2016

Self-Disclosure on Facebook: Comparing two Research Organisations

Kathryn Parsons
Defence Science & Technology Group, kathryn.parsons@dsto.defence.gov.au

Dragana Calic
Defence Science & Technology Group, Dragana.Calic@dsto.defence.gov.au

Carlos Barca
The University of Adelaide, Carlos.Barca@adelaide.edu.au

Self-Disclosure on Facebook: Comparing two Research Organisations

Kathryn Parsons
Defence Science and Technology (DST) Group
Edinburgh, South Australia
Email: Kathryn.Parsons@dsto.defence.gov.au

Dragana Calic
Defence Science and Technology (DST) Group
Edinburgh, South Australia
Email: Dragana.Calic@dsto.defence.gov.au

Carlos Barca
School of Psychology
The University of Adelaide
Adelaide, South Australia
Email: Carlos.Barca@adelaide.edu.au

Abstract

This study investigated why employees self-disclose on Facebook, and whether there is a difference in self-disclosure between employees of an Australian government organisation and an academic institution. We employed quantitative and qualitative approaches, including an online questionnaire of 216 participants and ten interviews. The two organisations were compared on organisational variables, and measures of Privacy Concerns, Privacy Behaviour and Propensity to Trust as potential predictors of self-disclosure. Privacy Behaviour and Propensity to Trust were significant predictors for the government organisation, whereas demographic and organisational factors were the main predictors for the academic institution. Furthermore, qualitative findings revealed that, whilst the government participants focussed on the costs of self-disclosure on Facebook, the academic institution participants focussed on the benefits of self-disclosure. These results provide preliminary support for our online self-disclosure model, and highlight the importance of considering different organisations and populations in studies of online self-disclosure and privacy.

Keywords self-disclosure, privacy behaviour, privacy paradox, social media, Facebook

1 Introduction

Social Media (SM) has attracted large numbers of users worldwide, and has become a significant part of daily routine and social interaction (Fogel & Nehmad, 2009; Wilson, Gosling, & Graham, 2012). Facebook is currently among the most popular SM websites, with over one billion active users (Statistics Brain, 2015). However, with the increase of SM popularity, potential online privacy and security issues have come to the fore (Debatin, Lovejoy, Horn, & Hughes, 2009; Dey, Jelveh, & Ross, 2012). Organisational Reviews of SM have flagged many potential concerns, and recommend cautious use (Arico & Srinivasan, 2014; George Patterson Y&R, 2011; Parsons, McCormac, & Butavicius, 2011). With large amounts of personal information available on SM, users could unintentionally expose themselves, their work colleagues and their organisations to serious risks. These risks may include becoming a victim of phishing, stalking or extortion (Molok, Chang, & Ahmad, 2010). Phishing is a social engineering technique used to trick users into providing private information (Parmar, 2012; Parsons et al., 2015).

It is important to understand how people engage with SM and whether their workplace practices affect how they use SM. Employees of organisations where sensitive information is frequently handled, such as in the defence, security, financial or technology sectors, may be more exposed to cyber threats than other industries (Arico & Srinivasan, 2014). Simply put, we hypothesise that individuals who handle more sensitive information will be more cautious about the information, both personal as well as organisational, that they disclose on Facebook. Hence, this paper examines self-disclosure on Facebook, within two Australian organisations. A government organisation, where employees frequently handle sensitive information, will be compared to an academic institution, where sensitive information is handled less frequently. For the purposes of this paper, sensitive information refers to information such as: intellectual property, financial and classified information and data that could cause damage to an individual, organisation or national interests if it were disclosed to the public.

1.1 Cybersecurity in the Workplace

Cybersecurity involves the measures taken to protect a computer or computer system (Bullock, Haddow, & Coppola, 2013). The threat of cybercrime is ever growing, affecting individuals as well as industry, both private and public, with some estimates proposing a global cost of $1 trillion every year (Lewis & Baker, 2013). The disclosure of personal and organisational information on SM can have a detrimental effect on cybersecurity.

