Trading Friendship for Value: An Investigation of Collective Privacy Concerns in Social Application Usage

Research-in-Progress

Chun Fung (Ben) Choi
Department of Information Systems,
School of Computing
National University of Singapore
Singapore 119077
choichun@comp.nus.edu.sg

Zhenhui (Jack) Jiang
Department of Information Systems,
School of Computing
National University of Singapore
Singapore 119077
National University of Singapore
(Suzhou) Research Institute, 377 Lin
Quan Street, Suzhou Industrial Park,
Jiang Su Province, People's Republic of
China, 215123
jiang@comp.nus.edu.sg

Abstract

Online social applications do not only acquire individuals' personal information but also at times collect the personal information of an individual's social networks. Despite the importance of protecting collective privacy, this topic has received little attention in the information system community. To fill this gap in the literature, this article focuses on three unique issues pertinent to collective privacy. First, drawing on the Communication Privacy Management theory, we offer a theoretical framework on the dimensionality of collective privacy concerns (CPC). Second, we propose to operationalize the three dimensions of CPC using a second-order reflective construct, and we plan to develop a scale for it. Third, we identify antecedents of CPC pertinent to the context of social application usage and propose to test a research model on the relationships between these antecedents and CPC as well as the downstream effect on behavioral intentions.

Keywords: Online social networks, collective privacy concerns, social applications

Introduction

In recent years, online social networks (OSNs), such as Facebook and MySpace, have introduced third-party developed social applications, which have attracted massive usage across the globe. While these applications are generally free-of-charge, the software companies are big businesses. For example, Zynga, the marker of popular applications such as “FarmVIlle” and “CityVille”, had reported revenue of $1.14 billion and a market capitalization of over $8 billion in 2011 (Ingram 2011). Indeed, according to Hann et al. (2011), the economy of social applications led to the creation of almost a quarter of a million new jobs and over $15 billion in spinoff benefits for the American economy.

Yet, the success of social applications is not without problems. The pervasive use of social applications does not only threaten individuals’ personal privacy but also the collective privacy of individuals’ social networks. By making social applications available to users, firms are now able to collect immense amount of data about users as well as their friends, who might not be using the applications. For example, Angwin and Singer-Vine (2012) analyzed 100 of the most-used applications on Facebook and found that users did not only expose their public profile information, such as name, profile photo, and gender, but also reveal sensitive details about religious, political, as well as sexual preferences. Furthermore, the article found that the scope of information collected by Facebook applications at times went beyond the application users by acquiring their friends’ profile information. Overall, the unconstrained collection of profile information has stirred privacy concerns among OSN users.

Past Information System (IS) research has substantially advanced our understanding of information privacy (e.g., Bélanger and Crossler 2011; Hong and Thong 2013; Malhotra et al. 2004; Smith et al. 2011; Smith et al. 1996). While IS research deals with numerous aspects of information privacy, its focus has been on individuals’ concerns over personal information. As a result, to the best of our knowledge, no research has been done to examine individuals’ concerns of collective privacy in the online environment. Collective privacy is particularly important in social application usage due to the unique profile information requirement. While individuals typically are required trade some personal information for online services (i.e., cloud storage), they might be required to expose not only their personal information but also reveal the information that their friends have shared. For example, in using the TripAdvisor application, the provider receives individuals’ profile information (i.e., email addresses, work history, and photos) and information they have received from friends (i.e., friends’ profile information, shared photos, and shared status updates).

To address this gap, this study aims to contribute to the privacy literature by focusing on the social application context and examining individuals’ collective privacy concerns (CPC), which is defined as the degree to which an individual is concerned about exposing the information that is shared within his or her online social networks. Whereas personal privacy concerns center on an individual’s subjective views with regards to his or her privacy, collective privacy concerns focus on issues associated with the privacy of a group. Specifically, we (1) theoretically examine the conceptualization of CPC, (2) operationalize the notion of CPC and develop a scale for it, and (3) propose and empirically test a research model centering on CPC. Drawing on the Communication Privacy Management (CPM) theory, we propose that concerns of collective privacy are manifested in three major dimensions, namely permeability concerns, ownership concerns, and linkage concerns (Petronio 1991). Our research model will help explicate the way characteristics of social applications shape individuals’ collective privacy concerns, which in turn, affect individuals’ usage behavior. Results of this study will have both theoretical and practical implications. From a theoretical perspective, this study will offer, to the best of our knowledge, the first comprehensive framework to the literature that helps understand the notion of collective privacy in online social networks. From a practical perspective, the proposed research will provide important managerial guidance to practitioners to evaluate their application designs.

