Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

SOCIAL NETWORK PRIVACY DISPOSITIONS: AN OBJECTIVE MEASUREMENT SCALE AND A CAUSAL MODEL

Ben CF Choi
UNSW Australia Business School, chun.choi@unsw.edu.au

Jie Yu
Nottingham University Business School, Jie.YU@nottingham.edu.cn

Yi Wu
Tianjin University, yiwu@tju.edu.cn

Zhenhui (Jack) Jiang
National University of Singapore (Suzhou), jiang@comp.nus.edu.sg

SOCIAL NETWORK PRIVACY DISPOSITIONS: AN OBJECTIVE MEASUREMENT SCALE AND A CAUSAL MODEL

Ben CF Choi, School of Information Systems, Technology, and Management, UNSW Australia Business School, UNSW Australia, Australia, chun.choi@unsw.edu.au

Jie Yu, Nottingham University Business School, China, jie.yu@nottingham.edu.cn

Yi Wu, College of Management and Economics, Tianjin University, China, yiwu@tju.edu.cn

Zhenhui (Jack) Jiang, 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

The Information Systems literature has substantially advanced understanding of privacy in both offline contexts and online environments. Despite the rich understanding, existing studies predominately focused on elucidating privacy issues specific to individuals. The increasingly popular usage of mobile apps with social media integration has fundamentally challenged current understanding and conceptualization of information privacy. In particular, mobile apps allow information collection beyond individuals' personal scope (i.e., his/her personal information) and extend the scope of acquisition into individuals' online social networks (i.e., his/her list of friends on Facebook). To fill this gap in the literature, drawing on the Communication Privacy Management Theory, this proposal focuses on three unique dimensions of social network privacy dispositions, namely permeability, ownership, and linkage. Second, we propose to operationalize these three dimensions of social network privacy dispositions using a second-order reflective construct, and we plan to develop an objective measurement scale for it. Lastly, we plan to validate the construct using a nomological network.

Keywords: Social Network Privacy Dispositions, Mobile Apps, Logging Autonomy, Peer Usage.

1 INTRODUCTION

In recent years, use of online social networks (OSNs) in a variety of application settings has gained substantial traction and attention. In particular, between December 2013 and June 2014, mobile app usage has grown by 62 percent (Flurry Analytics 2014). Yet, the success of mobile apps is not without problems. The pervasive use of mobile apps does not only threaten the privacy of users' online social network profile information but also exposes them to unrestrained monitoring. By making mobile apps integrated with online social networks, firms are now able to collect immense amount of information about users. For example, Featherman and Pavlou (2003) analyzed 100 of the most-used apps on Facebook and found that users did not only expose their public profile information, such as name, profile photo, and gender, but also revealed sensitive details about religious, political, as well as sexual preferences. Overall, the unconstrained collection of profile information has stirred privacy concerns among users.

Past Information Systems (IS) research has substantially advanced our understanding of information privacy (e.g., Gefen and Ridings 2002; Ma et al. 2011; Malhotra et al. 2004; Sheng et al. 2008; Smith et al. 1996). While IS research deals with numerous aspects of information privacy, the concept of privacy concerns is typically operationalized using subjective measurement scales. Theorists have generally agreed that objective measurement scales are superior compared to subjective scales. In particular, by measuring privacy dispositions subjectively, respondents will be prompted about the importance of privacy. Accordingly, their sensitivity towards potential privacy issues could be artificially elevated. To the best of our knowledge, no research has been conducted to examine individuals' concerns of privacy objectively. Hence, our research question is, what are the key objective dimensions of privacy dispositions specific to online social networks?