The unintentional disclosure of an organisation's sensitive information through the irresponsible use of SM can lead to potential loss of productivity and can result in significant consequences to an organisation's reputation and future revenue (Molok et al., 2010). A recent report by the Guardian revealed that a number of government departments have unintentionally released confidential information (Ramesh, 2015). For example, Northamptonshire county council accidentally published data on more than 1,400 children, including names, addresses, religion and special educational needs status (Ramesh, 2015). In another case, the Israeli military cancelled an entire operation after one of its military personnel disclosed the location and time of an upcoming raid in their Facebook status update (BBC News, 2010).

Disclosing personal information on SM can also have serious consequences. For example, this information can be used to facilitate spear-phishing. Spear-phishing is a specific type of phishing; whereas standard phishing emails are generic, and sent to many users, spear-phishing emails are highly personalised, and are aimed at, and sent to, specific individuals. Consequently, spear-phishing has been found to be more effective at eliciting information from users (Butavicius, Parsons, Pattinson, & McCormac, 2015; Parmar, 2012). Organisations where employees handle sensitive information, such as in the defence, security, financial or technology sectors, may be more at risk compared to other industries (Arico & Srinivasan, 2014). Accordingly, government departments faced the highest number of spear-phishing attacks (Symantec Corporation, 2014). While stringent security procedures may help to mitigate cyber risks within organisations, little is known about how employees of these organisations behave online.

1.2 Why do People Self-Disclose?

Self-disclosure involves the information that individuals willingly and deliberately reveal about themselves, such as their personal details, photos and experiences (Pearce & Sharp, 1973). For most SM websites, the information disclosed can be made private or public. However, even if a user has a private profile, the general public can usually view some of their details. This has led many to question the privacy and security of SM (e.g., Acquisti & Gross, 2006; Fogel & Nehmad, 2009; Shin, 2010).

Even though most people understand the issues and risks associated with SM, they often continue to disclose personal information (Shin, 2010). This discrepancy between people's privacy concerns and their online behaviour has been described as the privacy paradox (Barnes, 2006; Taddicken, 2014). To date, empirical findings on the privacy paradox have been inconsistent (e.g., Dienlin & Trepte, 2015; Utz, 2009). These inconsistent findings may be at least partially due to different definitions and conceptualisations of privacy concerns and behaviours, and research failing to consider the multidimensional nature of privacy. For example, behaviour could be assessed in regards to the things that people do to protect their privacy (e.g., clearing one's browser history), or the actual information that people disclose online (e.g., disclosing their phone number on Facebook). Previous studies have primarily considered only one of these aspects of behaviour (e.g., Acquisti & Gross, 2006; Ellison, Vitak, Steinfield, Gray, & Lampe, 2011). In this study, we consider both of these forms of online behaviour, the actual information that people self-disclose online as well as the things that people can do to protect this information, to measure self-disclosure within the Facebook specific context.

Adapted from Posey et al. (2010), the exploratory model of online self-disclosure presented in Figure 1 proposes that, when deciding whether to self-disclose, people weigh up the costs and benefits, and this is affected by both social and individual factors. In line with Posey et al. (2010), our model draws on a number of theories, including Social Exchange Theory, Social Penetration Theory, and Communication Privacy Management Theory (Altman & Taylor, 1973; Jarvenpaa & Staples, 2001; Petronio, 2002). However, our approach is exploratory, rather than one of theory verification. This is in line with the recommendation of Karjalainen (2011) who argues that focusing on a single theory may neglect potentially important variables.