Literature Review

Communication Privacy Management Theory

Online social network users often consider the usage of social applications as a risky behavior not only because it exposes their personal profile information to service providers but also put their friends’ profile information to the scrutiny of the hosts (Angwin and Singer-Vine 2012). For this reason, users’ concerns about information privacy cannot be fully understood without investigating how individuals manage their shared privacy in online social networks. The CPM theory is especially useful for studying collective privacy management (Petronio 2002). It has been applied widely to explain various phenomena including blogging privacy management and information concealment in electronic commerce (e.g., Child and Agyeman-Budu 2010; Metzger 2007). This theory has also been used as a conceptual tool for explaining individuals' behavior in the context of collective privacy (e.g., Afifi 2003).

The CPM theory posits that individuals manage their privacy by erecting "boundaries", which regulate how individuals disclose private information to others and how this relational process is coordinated (Petronio 2002). According to the theory, by revealing private information, a personal privacy boundary is transformed into a collective boundary in which the discloser shares the control of the information with the recipient. Be it concealment from or further exposure to additional parties, both the discloser and recipient might make decisions related to regulating the shared privacy boundary.

When applied to collective privacy, the CPM theory suggests that an individual manages collective privacy based on three important principles, the permeability principle, the ownership principle, and the linkage principle. As a result, it is possible to characterize the notion of collective privacy concerns in terms of three dimensions, namely *permeability concerns*, *ownership concerns*, and *linkage concerns* associated with the management of collective privacy boundaries. Permeability concerns represent individuals' concerns of collective privacy boundary regulation based on the types of collective information exposure. Meanwhile, ownership concerns underscore the importance of controlling subsequent shared information usage. Finally, linkage concerns emphasize individuals' worries about the recipients of the shared information. Thus, we conceptualize CPC as the degree to which an OSN user is concerned about exposures of shared information, the ability to regulate subsequent usage of the shared information, and the recipient of the shared information.

Permeability Concerns

The CPM theory is strongly rooted in the principle of permeability management (Petronio 2002). According to this principle, individuals manage collective privacy by regulating collective information disclosure. In particular, individuals want to control the types of shared information to be disclosed to others. Past empirical studies have revealed that individuals' privacy concerns vary in accordance to the types of information exposures. For instance, Malhotra et al. (2004) found that individuals were highly concerned about their privacy when sensitive personal information was exposed to online marketers. Furthermore, they noticed that individuals' privacy could be substantially undermined when they lost control over their information (i.e., disclosure to online vendors). In the context of online social networking, evidence suggests that users are concerned over revealing sensitive topics about friends, such as shared secrets and intimate jokes, which would threaten collective privacy (Child and Agyeman-Budu 2010).

Indeed, concerns over types of collective exposures are captured through collection in the privacy literature (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). However, according to the CPM theory, the importance of privacy concerns associated with the exposures of collective information in online social networks can be succinctly conveyed by the permeability based factor. Thus, we posit *permeability concerns*, which refer to the degree to which an individual is concerned about the type of collective privacy information exposed to others, as an important factor characterizing CPC.

Ownership Concerns

According to Petronio (2002), individuals expect to retain full ownership of the privacy boundaries even though their personal information has been shared with others. In fact, evidence suggests that an individual might have a great stake in how personal information is handled or feel that he or she should have total control of its subsequent usage, despite having shared the information with others (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). Thus, we propose that an individual's concerns for collective privacy center on whether the individual can retain their ownership over the shared privacy boundaries.

Several studies have suggested that in reality individuals want to have the ability to fully retain their ownership over information. For example, Xu et al. (2010) examined location-based service usage and found that individuals who retained full ownership over their locational information were more willing to reveal their locations to service providers compared to those who could not. Similarly, in a study on the effect of online privacy information, Tsai et al. (2011) noted that consumers paid special attentions on continued ownership associated with their personal data in deciding personal information disclosure to online firms. In sum, past research has highlighted the importance of individuals' concerns over information ownership. Accordingly, we content that *ownership concerns*, as the extent to which an individual is concerned about their ownership over the shared privacy boundary, is likely to be an important component reflecting CPC.