To address this research question, this study aims to contribute to the privacy literature by focusing on the mobile apps context and proposing an objective measurement scale of privacy concerns, which is named as social network privacy dispositions (SNPD). Social network privacy dispositions are defined as the degree to which a user is concerned about protecting his/her privacy space in online social networks. Social network privacy dispositions not just focus on the informational aspects of privacy concerns, which is similar to those in past IS research, but also center on the impact of social networking characteristics on privacy. Specifically, we plan to (1) theoretically examine the conceptualization of SNPD, (2) operationalize the notion of SNPD and develop an objective scale for it, and (3) propose and empirically test a research model centred on SNPD. Drawing on the Communication Privacy Management (CPM) theory, we propose that social network privacy dispositions manifest in three major dimensions, namely permeability, ownership, and linkage (Xu et al. 2012). Our research model will help explicate the way characteristics of mobile apps shape individuals' usage intention. Additionally, following past information privacy research, we would explore how social network privacy dispositions moderate the relationships between app characteristics and usage intention. 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 social network privacy dispositions in online social networks. From a practical perspective, the proposed research will provide important managerial guidance to practitioners to evaluate their app designs.

2 LITERATURE REVIEW

2.1 Information Privacy and Privacy Space

The rich body of work in privacy has made available several conceptualizations of privacy. For example, according to Westin (1967), privacy is defined as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others. In another seminal work, Altman (1973) conceptualizes privacy as a control mechanism, defining it as the selective control of access to the self or to one's group. Overall, despite the rich conceptualizations, past research has largely focused on the importance of control in maintaining privacy. More important, the privacy

literature highlights the dialectic and non-monotonic nature of privacy. In particular, ample evidence suggests that individuals seek an optimal level of privacy in social interactions. In other words, despite the explicit risks and threats associated with privacy exposure, individuals would choose to release personal information for certain benefits (Hann et al. 2005).

Past IS research has typically focused on privacy specific to information exchange and developed substantial insights into information privacy. For instance, Xu et al. (2012) examined the impact of control agency in reducing privacy concerns and noted that information privacy is a state of limited access to personal information. Furthermore, the IS literature has also provided several deep insights in measuring individuals' concerns for information privacy. Specifically, Smith et al. (1996) developed the Concern for Information Privacy (CFIP) scale, which is often considered as one of the most reliable scales for measuring privacy concerns (Bansal and Gefen 2010). Malhotra et al. (2004) developed a multidimensional scale of Internet Users Information Privacy Concerns (IUIPC), which identified three dimensions of Internet privacy concerns: collection of personal information, control over personal information, and awareness of organizational privacy practices.

2.2 Communication Privacy Management Theory

Online social networks users often protect their privacy by prudently managing personal profile, which typically contains extensive personal information. For example, in establishing personal profiles, Facebook users are encouraged to provide information on their names, genders, birthdays, and education background. Likewise, LinkedIn users are prompted to reveal their employment history, including current positions, past positions, and projects. More important, personal profiles do not only contain static personal information but are frequently enriched with updates about the users. For this reason, personal profiles essentially constitute users' privacy space in the online social networking environment and hence needs to be cautiously managed.

The CPM theory is especially useful for studying privacy space management (Petronio 2002). It has been applied widely to explain various phenomena including blogging privacy management and information concealment in electronic commerce (e.g., Metzger 2007; Shen et al. 2005). This theory has also been used as a conceptual tool for explaining individuals' behavior in the context of personal privacy (e.g., Afifi 2003). According to the theory, individuals manage their privacy by erecting psychological boundaries, which regulate how individuals make decisions to disclose private information to others and how this relational process is coordinated (Petronio 2002). Furthermore, individuals typically routinize boundary management by formulating rules which help govern the exposure of privacy as well as the admissions of others through the boundaries. In essence, these rules are often stable and consistently exercised in the form of individual dispositions and beliefs.

When applied to online social networks, CPM theory suggests that a user manages his/her privacy space 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 social network privacy dispositions (SNPD) in terms of three dimensions, namely *permeability disposition*, *ownership disposition*, and *linkage disposition,* associated with the management of personal privacy space. Permeability disposition represents individuals' beliefs associated with personal information exposure. Meanwhile, ownership disposition underscores regulating admissions to privacy space. Lastly, linkage disposition emphasizes individuals' concerns over uncontrolled social connectivity. Overall, we conceptualize SNPD as the extent to which an online social networks user is concerned about privacy space exposure, invasion, and interconnectivity.