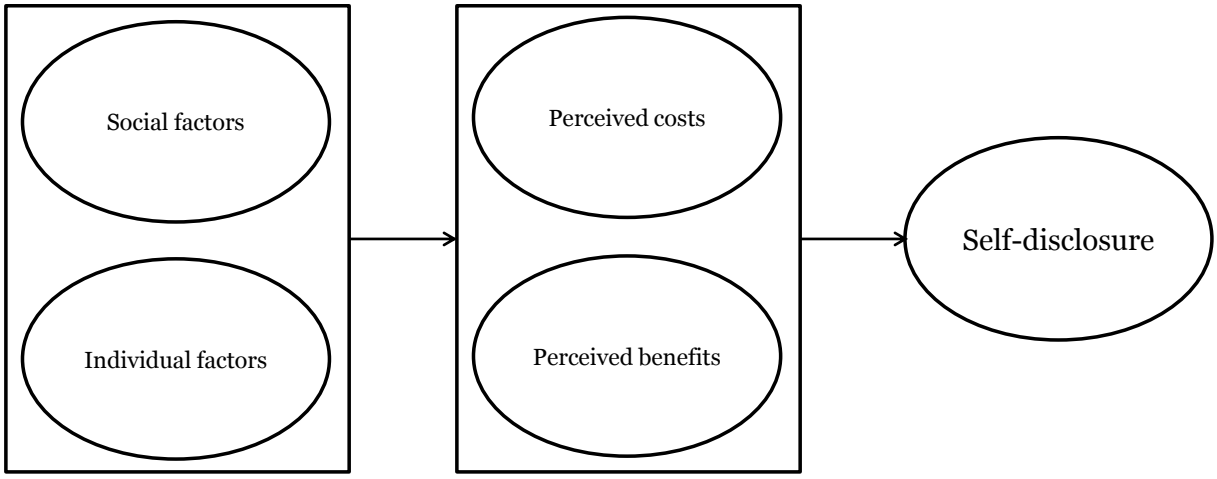

Figure 1: Online self-disclosure model (adapted from Posey et al. (2010))

The individual factors include demographics and personality variables, such as propensity to trust. There is evidence that different genders use different rules when determining whether to disclose (Petronio, 2002). For example, Walrave, Vanwesenbeeck, and Heirman (2012) found that female adolescents were more protective of their online privacy, and Chang and Heo (2014) found that males perceived less risk, and were therefore more likely to self-disclose. Previous research has revealed that trust can predict purchasing and disclosure behaviour (Joinson, Reips, Buchanan, & Schofield, 2010; Metzger, 2006). Trust has also been found to mediate SM behaviours, in terms of how trusting an individual is and the extent to which a particular SM site is perceived as trustworthy (Malhotra, Kim, & Agarwal, 2004; Taddei & Contena, 2013). The frequency and nature of self-disclosure is also influenced by social factors, such as the desire for acceptance (Posey et al., 2010). Essentially, individuals who desire to be more similar to those in their environment are more influenced by the behaviour of others. Cialdini (2009) has referred to this as the principle of social proof. For example, if members of one's social network frequently share photos on their Facebook page, people who are influenced by this principle will be more likely to do the same.

Potential costs of self-disclosure could include exposure to risks that may jeopardise personal safety, or the safety of others (Petronio, 2002). For example, personal information disclosed on SM could be used for malicious purposes. Benefits associated with self-disclosure could include improved well-being, relationship maintenance, emotional support, and exposure to new information (Ellison, Steinfield, & Lampe, 2007; Taddei & Contena, 2013). Also, reciprocity is often described as an

important benefit of self-disclosure, and simply put, is based on the idea that people are more likely to self-disclose if they have been a recipient of such disclosure (Posey et al., 2010).

1.3 Present Study

The primary aim of the present study was to investigate whether there is a difference in self-disclosure on Facebook between employees of a government organisation and an academic institution. A range of organisational variables, privacy related behaviours and attitudes were measured to address the following research question: *Why do employees self-disclose on Facebook?*

2 Method

Using a between-groups design, we employed a dual methodology, incorporating qualitative and quantitative approaches. A total of 216 participants, all Facebook users, completed an online questionnaire. This consisted of 138 participants from the government organisation, and 78 participants from the Academic institution. The age distribution and education level were very similar between the two organisations. However, the gender distribution varied with a predominantly male sample (65%) for the government organisation, and predominantly female sample (71%) for the academic institution. The samples were also similar in their primary function, namely, research, and both organisations have SM policies, and provide training on information and cyber security.

2.1 Measures

The questionnaire was administered during June and July 2014, and took approximately 20 minutes to complete. To evaluate the influence of organisational differences, participants were asked about their organisation's SM policy and their access to sensitive information. Participants were provided with the following practical definition of sensitive information:

> *"Sensitive information refers to information such as: intellectual property, financial and classified information and data that could cause damage to an individual, organisation or national interests if it were disclosed to the public".*

The online questionnaire also included demographic questions, and incorporated the following measures:

The **Privacy Concerns Scale** (Buchanan, Paine, Joinson, & Reips, 2007) measures an individual's concerns in relation to their online privacy. The measure contains 16 items; participants respond to each item on a five-point Likert scale. Higher scores indicate more privacy concerns for Internet related security topics. The Cronbach's alpha coefficient, which is a measure of the reliability of the scale, was .95 in this study.