Linkage Concerns

According to the CPM theory, *linkage* coordination illustrates issues associated with the recipients of privacy exposures. Establishing linkage means that collective information is exposed to additional recipients. Past research examining information privacy has underscored the importance of recipients in privacy exposures. For instance, Andrade et al. (2002) examined self-disclosure to online companies and found that consumers were more likely to disclose personal information to more reputable firms than to less reputable ones. Likewise, Xie et al. (2006) revealed that individuals were most willing to reveal personal information to companies that they found honest and reliable. In a study examining the personalization privacy paradox, Awad and Krishnan (2006) noted that consumers' willingness to be profiled online depended on their understanding of the online companies.

In relation to online social networking, the linkage principle examines the extent to which individuals are concerned over exposing friends' information. The online social networking environment offer novel ways for individuals to expose collective information to service providers. For instance, by adopting a social application, individuals might not only expose friends' public profile information but also reveal their private profile information, which could be invisible and unknown to the individuals. Consequently, establishing boundary linkage to social application providers will increase individuals' collective privacy concerns. Therefore, we posit that an individual's linkage concerns, defined as the extent to which an individual is concerned about the additional recipient of the shared privacy information, are likely to be a unique component of CPC.

Research Model and Hypotheses

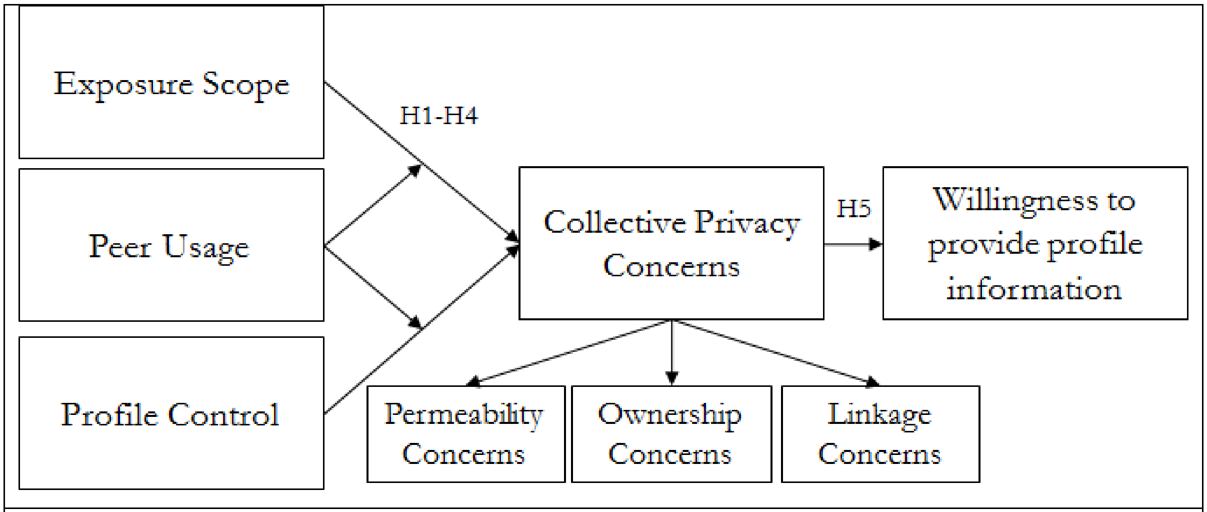

Figure 1. Research Model

This study focuses on three important antecedents of CPC, which represent the key factors that influence social application usage. The three antecedents of CPC are exposure scope, profile impersonation, and peer usage (Figure 1). First, to use a social application, users are typically required to expose some profile information to the application provider. The exposure might have a personal scope, which covers a user's personal profile information, or a social scope, which covers not only the profile information of the user but also that of his or her friends. Accordingly, this study examines exposure scope, which is defined as the range of profile information being revealed to the social application provider.

Second, prior to using a social application, users are often required to give up some control of their personal profiles. By surrendering profile control, users permit social applications to act on their behalf in some of their online social networking activities. For instance, a social application might post updates with regards to a user's application usage, without his or her knowledge. Furthermore, the application might act on the user's behalf in sending application requests to friends. Therefore, we examine how the usage of social application can challenge *profile control*, which refers to the extent of control an individual has over his or her personal profile. Low profile control depicts individuals' inability to control information disseminated on their personal profiles, while high profile control represents individuals' retaining full control over their profiles.

