Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 8th, 2009

"Big Yellow Taxi": The Erosion of Personal Privacy within Social Media

Andrew Boyd, Kaven Williams, Ron Chin, Scott Densten, Diana Diamond, Chris Morgenthaler
Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA

Abstract

Existing constructs for privacy concerns and behaviours do not adequately model deviations between user attitudes and stated user behaviours. While a number of studies have examined supposed deviations from rationality by online users, the true explanations for these stated behaviours may lie in factors not previously addressed in privacy concern constructs. A group of researchers at Pace University created an online survey of privacy attitudes for social media user and our preliminary findings have significant implications for the study of online privacy management. Many studies referenced below have inferred positive correlations among security knowledge, privacy attitude, and privacy intentions. This is not the case for social media, and the reasons underlying this apparent divergence from rationality require closer examination and point us in future directions for privacy research.

1. Introduction

Privacy of personal information continues to be a major concern for most individuals [1][2][3]. When assessed within existing privacy concern models during recent years, information privacy concerns can be seen to be gradually eroding [6][4][3]. Additionally, individual attitudes towards privacy have not historically aligned with privacy behaviours. The roots of this paradox lie far outside the field of computer science. A balance between the personal and the corporate, between the individual and state, and between belief and behaviour, form the core of many academic, political, economic and faith constructs.

The antecedents of an individual's 'sense of self' lie far outside the scope of this study; nonetheless, some of the most striking examples of the gap between privacy attitudes and behaviour have arisen in the past decade as internet technologies have been increasingly adopted by our global society [6][7]. These gaps become particularly acute when we examine the field of social media technologies. As stated by the songwriter Joni Mitchell several decades ago, "You don't know what you've got 'til it's gone." This seems an entirely apropos description of the erosion of online privacy in recent years.

This paper presents preliminary results from an online survey of social media user attitudes and stated behaviours within the context of social networking web sites. Within our survey, we implemented the Internet User Information Privacy Concern construct to determine basic privacy attitudes and make them historically comparable to a range of studies, and then asked questions specific to social media usage [1].

2. Hypothesis Development

After surveying the bibliography of work in this area, and having determined that gaps between privacy attitudes and stated privacy behaviours are not adequately explained by existing constructs, we determined that the Internet User Information Privacy Concern model provided the best 'core' set of questions for our survey requirements [1][2][3][13][15]. IUIPC has been referenced and implemented in over 14 studies, and has achieved relatively wide acceptance.

However, we also wanted to establish a baseline for the stated behaviours of internet users based on a range of demographic co-variants. This would enable us to test demographic co-variants for their impact upon privacy attitudes and stated behaviours towards social media. Accordingly, we constructed a series of questions specifically targeted to personal information disclosure within the context of social networking communities.

These hypotheses and our preliminary findings are outlined in the following summary chart.

Number	Hypothesis	Preliminary Finding
H1	Social media privacy attitudes vary by age.	Supported.
H2	Social media privacy attitudes vary by education.	Supported.
H3	Social media privacy attitudes vary by internet experience.	Not supported.
H4	Social media privacy attitudes do not vary by ethnicity.	Supported.
H5	Social media privacy attitudes do not vary by nationality.	Supported.
H6	Social media privacy attitudes do not vary by gender.	Supported.
H7	Social media privacy attitudes vary by an individual's sense of having been a victim.	Not supported.
H8	Social media privacy attitudes vary by the importance individuals assign to having a large group of online friends.	No supported.
H9	Social media privacy attitudes vary by media exposure to social networking risks.	Not supported.
H10	Social media privacy attitudes vary by online context.	Supported.

A more detailed description of these hypotheses appears in the 'Findings' section of this paper.

The graphic below shows how these additional co-variants relate to the first and second order elements of IUIPC.

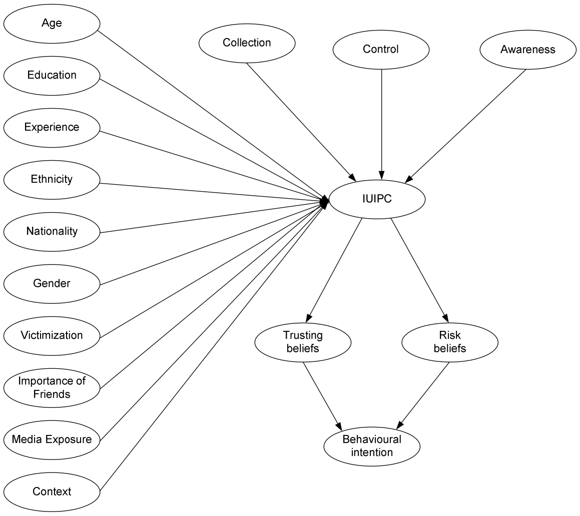

Figure 1: Pace Social Media Survey extension of IUIPC

2.1. IUIPC model

The IUIPC model draws upon Social Contract theory to present a theoretical framework consisting of multidimensional first and second order elements, as well as a series of demographic covariates.