The **Privacy Behaviour Scale** (Buchanan et al., 2007) focusses on the things that people do to protect their privacy. This measure contains six **General Caution** questions, which assess individuals' general protection behaviours. It also contains six **Technical Protection** questions, which reflect the use of technology to protect privacy. Items are measured on a five-point Likert scale and higher scores indicate more security conscious privacy behaviour. The Cronbach's alpha coefficient for General Caution was .82, and .79 for Technical Protection.

The **Propensity to Trust Scale** (Cheung & Lee, 2006) contains two items, and measures an individual's tendency to trust on a five-point Likert scale. Higher scores indicate a higher tendency to trust. The Cronbach's alpha in this study was .81.

The **Risky Facebook Behaviours Scale** (Appendix A) measures the extent to which individuals engage in risky behaviours on Facebook, which we conceptualise as Facebook self-disclosure. This scale was developed for this study, and contains 12 items. It focusses on actual behaviours that users may engage in, rather than their opinions or attitudes. The scale incorporates items on the specific information that people may disclose on Facebook. These items were chosen to represent the information requested when creating a Facebook profile. The scale also incorporates items on the things that people can do to protect their privacy on Facebook, such as limiting access to their profile by making it private. A higher score indicates more risky Facebook behaviour. To assess its validity, the items were piloted with experienced Facebook users and wording was modified to avoid confusion.

The Cronbach's alpha coefficient in this study was .55. Hair, Black, Babin, Anderson, and Tatham (2006) argued that alpha coefficients close to .60 are acceptable for exploratory research. This level of internal consistency can be expected given the diversity of the psychological construct being measured (Field, 2009). Essentially, the patterns of behaviour associated with how people self-disclose online

may be expected to vary. For example, the scale includes items about specific information that the respondent might share on Facebook, and although it is commonly accepted to disclose your name, it is far less common to share your phone number or personal address.

2.2 Qualitative Component

As part of the online questionnaire, participants were asked the following open-ended question, "What, if anything, do you consider before posting to social media?" Also, on completion of the online questionnaire, participants were invited to take part in a follow-up interview. Brief 15 minute interviews were conducted with five government organisation participants and five academic institution participants. Interview questions focused on reasons for self-disclosure, and an example question included, *"What do you think influences your online behaviour and the information you disclose on the Internet?"* Each interview was conducted with one interviewee and two investigators.

3 Results

The primary aim of this study was to investigate whether there is a difference in self-disclosure on Facebook between employees of a government organisation and an academic institution. First, we compared the two samples on organisational differences that may have affected self-disclosure. A chi-square test was conducted to compare the groups on whether they knew that their organisation had a SM policy. The government participants were significantly more likely to know that their organisation had a SM policy, X^2 (2, N = 216) = 84.92, $p < .001$. Furthermore, an independent samples t-test showed that the government participants (M = 3.68, SD = 1.16) reported handling sensitive information more frequently compared to the academic institution participants (M = 3.00, SD = 1.29), t (214) = 3.98; $p < .001$, d = .56.

We then compared the two samples on a number of potential predictors of self-disclosure on Facebook, namely, Privacy Concerns, General Caution, Technical Protection and Propensity to Trust. We also compared the two samples on the Risky Facebook Behaviours Scale. As shown in Table 1, the samples differed significantly in regards to Technical Protection, Propensity to Trust and Risky Facebook Behaviours. These results suggest that the government participants were more likely to use technical controls to protect their privacy, and less likely to self-disclose on Facebook. Although the academic institution participants scored higher on the Propensity to Trust measure than the government participants, the magnitude of the difference was small.