Lastly, users are known to consider friends' usage in adopting social applications. Past studies suggest that friends' usage is indicative to the extent of collective norm (e.g., Vir Singh and Phelps Forthcoming). Specifically, it is known that high usage represents consensus and acceptance whereas low usage implies general disapproval. In view of the importance of friends' usage, this study examines the role of *peer usage* in shaping collective privacy concerns. Peer usage is defined as the extent to which a social application has been adopted by an individual's online social network friends.

The research variables and their relationships in the model are explained in detail as follows.

Exposure scope

Exposure scope represents the range of profile information being revealed to the social application provider. It is known that individuals' privacy concerns depend on the type of information requested by marketers (Phelps et al. 2000). In particular, releasing friends' information is perceived as more risky than releasing personal information (Petronio 2000). Although the disclosure of personal information might often trigger privacy concerns, in general the exposure of others' personal information is known to be viewed as betrayal and selfish (Child and Agyeman-Budu 2010). One on hand, the disclosure of personal information is typically a voluntary decision in which individuals disclose personal information, at their own privacy costs, for personal gains (Dinev and Hart 2006). On the other hand, when disclosure exposes information about friends, individuals are essentially gaining benefits at the costs of others.

Despite the importance of exposure scope, to our best understanding, no study has considered this issue explicitly and empirically examined the phenomenon. To fill this gap in the literature, our research model is specifically developed to explicate the effects of exposure scope on individuals' collective privacy concerns. In general, our model proposes that a personal exposure scope, compared to a social exposure scope, will lead to weaker collective privacy concerns. Specifically, we expect that exposures of friends' profile information will make an individual suspicious; consequently, this exposure scope will increase the individual's concerns over collective privacy. Our rationale is that with a social exposure scope, the individual is exposing friends' information, which might be perceived as a breach of trust in protecting the privacy of friends. As a result, when the social application has a social scope of information acquisition, individuals are likely to be highly wary about collective privacy. Therefore, compared to a scope of personal exposure only, a social exposure scope will increase collective privacy concerns.

H1: Compared to a personal exposure scope, a social exposure scope will lead to higher collective privacy concerns.

Profile Control

Within the framework of the privacy regulation theory (Altman 1993), individuals desire to avoid being manipulated, dominated, or exposed by others. In particular, privacy concerns are pertinent to individuals' ability to control transactions (i.e., interactions and communications) that regulate access to self and that, as a consequence, reduce vulnerability and increase decisional and behavioral options (Margulis 2003). For example, Hoadley et al. (2010) examined privacy issues associated with Facebook applications and found that the news feed application took away individuals' autonomy by reducing their control over personal profile, which triggered privacy concerns. Likewise, in a review of privacy research in IS, Bélanger and Crossler (2011) noted that individuals' ability to control personal information was an important determinant of privacy concerns.

A general consensus in the privacy literature shows that the ability to control personal information influences privacy concerns (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). This implies that an individual's personal profile control in online social networks will influence their experience of privacy concerns. While individuals in general are able to manage information disclosure on their personal profiles, social applications might expose private information and hence reducing their personal profile control. Additionally, by taking over personal profiles, social applications do not only challenge individuals' privacy but also violate the privacy of their friends in online social networks. This is because posting made by the social applications are typically seen as unsolicited disseminations, which could potentially violate friends' "right to be left alone" (Schwartz 1977). Therefore, we expect low profile control will increase collective privacy concerns.

H2: Compared to low profile control, high profile control will lead to lower collective privacy concerns.

Peer Usage

The social influence perspective was developed to explain how social information influences an individual's attitude (Salancik and Pfeffer 1978). Rather than being viewed as a stable individual characteristic, the social influence perspective views attitude as an outcome that is socially constructed, rather than fixed and immutable characteristics existed prior to the formation of an attitude specific to an issue. The social information cues that individuals receive from their environment will be used to help construct and shape the realities. Thus, if individuals tend to be exposed to more positive social cues regarding a social application, these individuals will be more likely to express positive feelings towards the application.

Past research has proposed a myriad of mechanisms to explain the influence of social information on individuals' attitude, such as peer pressure and the bandwagon perspective (Arbahamson 1996). Nevertheless, many explanations of social influence are built upon the conformity principle, which contends that individuals change his or her attitude to match the attitude of others (Cialdini and Goldstein 2004). In particular, the Social Impact Theory (SIT) (Latané 1981) posits that an individual occupying a given social space will be more likely to conform to the attitudes, beliefs, and behavioral propensities exhibited by the local numerical majority than by either the local numerical minority or less proximate persons.

