Privacy and Trust: The role of situational and dispositional variables in online disclosure

Adam N. Joinson[1], Carina Paine[1], Ulf-Dietrich Reips[2] and Tom Buchanan[3]

[1]Institute of Educational Technology, The Open University, Milton Keynes, UK, MK7 6AA
{A.N.Joinson, C.B.Paine}@open.ac.uk
[2]Department of Psychology, University of Zurich
u.reips@psychologie.unizh.ch
[3]Department of Psychology, University of Westminster, Regent Street, London, WC1.
buchant@westminster.ac.uk

Abstract. Ambient technologies require users to make fine-grained judgments regarding the privacy of their personal information. In the present paper, we discuss potential patterns that link privacy concerns, perceived privacy and trust in the disclosure of personal information online. A sample of 759 participants completed measures of privacy concern at Time 1, and perceived privacy, trust and disclosure at Time 2. Regression analyses and structural equation modeling showed independent effects for dispositional privacy concerns and situational variables (perceived privacy and trust). The results are discussed in light of the likely privacy requirements for ambient identity technologies. The privacy scales developed are made available for free use in privacy related projects.

1 Introduction

The use of new technology, and particularly the Internet, increasingly requires people to disclose personal information online for various reasons (e.g. to establish their identity, for marketing purposes or for personalization). In addition to this increased need for disclosure, the development of ambient and ubiquitous technologies has raised the possibility that devices will communicate, or even broadcast, personal information without recourse to the user themselves. This can include location-based information or authentication / identity data.

These technological developments have raised a number of privacy concerns. The disquiet surrounding Identity cards in the UK, Total Information Awareness in the US, and radio frequency identification tags (RFID) globally, suggest that negotiating such a balance will be difficult. The use of many e-society services will demand that people make fine-grained judgements regarding the balance between their privacy concerns and the need to disclose personal information.

However, relatively little is known about how people make decisions about when to disclose personal information, and when to conceal it. A number of possible variables have been highlighted, including privacy and trust [1]. To examine privacy first, it is

usually argued that people have a level of privacy concern [2] that varies across individuals. In this context, concern for privacy is a subjective measure—one that varies from individual to individual based on that person's own perceptions and values. In other words, different people have different levels of concern about their own privacy. One scheme for categorizing the different levels of privacy concerns is the Westin privacy segmentation [3]. This divides respondents into one of three categories depending on their answers to three statements. The three categories of respondents are: *The Privacy Fundamentalists* who privacy as an especially high value which they feel very strongly about; *The Privacy Pragmatists* also have strong feelings about privacy. They weigh the value to them and society of providing personal information; *The Privacy Unconcerned* have no real concerns about privacy. Westin [3] reports that 87% of Internet users are 'concerned' about threats to their privacy while online, with 56% being 'very concerned'; others have reported 70% of American consumers worry about online privacy [4].

Alongside people's general privacy concerns and attitudes, it is also important to take into account the specific context of an interaction. We do not simply choose to adopt a privacy-disclosure strategy and stick with it – instead, how we regulate the disclosure of personal information is based on the dynamics of an ongoing interaction [5]. Within the context of human-computer interaction, this dynamic will include aspects such as the costs and benefits of disclosure, trust and perceived anonymity and privacy. Because self-disclosure makes people vulnerable [6], according to [5], disclosure will only occur when personal information will not leak outside of the specific interaction. But, if this is indeed the case, then trust is clearly a critical issue. However, if this vulnerability is reduced (e.g. through anonymity), then the issue of trust may be less important. For instance, people are often willing to disclose personal information to strangers on a train because the ramifications of such revealed vulnerability are lessened [6].

In the present paper, we present a study that examined the links between people's privacy concerns, their perceived privacy and trust in the recipient of the disclosure. We examine a number of potential ways in which these dispositional and situational variables might interact to determine whether or not people disclose personal information to a website. As a practical application, we present measures that can be used in determining visitors' privacy concerns when developing or improving websites and web services.

2 Method

2.1 Participants. Participants were 759 members of an online research panel of Open University (OU) students called 'PRESTO'. The OU is an adult distance learning institution with nearly all students studying part time from home or work. In total 1935 members of the research panel were invited by e-mail to complete the web-based survey (response rate=39%; retention rate=67%). Of the 759 respondents, 64% (487)

were female, 36% (272) were male. The mean age of the sample was 43 years, (range=17–84 years, *SD*=11.11).

2.2 Materials. A set of 16 privacy attitude items and 12 privacy behaviour items developed previously by the authors were used [7]. For all privacy items responses were made on a 5-point scale. In addition, the privacy behaviour items consisted of both 'general caution' items (e.g. reading privacy policies, license agreements etc.) and 'technical protection' items (e.g. removing cookies, clearing internet browser history regularly etc.).