	Government organisation M (SD)	Academic institution M (SD)	*t*	*p*	*d*
Privacy Concerns	41.72 (11.82)	45.50 (16.67)	-1.94	.054	-.28
General Caution	18.59 (4.53)	17.49 (5.77)	1.56	.120	.22
Technical Protection	21.97 (4.27)	20.00 (5.88)	2.83	.005*	.40
Propensity to Trust	5.33 (1.61)	5.83 (1.96)	-2.06	.041*	-.29
Risky Facebook Behaviours	3.65 (1.42)	5.26 (1.94)	-6.97	.001**	-.99

Table 1. Independent samples t-tests for the government organisation (n = 138) and the academic institution (n = 78)

Given these differences between the two samples, two four-stage hierarchical multiple regressions were conducted (i.e., one for each organisation) to determine which of the measured variables may predict participants' self-disclosure on Facebook (see Table 2). Gender and age were entered at stage one of the regression to control for these variables. The organisational variables (i.e., how frequently participants access sensitive information and knowledge of their organisation's SM policy) were entered at stage two. The Privacy Behaviour variables (i.e., General Caution and Technical Protection) were entered at stage three, and Propensity to Trust and Privacy Concerns at stage four.

For the government participants, none of the potential predictor variables in stage one and stage two were significant, accounting for only 3% of the variance in self-disclosure on Facebook. In stage three, however, introducing the Privacy Behaviour variables explained an additional 17% of the variance. In stage four, Propensity to Trust and Privacy Concerns explained an additional 7% of the variance.

Privacy Concerns was not a significant predictor, but Propensity to Trust was the most important predictor overall. Together, the eight independent variables accounted for 27% of the variance in self-disclosure on Facebook for the government participants.

A very different pattern of results was found using the same hierarchical multiple regression model for the academic institution. Unlike the government organisation, the main predictors for the academic institution were demographic and organisational variables. Both gender and age were significant at stage one, accounting for 10% of the variance. At stage two, the organisational variables accounted for an additional 7% of the variance. The variables introduced in stages three and four explained only an additional 2%, but overall, the model explained 19% of the variance. Gender and knowledge of SM policy were the most important predictors of the variance in self-disclosure on Facebook for academic institution participants.

	Government Organisation		Academic Institution	
Variable	β	*t*	β	*t*
Step 1	$F_{(2, 135)} = 2.02$, $R^2 = .03$^		$F(2, 75) = 4.14$, $R^2 = .10$*	
Gender (Female = 2)	-.06	-.73	-.28	*-2.44**
Age	-.16	-1.90	-.25	*-2.18**
Step 2	$\Delta F_{(4, 133)} = 1.10$, $R^2 = .03$^		$\Delta F_{(4, 73)} = 3.74$, $R^2 = .17$*	
Gender	-.08	-.86	-.26	*-2.32**
Age	-.15	-1.78	-.21	-1.89
Frequency sensitive information	-.03	-.38	-.14	-1.30
Knowledge of SM policy+	.04	.48	.23	*2.12**
Step 3	$\Delta F_{(6, 131)} = 5.46$, $R^2 = .20$**		$\Delta F_{(6, 71)} = 2.61$, $R^2 = .18$*	
Gender	-.07	-.84	-.27	*-2.33**
Age	-.07	-.79	-.14	-1.66
Frequency sensitive information	.04	.49	-.14	-1.28
Knowledge of SM policy	-.01	-.06	.23	*2.09**
General Caution	-.25	*-2.75**	-.13	-.89
Technical Protection	-.27	*-3.14**	.03	.24
Step 4	$\Delta F_{(8, 129)} = 5.80$, $R^2 = .27$**		$\Delta F_{(8, 69)} = 2.02$, $R^2 = .19$^	
Gender	-.08	-1.01	-.27	*-2.32**
Age	-.08	-1.02	-.19	-1.56
Frequency sensitive information	.03	.33	-.14	-1.28
Knowledge of SM policy	.00	.04	.22	*2.03**
General Caution	-.21	*-2.26**	-.17	-1.11
Technical Protection	-.22	*-2.59**	.02	.13
Propensity to Trust	.25	*3.22**	.01	.12
Privacy Concerns	-.07	-.73	.11	.85

* $p < .05$, ** $p < .001$, ^$p > .05$, + No = 2

Table 2. Summary of hierarchical regression analysis for the government organisation and academic institution for variables predicting self-disclosure on Facebook

3.1 Qualitative Component

To further investigate why employees self-disclose on Facebook, we analysed the open-ended responses from the questionnaire and the brief interviews, into thematic categories to describe meaningful patterns and themes in the data (Braun & Clarke, 2006). Participants from both groups frequently discussed how their self-disclosure on Facebook was perceived by those around them. While government participants focussed on the negatives, the academic institution participants were more likely to consider the positive implications.