In online social network, the majority's attitude towards a social application can be implied by the extent of peer usage, which represents the amount of friends using the application. In cases of low peer usage, the majority of an individual's friends have not adopted the social application. By using the social application, the individual might become the early adopter who introduces this application into his or her social networks and triggers exposures of profile information. Therefore, without a convergent attitude towards the application, the individual could be highly concerned about the scope of information exposure associated with application usage. In particular, when the exposure scope involves friends' profile information, the individual is violating friends' privacy rights and breaching their trust over protecting shared privacy. In contrast, when the exposure scope involves the individual's profile information, social application usage would only reveal his or her personal information, which does not pose a challenge to the shared privacy. Hence, when peer usage is low, social exposure scope will lead to higher level of collective privacy concerns than personal exposure scope.

On the contrary, when peer usage is high, the majority of the individual's social network has adopted the social application. As a result, according to the SIT, the individual is likely to conform to his or her friends' convergent attitude towards the social application, regardless of the scope of information exposure. This is because high peer usage is a clear indication that the individual's friends are not entirely concerned about exposing their profile information in using the social application. Furthermore, high peer usage also implies that the exposure of profile information has been widely regarded as socially acceptable among friends. Thus, we predict the following effects:

H3: There is an interaction effect between exposure scope and peer usage on collective privacy concerns, i.e., exposure scope has a stronger effect in the low peer usage condition than in the high peer usage condition.

We hypothesize that the effect of profile control on collective privacy concerns is moderated by peer usage. In cases of low peer usage, an individual who is adopting the social application has no established norm to follow (Mason et al. 2008). As such, when profile control is low, the individual is likely to be concerned about violating the privacy of others. High profile control, however, implies that the adoption is less likely to intrude the privacy of friends, as the individual retain a high degree of control over his or her personal profile (Petronio 1991). In particular, when profile control is high, the individual might protect shared privacy by actively regulating the profile information collected by the application. Furthermore, with high profile control, the individual might prevent the application from making posting on his or her behalf, and hence preserving their friends' privacy rights. Therefore, when peer usage is low, high profile control helps the individual protect the privacy of his or her social networks.

In contrast, when peer usage is high, the individual's social network has widely adopted the application. This implies that the individual's friends are in general unconcerned about exposing private information in exchange for the social application. Moreover, although low profile control exposes friends to postings made by the application, high peer usage assures the individual that his or her friends would not be offended by unsolicited disseminations. Therefore, when peer usage is high, the decrease in the level of collective privacy concerns will not be as marked as when peer usage is high. We thus predict the following hypothesis:

H4: There is an interaction effect between profile control and peer usage on collective privacy concerns, i.e., profile control has a stronger effect in the low peer usage condition than in the high peer usage condition.

Profile Information Provision

Collective privacy concerns, in turn, should be related to the willingness to provide profile information to use social applications. Ample empirical evidence suggests that individuals' concerns about privacy are the single most important reason for declining to use Internet services. For instance, Son and Kim (2008) found that individuals with high privacy concerns typically believed online firms would behave opportunistically with their information and hence would refuse information provision to protect their privacy.

In the context of online social application usage, collective privacy concerns also represent individuals' worry about opportunistic behavior related to the profile information submitted to application provider. Sources of opportunistic behavior include selling to, or sharing information with, parties not involved in the immediate transactions, such as third-party marketing firms, other application providers or government agencies (Preston 2004). The concern that third parties could use profile information in unintended ways or that information might not be securely protected reflects the possibility that individuals might suffer the consequences of opportunistic behavior with respect to profile information disclosed to application providers. This concern makes individuals hesitant to disclose profile information necessary to complete the installation of the social application.

H5: A higher level of collective privacy concerns will lead to lower level of willingness to provide profile information to install social applications.

Methodology

Two empirical studies will be conducted to develop and test a new scale of CPC. The purpose of Study 1 is to develop measures for the three dimensions of CPC (e.g., permeability concerns, ownership concerns, and linkage concerns). Study 2 is designed to establish the second-order factor. In this latter study, we also plan to formally test the research model and hypotheses. Specifically, we plan to solicit actual Facebook users to participate in our study and develop a social application, which shall be installed by the participants. The main purpose of this application is to capture (1) actual social application usage, (2) characteristics of the adopted social applications, and (3) the extent of peer usage prior to adoption. The application shall also help facilitate the survey questionnaire which measures other research constructs.