In addition, two existing privacy measures were also included. The first of these measures was the Westin Privacy segmentation [3]. This measure requires that participants respond to three privacy related statements on a four-point scale. On the basis of their responses, participants can be divided into one of the three categories of privacy concern. The second was the Internet Users Information Privacy Concerns (IUIPC; [8]), which requires responses to 10 items on a 7-point scale. Participants were also asked about their internet use (history, breadth of use, and time spent online).

Participants also completed a 16-item measure of behavioural self-disclosure developed by the authors [9]. In this measure, participants respond to a sensitive item such as 'How many different sexual partners have you had?' using one of three options: they could submit the default 'please choose'; disclose the information; or choose an 'I prefer not to say' option. A self-disclosure score was calculated by summing the number of questions disclosed to. A non-disclosure score was calculated by summing the number of items that were either submitted on the default (called 'passive' non-disclosure) or where an 'I prefer not to say' option was chosen (called 'active' non-disclosure). Participants also completed measures of dispositional self-disclosure (10 items from the International Personality Item Pool (IPIP)) and of socially desirable responding (Balanced Inventory of Desirable Responding (BIDR, [10]). At end of the survey respondents' levels of trust and perceived privacy (anonymity and confidentiality) in relation to the survey were measured. For example, they responded on a 5-point scale to items such as "I am sure that my responses will remain confidential".

2.3 Procedure. An invitation to complete the study was sent to panel members by e-mail. At Time 1, members were informed that the survey consisted of a series of questions about any privacy concerns they may have when they use the Internet, and their privacy related behaviour. At Time 2, participants were told that some of the topics covered in the survey might be sensitive, but that it was important for them to respond. The "prefer not to say" option was outlined and they were told that the use of it would not imply any particular response. Times 1 and 2 were conducted six weeks apart to minimize the possible impact of the privacy measures on later disclosure behaviour.

At both time points, participants were informed that all information provided would remain confidential and that they could withdraw from the survey at any stage. For all items participants were prompted to use the full scale when responding and not only

the labeled response options. At the end of each page of the survey participants' responses were submitted.

The survey at Time 1 was left open for two weeks. Participants took, on average, 13 minutes to complete this part of the survey. One month after data collection for Time 1 was complete, an invitation to Time 2 was sent out to the same panel of participants. This survey was also left open for two weeks. Participants took, on average, 13 minutes to complete it.

3. Results

As described, respondents could make one of three responses to the 16 sensitive items (disclosure of information; passive non-disclosure; or active non-disclosure). The mean number of active non-disclosures was 0.45 (SD=1.05, range=0-10). Active non-disclosure was higher, on average, than passive non-disclosure (mean=0.09, SD=0.57, range: 0-13).

A stepwise linear regression was calculated to examine the effect of the various privacy and dispositional variables on non-disclosure. Two further demographic variables – age and gender – were also added to the regression equation. The final model (R^2=.11) incorporated five steps: Trust (ß = -.16), Impression management (ß =. 12), Privacy concerns (ß = .11), gender (ß =.09) and perceived privacy (ß =-.11).

3.3 Structural equation modelling

To further examine the nature of the relationship between situational and dispositional aspects of privacy on behaviour, structural exploratory modeling using the AMOS software program was undertaken to examine a model comprising two independent paths – one comprising situational factors (perceived privacy mediated by trust) and a second dispositional path (privacy concern). Two further models were also tested – the first proposing that the impact of perceived privacy, privacy concerns and personality on privacy behaviour is *mediated* by trust [8, 11]. The second proposed that in addition to this mediation, a separate path exists between privacy concern, past behaviour and privacy behaviour [1].

The comparison of the three models, using goodness of fit indices (GFI), is presented in Table 1. Multiple GFI are used [12]. Specifically, the Chi-squared (X^2) value divided by the degrees of freedom (X^2/DF), the comparative fit index (CFI) and the root mean square error of approximation (RMSEA) were used, alongside the variance explained, to evaluate the models. As a rule of thumb, an adequate model fit to the data would have a CFI of .95 or above, a RMSEA of below .05, and a X^2/DF between 1 and 3. Using the multiple indices in Table 1, model 3 represents the best fit to the data, and can be characterized as a good fit. This model also explained marginally more variance in the dependent variable (non-disclosure) than the other two models.

Table 1: Goodness of Fit (GFI) indices, three models

	Fit indices				
Model	X^2	df	X^2/DF	CFI	RMSEA
Model 1 (Trust as mediator)	41.634	6	6.939	.932	.089
Model 2 (Trust as mediator, path through behaviour)	14.834	5	2.967	.982	.051
Model 3 (Separate path-ways)	5.429	3	1.810	.995	.033

The structural equation model that provided the best fit to the data is shown in Figure 1.

