nature of disclosure at the point of the behavioural action be gained, but also the potential causes of the privacy paradox can be highlighted.

Furthermore, the design of the model to demonstrate salient beliefs makes it a particular effective basis for identifying and introducing those beliefs into a user interface in order to prevent the disconnect between concern/intention and actual behaviour. As such, it remains in the interests of future research to implement the model in just such a way as described here performing experiments on the effects of specifically designed privacy tutors on behaviour.

## References

Ackerman, M. S. and L. Cranor (1999). "Privacy Critics: UI Components to Safeguard Users' Privacy." Conference on Human Factors in Computing Systems: 258-259.

Ackerman, M. S. and S. D. Mainwaring (2005). Privacy Issues and Human-Computer Interaction. In L. Cranor & S. Garfinkel Security and Usability: Designing Secure Systems That People Can Use. L. Cranor and S. Garfinkel. Sebastopol, CA, O'Reilly**:** 381-400.

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.

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

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

Ajzen, I. and M. Fishbein (1980). Understanding Attitudes and Predicting Social Behaviour. Englewood Cliffs, NJ, Prentice Hall.

Bandimarte, M., A. Acquisti, et al. (2010). Misplaced Confidences: Privacy and the Control Paradox. Workshop on the Economics of Information Security, Harvard.

Barnes, S. B. (2006). "A Privacy Paradox: Social Networking in the United States." First Monday **11**(9).

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

Fang, L. and K. LeFevre (2010). "Privacy Wizards for Social Networking Sites." World Wide Web Conference.

Heeger, D. (1998). Signal Detection Theory. California.

John, L. K., A. Acquisti, et al. (2009). The Best of Strangers: Context Dependent Willingness to Divulge Personal Information. The Best of Strangers. Pittsburgh, Carnegie Mellon-University.

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

Lipford, H. R., A. Besmer, et al. (2008). "Understanding Privacy Settings in Facebook with an Audience View." Proceedings of the 1st Conference on Usability, Psychology, and Security

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.

Malhotra, N. K., S. S. Kim, et al. (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." Information Systems Research **15**(4): 336-355.

Martiskainen, M. (2007). Affecting Consumer Behaviour on Energy Demand. SPRU - Science and Technology Policy Research. Sussex, University of Sussex.

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

McGuigan (1997). Experimental Psychology: Methods of Researcg. Eastbourne, Prentice-Hall Inc.

Norberg, P. A., D. R. Horne, et al. (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours." The Journal of Consumer Affairs **41**(1): 100-126.

Paine, C., U.-D. Reips, et al. (2006). "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'." Information Systems Research **15**(4).

Preibusch, S. (2010). "Experiments and formal methods for privacy research." Privacy and Usability Method pow-wow.

Sasse, M. A., S. Brostoff, et al. (2001). "Transforming the 'Weakest Link' - a human/computer interaction approach to usable and effective security " BT Technology Journal **19**(3): 122-131.

Schneier, B. (2009). "Privacy Salience and Social Networking Sites." Schneier on Security - A blog covering security and security technology Retrieved July 16, 2009, from http://www.schneier.com/blog/archives/2009/07/privacy_salienc.html.

Sheppard, B. H., J. Hartwick, et al. (1988). "The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research." Journal of Consumer Research **15**: 325-343.

Stutzman, F. and J. Kramer-Duffield (2010). "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook." Computer Human Interaction.

Tanner, J., P. Wilson, et al. (1954). "A decision-making theory of visual detection " Psychological Review **61**(6): 401-409.

Tonglet, M., P. S. Phillips, et al. (2004). "Using the Theory of Planned Behaviour to Investigate the Determinants of Recycling Behaviour: a Casue Study from Brixworth, UK." Resources, Conservation and Recycling **41**: 191-214.

Tsai, J. Y. (2009). The Impact of Salient Privacy Information on Decision-Making. Carnegie Institute of Technology. Pittsburgh, Carnegie Mellon University. **Doctor of Philosophy in Engineering and Public Policy:** 319.