Discussion, Implications, and Future Research

Theoretical Implications

Drawing on the CPM theory, this study offers a theoretical framework to explain the dimensions of online social network users' concerns for collective privacy. Specifically, we discussed notions of (1) permeability, (2) ownership, and (3) linkage and tied them to dimensions of collective privacy concerns – "what type of information is exposed" (permeability concerns), "how is the exposed information controlled" (ownership concerns), and "who is the recipient of the information" (linkage concerns). We believe that our theory-driven approach to collective privacy concerns will complement existing scales which focus on personal privacy concerns.

CPC is developed to reflect the notion of collective privacy because of the widespread use of online social network. It is strongly rooted in a general conceptual framework drawing on the CPM theory. Therefore, under an assumption that the essence of collective privacy concerns lies in the notion of shared privacy boundary management, our scale is likely to be generalizable across a variety of other privacy contexts. For instance, new privacy-threatening technologies such as location-based services and face recognitions are continuously being developed. As mentioned earlier, CPC centers on issues associated with shared privacy boundary management; therefore, the scale can be adapted to technical changes that may occur in the future.

Privacy research in the IS domain has mostly focused on individuals' privacy concerns in general (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). In this study, we examine individuals' concerns over collective privacy at a specific level as well as investigate the unique antecedents in the context of social application usage. Overall, this study shall reveal evidence that individuals' behavior in the context of collective privacy is a complex phenomenon; thus, researchers should be ready to employ sophisticated technique to examine individuals' reactions to collective privacy threats.

Practical Implications

Our findings shall help establish a CPC scale, which will be a worthy candidate for consideration as an indicator of online social network users' collective privacy concerns. From a managerial perspective, our study provides evidence that users consider (1) the type of information revealed, (2) how is the exposed information controlled, and (3) who is the recipient of the information. Therefore, at the very least, developers should make sure that users can easily check the type of information collected by the social application, the privacy policies, and the organizations collecting and using the information.

Limitations and Future Research Directions

Some limitations of this study should be mentioned. It is plausible that individuals' reactions to a specific collective privacy threat are highly dependent on contextual factors. Thus, it remains to be seen whether the results of this study retain their validity with different contextual variables, such as types of social applications and compositions of online social networks.

This study considers the impact of social application usage in the context of collective privacy, namely exposure scope, profile control, and peer usage. Yet, it is possible that other aspects of social application usage also play an important role in individuals' concerns for collective privacy. For example, individuals are likely to consider the nature of their social networks in using social applications. In particular, individuals derive his or her self-concept from the knowledge of memberships in a social group (or groups) with the value and emotional significance this individual attaches to that membership (Trafimow and Finlay 2001; Wann and Grieve 2005). Therefore, when the overlap of multiple in-groups is perceived to be high, the individual maintains a relatively simplified identity structure whereby memberships in different groups converge to form a single in-group identification. In contrast, when a person acknowledges and accepts that memberships in multiple in-groups are not fully convergent or overlapping, the associated identity structure is both more inclusive and more complex (Roccas and Brewer 2002).

Additionally, usage of social applications could be influenced by individuals' personality traits. For example, since extraverts enjoy developing interpersonal bonding, they might be more willing to disclose profile information in using social applications. Evidence suggests that highly innovative individuals are willing to try new technologies. Therefore, it is plausible that innovative individuals might be more ready to reveal profile information in adopting social applications. Computer playfulness is known to influence the extent to which an individual enjoys using computers. Therefore, it is reasonable to expect that playful individuals could be very willing to adopt social applications.

Conclusion

In summary, our study identifies collective privacy concerns as a major problem affecting individuals' usage behavior in online social networks. This proposal introduces the development of a CPC scale, which is expected to reasonably represent the three dimensions of collective privacy concerns, namely permeability concerns, ownership concerns, and linkage concerns. Using this scale, we shall be able to demonstrate how individuals' collective privacy concerns negatively influences their willingness to provide profile information. We believe that the CPM theory presented in this study will be a solid basis for studying novel issues related to collective privacy.

Acknowledgements

The authors also thank the Ministry of Education (MOE) of Singapore [Grant: MOE2009-T2-1-062] for its financial support.

References

Afifi, T.D. 2003. "'Feeling Caught' in Stepfamilies: Managing Boundary Turbulence through Appropriate Communication Privacy Rules," *Journal of Social and Personal Relationships* (20:6), pp. 729-756.