For example, the IUIPC construct states that individual attitudes towards the collection and control of personal information and awareness of information privacy practices constitute a user's IUIPC profile [1]. This individual IUIPC profile influences trusting beliefs and risk beliefs, which in turn have an impact upon behavioral intent.

Demographic co-variants are also related to individual IUIPC profiles [1][9]. A limited number of demographic co-variants were included in the initial version of IUIPC proposed by Malhorta et al, and this study expands that list to include social media specific co-variants. Our hypotheses posit that specific co-variants are correlated to specific privacy attitudes.

3. Methodology

Our research team developed a survey based upon the IUIPC survey questions established by Malhortra et al [1]. Our survey adapted these questions for a social media context, and added a series of questions to establish demographic co-variants for each respondent. Demographic questions utilized the appropriate categories for questions like gender, ethnicity, and age, while IUIPC questions were scored on a seven-point Likert Scale. Responses were collected and tabulated, and statistical analysis is in process.

Our survey was administered through an online survey engine during the months of March and April 2009; the link to the survey was distributed via mass a series of broadcast emails to the Pace University email system by system administrators, email contacts from address books of team members, friends of team members on social network sites, and other friends, family, coworkers, students and classmates.

We first asked a series of baseline questions to establish the demographic co-variants listed in Figure 1 and to determine specific aspects of stated user behaviour such as type of information listed in Social Network Profiles and frequency of social network usage. Users then completed a series of questions asking users what type of information they make available on social network sites such as Facebook, MySpace, LinkedIn and Twitter.

The core IUIPC segment of the survey consisted of three questions about individual privacy concerns for control of personal information on Social Networking Sites, four questions about individual privacy concerns about the collection of personal information by Social Networking Sites, and three questions regarding individual privacy concerns about awareness of information privacy practices.

Data was then collected from the survey engine in the form of individual survey responses, summed data for all responses, and cross-tabulated data for all listed demographic co-variants. This data is being analyzed using chi-square tests for goodness of fit for data, significant statistical variations by demographic co-variant and correlations, or lack thereof, among IUIPC elements.

4. Hypothesis Testing and Findings

Preliminary hypothesis testing and findings were conducted for the ten hypotheses specific to social media usage. Preliminary results appear below.

For this section of the study, we constructed ten hypotheses, based upon established IUIPC hypotheses and hypotheses specific to social media usage.

4.1. Hypothesis 1: Age co-variant

H1: *Social media privacy attitudes vary by age.* Privacy awareness varies by age; younger users are more aware of privacy issues, show similar levels of privacy concern to older users, and also modify their privacy settings more.

4.2. Hypothesis 2: Education co-variant

H2: *Social media privacy attitudes vary by education.* More educated users tend to be less concerned about privacy issues more liberal with online information disclosure.

4.3. Hypothesis 3: Internet Experience co-variant

H3: *Social media privacy attitudes vary by internet experience.*

All respondents to our survey were quite experienced. Within the scale we set, virtually all respondents were highly experienced users.

4.4. Hypothesis 4: Ethnicity co-variant

H4: *Social media privacy attitudes do not vary by ethnicity.*

No significant differences were observed among respondents of varying ethnicities. That said, respondents from western European origins tended to be somewhat more liberal in disclosure of information.

4.5. Hypothesis 5: Nationality co-variant

H5: *Social media privacy attitudes do not vary by nationality***.**

The majority of survey respondents resided in Canada and the United States. At this time, no significant differences are observed between American and Canadian respondents.

4.6. Hypothesis 6: Gender co-variant

H6: *Social media privacy attitudes do not vary by gender***.**

Our survey responses show that women are somewhat more conservative than men in the release of their personal information, but we have not yet established statistical significance for this finding.

4.7. Hypothesis 7: Victimization co-variant

H7: *Social media privacy attitudes vary by sense of having been a victim of privacy invasion.* Respondents who sensed being a victim were in the minority, many respondents were neutral and those who did feel themselves to be the victim of social network abuse were much more conservative in their attitudes.

4.8. Hypothesis 8: Group size co-variant

H8: *Social media privacy attitudes vary by the importance individuals assign to having a larger size in their group of social media friends.* We established no direct correlation between these factors. That said, qualitative comments from respondents indicated that younger users tended to have significantly larger groups of online friends.

4.9. Hypothesis 9: Media exposure co-variant

H9: *The importance of having a large online group of friends varies by social media respondent age.* We established no direct correlation, however, anecdotal evidence from users indicates that younger users tended to have more social network friends.

4.10. Hypothesis 10: Online context co-variant

H10: *Social media privacy attitudes vary by online context.*

Our study notes that, compared to previous studies in online shopping attitudes, social media users are more willing to part with personal information than online shoppers, and—even though their personal information may be a greater risk within the context of social networks.

5. Implications

Our study results indicate a number of trends and differentiations that either mark social media as being different from other online technologies such as e-commerce, or delineate an erosion in online privacy attitudes during recent years.

This paper reports on preliminary findings from our study and suggests possible implications that will be confirmed or denied as we continue to analyze data.