The negatives that government participants discussed centred primarily on security and professional implications. They often considered the policies of their organisation, as well as concerns for personal security. Hence, their focus was on the perceived costs and privacy risk of self-disclosure on Facebook.

> *"The policy of social media from work … that's always at the back of my mind."*
>
> *"Working here, definitely. You know what you should and should not be disclosing."*
>
> *"Due to privacy and security concerns (both work and personal), I do not post on social media. I only very occasionally access it to view posts from friends and family."*
>
> *"What my security officers might think of my posts. Whether, as a public servant, I'm allowed to express an opinion on the matter."*

In contrast, the academic institution participants focussed on potential positives and the importance of their social image. Respondents typically discussed self-disclosure in terms of value, to themselves and their audience. Overall, the academic institution participants focussed on the perceived benefits associated with self-disclosure on Facebook.

> *"What benefit will I get out of writing what I am writing, if nothing - why am I bothering?"*
>
> *"Whether audience would find it interesting or useful."*
>
> *"Whether the articles I post will be interesting to others (I predominantly post science articles), or engage/begin a dialogue with others."*
>
> *"I always consider the impact [that] this will have on my profile - I am very careful about cultivating a deliberate online profile."*

4 Discussion

In this study, we examined some potential variables that could predict why employees of a government organisation and an academic institution self-disclose on Facebook. This research was motivated by reports that government departments, where employees handle more sensitive information, may be more exposed to cyber threats and were found to be most attacked by spear-phishing compared to other industries (Arico & Srinivasan, 2014; Symantec Corporation, 2014). Hence, sharing both personal and organisational information on Facebook could expose their organisation to cyber threats. In this study, we were particularly interested in the extent to which individuals who work for a government organisation self-disclose on Facebook, and compared them to an academic institution. The study included an online questionnaire completed by 216 participants and follow-up interviews. The potential variables that could predict Facebook self-disclosure differed between the two organisations.

The government organisation and academic institution were compared on several potential predictors of self-disclosure on Facebook. This included organisational variables (i.e., how frequently participants access sensitive information and knowledge of their organisation's SM policy), as well as measures of Privacy Concerns, General Caution, Technical Protection and Propensity to Trust. Government participants were more likely to know that their organisation had a SM policy and they handled sensitive information more frequently compared to the academic institution participants. They were also more likely to implement technical safeguards, and had a lower propensity to trust. The government participants were also less likely to self-disclose on Facebook. These differences between the organisations provided justification for considering the two samples separately in determining why employees self-disclose on Facebook.

4.1 Why Employees Self-Disclose on Facebook?

The qualitative findings clearly show differences in self-disclosure between the two organisations, and these differences can be explained by the online self-disclosure model adapted from Posey et al. (2010). This model proposes that when deciding whether to self-disclose, people weigh up the costs and benefits, and consider the actions of those around them (Altman & Taylor, 1973; Petronio, 2002; Thibaut & Kelley, 1959). Qualitative responses provided evidence that both groups of participants considered their social network when self-disclosing. However, the trade-off between the costs and benefits was interpreted in a very different manner. The government participants focussed predominately on perceived costs and privacy risks, which suggests that they may have considered the consequences of potential cyber-attacks. In contrast, the academic institution participants were more likely to consider the perceived benefits of self-disclosure. They highlighted the importance of

obtaining value, for themselves and their audience, which other researchers have described as the benefits of social capital online (Ellison, Gray, Lampe, & Fiore, 2014; Ellison et al., 2007).

Using multiple hierarchical regressions of some potential predictors of self-disclosure on Facebook for the two samples, a very different pattern of results emerged. The measured variables explained 27% of the variance in self-disclosure for the government and 19% for the academic institution participants. This suggests that there are other variables at play. For example, the qualitative findings showed that those from the academic institution focussed primarily on the benefits of self-disclosure, which were not measured quantitatively in our study. These should be examined in future research.

For government participants, self-disclosure was most strongly predicted by propensity to trust. This is consistent with Joinson et al. (2010), who claim that trust is a key factor when deciding to share personal information with others. However, as trust was not a predictor for the academic participants, our findings indicate that this relationship may differ depending on the population of interest. Privacy behaviours, conceptualised as the things that people do to protect their privacy online, were also predicted self-disclosure for government participants, but not for those from the academic institution. Therefore, government participants who took steps to protect their personal information (i.e., General Caution) and implemented technical safeguards (i.e., Technical Protection) were less likely to disclose on Facebook. This might be because, as evidenced by our qualitative findings, the government organisation participants were more focussed on perceived costs and privacy risks.