Altman, I. 1993. "Dialectics, Physical Environment, and Persoanl Relationships," *Communication Monographs* (60:1), pp. 26-34.

Andrade, E.B., Kaltcheva, V., and Weitz, B. 2002. "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation," in *Advances in Comsumer Research,* S.M. Broniarczyk and K. Nakamoto (eds.). Association for Consumer Research, Valdosta, GA 2002, pp. 350-353.

Angwin, J., and Singer-Vine, J. 2012. "Selling You on Facebook." from http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html?mod=WSJ_WhatTheyKnowPrivacy_LeftTopNews#project%3DGRABBY1204%26articleTabs%3Dinteractive

Arbahamson, E. 1996. "Management Fashion," *Academy of Management Review* (21:1), pp. 254-285.

Awad, N.F., and Krishnan, M.S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Bélanger, F., and Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041.

Child, J.T., and Agyeman-Budu, E.A. 2010. "Blogging Privacy Management Rule Development: The Impact of Self-Monitoring Skills, Concern for Appropriateness, and Blogging Frequency," *Computers in Human Behavior* (26:5), pp. 957-963.

Cialdini, R.B., and Goldstein, N.J. 2004. "Social Influence: Compliance and Conformity," *Annual Review of Psychology* (55), pp. 591-622.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (1:17), p. 2006.

Hann, I.-H., Viswanathan, S., and Koh, B. 2011. "The Facebook App Economy." from http://www.rhsmith.umd.edu/digits/pdfs_docs/research/2011/AppEconomyImpact091911.pdf

Hoadley, C.M., Xu, H., Lee, J.J., and Rosson, M.B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), pp. 50-60.

Hong, W., and Thong, J.Y.L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.

Ingram, M. 2011. "Have Facebook Apps Really Created $15b in Economic Value?", from http://gigaom.com/2011/09/19/have-facebook-apps-really-created-15b-in-economic-value/

Latané, B. 1981. "The Psychology of Social Impact," *American Psychologist* (36:4), pp. 343-356.

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 System Research* (15:4), pp. 336-355.

Margulis, S.T. 2003. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2), pp. 243-261.

Mason, W.A., Jones, A., and Goldstone, R.L. 2008. "Propagation of Innovations in Networked Groups," *Journal of Experimental Psychology* (137:3), pp. 422-433.

Metzger, M.J. 2007. "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication* (12:2), pp. 335 - 361.

Petronio, S. 1991. "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples," *Communication Theory* (1:4), pp. 311-335.

Petronio, S. 2000. "The Boundaries of Privacy: Praxis of Everyday Life," in *Balancing the Secrets of Private Disclosures* S. Petronio (ed.). Mahwah, NJ: Lawrence Erlbaum., pp. 37-49.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumers Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1).

Preston, J. 2004. "Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data,").

Roccas, S., and Brewer, M. 2002. "Socia Identity Complexity," *Personality and Social Psychology Review* (6:2), pp. 88-106.

Salancik, G., and Pfeffer, J. 1978. "A Social Information Processing Approach to Job Attitudes and Task Design," *Administrative Science Quarterly* (22), pp. 427-456.

Schwartz, A.U. 1977. *Privacy - the Right to Be Let Alone*. Greenwood Press.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.

Smith, H.J., Milberg, S.J., and Burke, S.J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Son, J.-Y., and Kim, S.S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.

Stewart, K.A., and Segars, A.H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp. 36-49.

Trafimow, D., and Finlay, K.A. 2001. "Evidence for Improved Sensitivity of within-Participants Analyses in Tests of the Theory of Reasoned Action," *Social Science Journal* (38:629-635).

Tsai, J.Y., Serge, E., Lorrie, C., and Alessandro, A. 2011. " The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268.

Vir Singh, P., and Phelps, C. Forthcoming. "Networks, Social Influence, and the Choice among Competing Innovations: Insights from Open Source Software Licenses," *Information Systems Research*).

Wann, D.L., and Grieve, F.G. 2005. "Biased Evaluations of in-Group and out-Group Spectator Behavior at Sporting Events: The Importance of Team Identification and Threats to Social Identity," *Journal of Social Psychology* (145:5), pp. 531-546.

Xie, H., Teo, H.H., and Wan, W. 2006. "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior," *Marketing Letters* (17:1), pp. 61-74.

Xu, H., Teo, H.H., Tan, B.C.-Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-174.