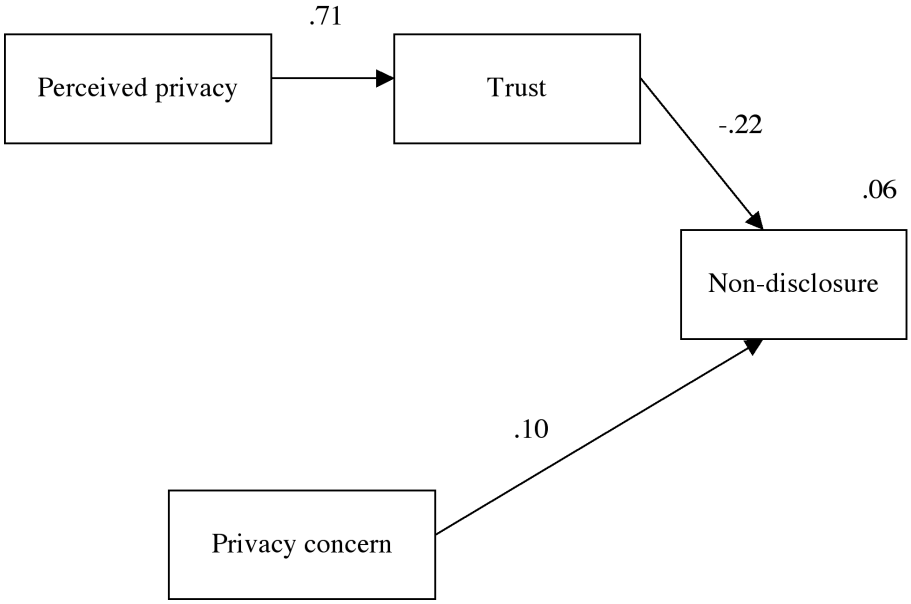

Fig. 1. Independent Situational and Dispositional pathways

4. Discussion

The results of the present paper suggest that both situational and dispositional aspects of privacy influence the decision to disclose personal information. Specifically, two independent paths were identified – one based on the specific aspects of the situation (the context), and one based on people's pre-existing privacy concerns.

With regard to ambient and ubiquitous technologies, the existence of two separate paths is important since it implies that privacy tools need to be designed at two levels within a technology. First, privacy is a *preference* that should be customizable by us-

ers according to their level of general privacy concern. Second, privacy is a *decision* that is influenced by the specific context of a request for personal information. Specifically, these contextual factors (in the present study) were people's perceived privacy (i.e. their anonymity and confidentiality) and the level of trust in the data gatherer. For ambient and pervasive technologies this poses a challenge in that it will not be possible to ask for a human-based decision each time an ambient technology communicates personal information to a third-party. Instead, it is assumed that a combination of identity management systems and agents will negotiate disclosure on people's behalf based on their privacy preferences.

The results of the present study suggest that a single set of privacy preferences embedded with an ambient device would not be sufficient since both preferences (e.g. general privacy concerns) and context-specific attributes (e.g. identifiability and trust) independently influence people's willingness to disclose personal information. We would suggest that future studies examine ways in which identity management systems, privacy preferences and agent-led negotiation can be combined to address privacy concerns in general, and the actual disclosure event specifically, when an individual is faced with the decision of whether or not to disclose personal information.

References

1. Metzger, M.J. (2004) Privacy, trust and disclosure: Exploring barriers to electronic commerce. Available online at http://jcmc.indiana.edu/vol9/issue4/metzger.html. Accessed on 20th June 2005.
2. Westin, A., 1967, *Privacy and Freeom*. New York: Atheneum.
3. Harris and Associates Inc., & Westin, A. (1998). E-commerce and privacy: What net users want. *Privacy and American Business and Pricewaterhouse Coopers LLP*. Retrieved June 20, 2005, from http://www. pandan. org/ecommercesurvey. html.
4. Jupiter Research (2002). *Security and privacy data*. Presentation to the Federal Trade Commission Consumer Information Security Workshop. Retrieved June 20, 2005. from http://www. ftc. gov/bcp/workshops/security/0205201leathern. pdf.
5. Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102-115.
6. Rubin, Z. (1975). Disclosing oneself to a stranger: Reciprocity and its limits. *Journal of Experimental Social Psychology, 11* (3), 233-260.
7. Buchanan, T., Paine, C.B., Joinson, A.N., and Reips, U-R. (in press). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*.
8. Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004) Internet users' Information privacy concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research, 15*, p.336-355.
9. Joinson, A.N., Paine, C.B., Buchanan, T.B., and Reips, U-D. (2006). Development and testing of a behavioral measure of self-disclosure online. Manuscript in preparation.
10. Paulhus, D.L. (1984). Two-component models of socially desirable responding. *Journal of Personality and Social Psychology, 46*, 598-609.
11. Nickel, J., and Schaumburg, H. (2004). Electronic Privacy, Trust and Self-Disclosure in E-Recruitment. In proceedings of CHI 2004, April 24-29, Vienna.
12. Hu, L., Bentler, P.M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives. *Structural Equation Modeling, 6* (1) p1-55.