For academic institution participants, self-disclosure was most strongly predicted by gender, with female participants less likely to disclose on Facebook. This is consistent with Chang and Heo (2014) who reported that males from an academic institution were more likely to self-disclose on Facebook due to less perceived risk. Similarly, Walrave et al. (2012) found that female adolescents were more protective of their online privacy and disclosed less. The only other significant predictor for the academic institution participants was whether they knew that their organisation had a SM policy.

Interestingly, privacy concerns were not found to predict self-disclosure for either organisation. This is consistent with the premise of the privacy paradox, which posits that although most people understand the issues and risks associated with SM, they often continue to disclose personal information (Shin, 2010). To date, the privacy paradox has had inconsistent support. In line with Dienlin and Trepte (2015), we argue this may be due to the failure to consider the multidimensional nature of privacy. For example, behaviour could be assessed in regards to the things that people do to protect their privacy, or the actual information that people disclose online, and in this study, we measure both within the Facebook specific context. This highlights the need for further research that considers the multidimensional nature of privacy behaviour.

4.2 Limitations and Future Research

Although, our regression models explained between 19 and 27% of the variance in self-disclosure on Facebook, this leaves room for further investigation of other potential predictors. For example, researchers measure potential benefits of self-disclosure, such as social capital. Additional individual differences could also be studied. For example, Utz (2009) found that individuals who scored more highly on impression management and narcissism employed less restrictive privacy settings. Also, this research does not consider many other organisational factors, such as organisational culture, training, and rewards and punishments. Organisational culture is considered a major factor in developing a better security culture to guide employee behaviour (Lim, Chang, Maynard, & Ahmad, 2009). Further research could examine information security training programs, which may influence the accepted security culture and knowledge of possible cyber threats. Research could also focus on multiple organisations, particularly those more at risk of cyber-attacks, such as government organisations.

A common limitation of questionnaire based studies is the reliance on self-report, resulting in potential biased responses. Future research could analyse individuals' SM accounts in combination with self-report measures. This may give a more objective assessment of online behaviour. Furthermore, the Risky Facebook Behaviours scale requires further validity testing. However, as the scale focusses on actual behaviours rather than more subjective attitudes or options, the pilot testing conducted was sufficient for the purposes of this study.

It is also important to replicate the findings in this study with more homogeneous samples. In our study, the majority of the participants from the government organisation were males, whereas the majority of the participants from the academic institution were females. Gender was found to be a predictor of self-disclosure on Facebook for the academic institution participants, however, not for the government organisation. It is possible that this may be a reflection of the gender distribution in the samples.

5 Conclusion

As the popularity of SM has rapidly grown and continues to evolve, privacy and security issues have become a major focus. With an increasing number of security threats to organisations, attention has shifted towards the impact of employees' online behaviour, both personal and work-related, on their organisations. Given the lack of research about organisations that may be more at risk of cybercrime, such as government organisations where employees more frequently handle sensitive information, this study sought to address this gap. We compared the variables that could predict self-disclosure on Facebook for an Australian government organisation and Australian academic institution, and the populations were influenced by very different variables. Whilst the government participants focussed on the perceived costs, the participants from the academic institution focussed predominately on the benefits associated with self-disclosure on Facebook. The results of this study provide preliminary support for our online self-disclosure model, and highlight the importance of considering different organisations and populations when analysing online behaviour. It is only through further analysis of a wide-range of populations that we will fully understand online self-disclosure and privacy.

6 Reference

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy enhancing technologies* (pp. 36-58): Springer Berlin Heidelberg.

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. New York Holt, Rinehart & Winston.

Arico, S., & Srinivasan, V. (2014). Enabling Australia's digital future: Cyber security threats and implications (pp. 48). Australia: CSIRO.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

BBC News. (2010). Israeli Military 'Unfriends' Soldier after Facebook Leak. *BBC NEWS*. http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2013). Cybersecurity and Critical Infrastructure Protection *Homeland Security: The Essentials*: Butterworth-Heinemann.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015, 30 Nov - 4 Dec). *Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails*. Paper presented at the 26th Australasian Conference of Information Systems (ACIS), Adelaide.