5.1. Leveling of privacy attitudes across age groups

Historical IUIPC studies have denoted greater differences among age groups than those identified within our study [1][3][6][9]. This suggests that privacy attitudes are either aligning across all age groups and contexts, or that privacy attitudes are genuinely different with social media contexts.

5.2. Ambiguities towards trust of social networking sites

At the end of our social media survey, we presented respondents with two scenarios, one of which was a ‘safe friending’ experience, where the respondent knew who originated the user request, and one of which was an ‘unsafe friending experience’, where the respondent did not know who originated the user request. In both scenarios, users were quite neutral about whether they felt their social networking site would use their personal information in a responsible manner.

This suggests that users have not yet established attitudes of trust or distrust towards social media providers; as such, social media trust attitudes can be regarded as a volatile and fluid subject area, that may change significantly in the coming months and years.

5.3. Knowledge, Experience and Comfort lead to increased disclosure

One train of thought in privacy management suggests that more informed users will exhibit greater vigilance in the protection of their personal information [6]. This supposition is not supported by this study. One possible explanation for this observed attitude and behaviour is that more informed social media users have accepted that their personal information has already been compromised, and consequently, they have come to terms with the loss of privacy, and are simply interested in communicating online.

This possible explanation has significant implications for online privacy management, because it may also help explain the gap between individual privacy attitudes and privacy behaviours. A model can be constructed to show that, even though individuals remain concerned about their personal privacy, their recognition that the privacy battle has already been lost helps explain why they behave in a seemingly irrational manner when disclosing personal information.

5.4. The problem of Context

Finally, social media technologies might encourage users to assume they are ‘among friends’, as opposed to being embedded within a commercial transaction. Even though the business models of social networking sites treat each individual social interaction as a transaction that can potentially be commoditized, for the end user, the experience is one of chatting with friends. This contextual determinant may be the single most significant factor in the recent erosion of online privacy behaviours and attitudes.

6. Future Directions for Research

As we continue to statistically analyze the data collected from this survey, additional areas of research may become apparent, however, at this point our areas of interest define themselves as:

1. Examining forces behind the leveling of privacy concerns across age groups.
2. Defining the ambiguities towards trust of social networking sites.
3. Discovering why knowledge, experience and comfort seem, perhaps counter-intuitively, to lead to increased disclosure of personal information.
4. Establish an appropriate role for the influence of context in online interactions, be they 'commercial' or 'social' interactions.

In the coming weeks, we hope to develop an inclusive model that incorporates these new discoveries and updates existing privacy attitude and behavioral models. Drawing upon our solid base of survey response data collected during the months of March and April 2009, and the significant amount of prior work in this field, we hope to create a privacy attitudinal and behavioral construct relevant to a range of online technologies.

References

[1] Malhotra, N., Kim, S., & Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. Information Systems Research, 15, 4 (2004), 336-355.

[2] D. Rosenblum, "What Anyone Can Know: The Privacy Risks of Social Networking Sites," IEEE Security and Privacy, vol. 5, no. 3, pp. 40-49, May/Jun, 2007

[3] Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

[4] Sarner A., Drakos N., Prentice S., "The Business Impact of Social Computing, 2008", Gartner Research, 16, 9, 2008

[5] Mahmood, Siponen, Straub, Rao, "Information Systems Security in a Digital Economy", MIS Quarterly, 1, 7, 2008

[6] Gross, Ralph, Alessandro Acquisti, and H. John Heinz III., "Information Revelation and Privacy in Online Social Networks", Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pp. 71-80, Alexandria, Virginia, 2005.

[7] Haythornthwaite, C., "Social networks and Internet connectivity effects", Information, Communication, & Society, 8 (2), pp.125-147, 2005.

[8] Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.htm l . March 28, 2009

[9] I. Brown T. Zukowski, "Examining the influence of demographic factors on internet users' information privacy concerns", Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, pp. 197–204, Port Elizabeth, South Africa, 2007

[10] A. Korolova, R. Motwani, and S. Nabar, "Link privacy in social networks", Proceeding of the 17th ACM conference on Information and knowledge management, pp. 289-298, Napa Valley, California, 2008

[11] Mahmood, Pahnila, and Siponen, "Employees' Behavior towards IS Secur ity Policy Compliance", Proceedings of the 40th Hawaii International Conference on System Sciences, Hawaii, 2007

[12]Http://www.GoCSI.com

[13] Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J., "An analysis of end user security behaviors", Computers & Security, 24, 2005, 124-133

[14] Ajzen, I., "The Theory of Planned Behavior", Organizational Behavior and Human Decision Processes 50,2, 1991, 179-211.

[15] Limayem, M., and Hirt, S.G., "Force of Habit andInformation Systems Usage: Theory and Initial Validation", Journal of Association for Information Systems, 4, 2003, 65-97.

[16] Aydin, C. E. and Rice, R. E., "Social worlds, individual differences, and implementation. Predicting attitudes toward a medical information system", Information & Management 20, 1991, 119-136.

[17] Deloitte. 2005 2005 Global Security Survey, http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritysurvey_2005-07-21.pdf

[18] Walls, A., “The Business Impact of Social Computing on Data Exposure in the Workplace”, Gartner Research, 5, 9, 2008