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior, 30*, 79-86.

Cheung, C. M., & Lee, M. K. (2006). Understanding consumer trust in Internet shopping: A multidisciplinary approach. *Journal of the American Society for Information Science and Technology, 57*(4), 479-492.

Cialdini, R. B. (2009). *Influence: Science and Practice*. New York: William Morrow.

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

Dey, R., Jelveh, Z., & Ross, K. (2012). *Facebook users have become much more private: A large-scale study*. Paper presented at the Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on, Lugano, Switzerland.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297.

Ellison, N. B., Gray, R., Lampe, C., & Fiore, A. T. (2014). Social capital and resource requests on Facebook. *New Media & Society, 16*(7), 1104-1121.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment *Privacy online. Perspectives on Privacy and Self-Disclosure on the Social Web* (pp. 19-32). Berlin, Germany: Springer.

Field, A. (2009). *Discovering Statistics Using SPSS* (Third edition ed.): SAGE Publications Ltd.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160.

George Patterson Y&R. (2011). Review of Social Media and Defence. Australia: George Patterson Y&R.

Hair, J. F., Black, B., Babin, B., Anderson, R. E., & Tatham, R. L. (2006). Multivariate data analysis. New Jersey: Pearson.

Jarvenpaa, S. L., & Staples, D. S. (2001). Exploring perceptions of organizational ownership of information and expertise. *Journal of management information systems, 18*(1), 151-183.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction, 25*, 1-24.

Karjalainen, M. (2011). *Improving Employees' Information Systems (IS) Security Behaviour: Toward a Meta-Theory of IS Security Training and a New Frameword for Understanding Employees' IS Security Behaviour*. (PhD), University of Oulu, Oulu. (A 579)

Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage *Center for Strategic and International Studies, Washington, DC*.

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). *Exploring the relationship between organizational culture and information security culture*. Paper presented at the Australian Information Security Management Conference.

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

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*(3), 155-179.

Molok, N. N. A., Chang, S., & Ahmad, A. (2010). *Information leakage through online social networking: Opening the doorway for advanced persistence threats*. Paper presented at the Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security, 2012*(1), 8-11.

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A., Calic, D., & Jerram, C. (2015). *Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?* Paper presented at the Proceedings of Australian Conference of Information Systems (ACIS), Adelaide, December.

Parsons, K., McCormac, A., & Butavicius, M. (2011). Don't judge a (Face)book by its cover: A critical review of the implications of social networking sites. Adelaide: DSTO.

Pearce, W. B., & Sharp, S. M. (1973). Self-disclosing communication. *Journal of Communication, 23*(4), 409-425.

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*: Suny Press.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181-195.

Ramesh, R. (2015, 16 July 2015). Public bodies are releasing confidential personal data by accident, activists say, *The Guardian*. Retrieved from

http://www.theguardian.com/technology/2015/jul/15/confidential-personal-data-release-accident-councils-nhs-police-government

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428-438.

Statistics Brain. (2015). Facebook Statistics. Retrieved November, 2015, from http://www.statisticbrain.com/facebook-statistics/

Symantec Corporation. (2014). Internet Security Threat Report 2014. *19*.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*, 821-826.

Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.

Thibaut, J. W., & Kelley, H. H. (1959). *The Social Psychology of Groups*. Herndon, VA: Transaction Publishers

Utz, S. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2).

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1), Article 1.

Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A Review of Facebook Research in the Social Sciences. *Perspectives on Psychological Science, 7*(3), 203-220.

Appendix 1: Risky Facebook Behaviours Scale

- Is your profile public (as opposed to private)? *
- Have you ever accepted a friend request from someone you didn't know? *
- How frequently do you change your Facebook password? ^
- How frequently do you review your security settings on Facebook? ^
- Do you provide the following information on Facebook? #
    - Place of work
    - Date of birth
    - Role/position at your organisation
    - Phone number
    - Address
    - Location
    - Personal email
    - Real name

* Yes; No; Not applicable

^ Never; Less than once a year; Annually; Semi-annually; More than once a month

Yes, I provide this information; I partially provide this information; No, I do not provide this information