2.2.1 The Permeability Principle

The CPM theory is strongly rooted in the principle of permeability management (Petronio 2002). According to this principle, individuals manage privacy space by regulating information disclosure. In particular, individuals want to be vested with the control of types of shared information to be disclosed to others. Past empirical studies have revealed that individuals' privacy concerns vary in accordance to

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. Likewise, Phelps et al. (2000) revealed that individuals were especially wary about their privacy when highly personal information was exposed in online commercial transactions. In the context of online social networks, evidence suggests that users are concerned over revealing sensitive topics, such as shared secrets and intimate jokes, which would threaten collective privacy (Shen et al. 2005). Indeed, concerns over types of information exposures are captured through individuals' enactment of control in the privacy literature (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). More important, emerging evidence underscores the centrality of control, in both regulating self-exposure as well as managing intrusion to privacy space, as a predominate indication of privacy concerns in the online environment. Accordingly, consistent with past information privacy research, we posit *permeability*, as the extent to which an online social networks user is concerned about over-exposure of personal information, as an important dimension of social network privacy dispositions.

2.2.2 The Ownership Principle

Petronio (2002) theorizes that individuals expect to retain full ownership of the privacy boundaries even though their privacy space is tightly coupled with that of others. In particular, despite being in closed relationships, individuals expect to retain some extent of their privacy space by maintaining both physical and psychological distance as well as reserving instances of solitude. Thus, we propose that an online social networks user's disposition of privacy space ownership centers on whether the user can maintain control over admissions to his/her personal profile. In online social networks, admissions to personal profiles can be voluntarily enacted and involuntarily enforced. Whereas voluntary admission is often exercised through users' status updates and acceptance of friend requests, involuntary admission can be enforced through friends' postings and status updates made by other applications. The information privacy literature suggests that in reality individuals want to have the ability to fully retain their boundary ownership. 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. In sum, past research has highlighted the importance of individuals' disposition over privacy boundary ownership. Accordingly, we content that *ownership*, as the extent to which an online social networks user is concerned about their ownership over the privacy boundary, is likely to be an important component of SNPD.

2.2.3 The Linkage Principle

According to the CPM theory, the *linkage* principle illustrates privacy issues associated with establishing new social connectivity in communications. Establishing linkage means that individuals' personal information is exposed to additional recipients. Past research examining information privacy has underscored the importance of regulating social connectivity in maintaining privacy. For instance, Jiang et al. (2013) examined synchronous online social interactions and found that perceptions of anonymity was an important consideration in individuals' privacy evaluation. Likewise, Sutanto et al. (2013) investigated personalization in smartphone applications and reported that compared to safekeeping identity information with the service providers, users were less concerned about privacy when they were allowed to retain identity information within their phone. In essence, ample information privacy research highlights the importance of linkage regulation through anonymity and concealment. The online social networking environment offers novel ways for individuals to achieve anonymity and concealment. While the technological features predominately focus on promoting individuals' identity and enhancing social exposures, several privacy features are provided to limit user visibility. For example, on Facebook, users might choose to be unsearchable to the general public and hence turning their personal profiles invisible to strangers. Considering the importance of the linkage principle, we posit that *linkage*, which refers to the extend to which an online social networks user is concerned about his/her profile visibility, is likely to be an important component of SNPD.

3 RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

Drawing on the literature above, this study proposes an objective measurement scale to capture online social networks users' social network privacy dispositions. Specifically, corresponding to the CPM theory, the proposed social network privacy dispositions consist of three dimensions, namely permeability, ownership, and linkage. Permeability subsumes users' concern about over-exposure of personal information, which can be reflected in the amount of static disclosure in personal profiles. Ownership centers on users' concern about privacy boundary regulation, which is realized through the amount of dynamic disclosure. Finally, linkage focuses on the public visibility of personal information, which is attained by customizing the searchability of personal profiles.

To validate the proposed measurement scale, a causal model is developed (see Figure 1).

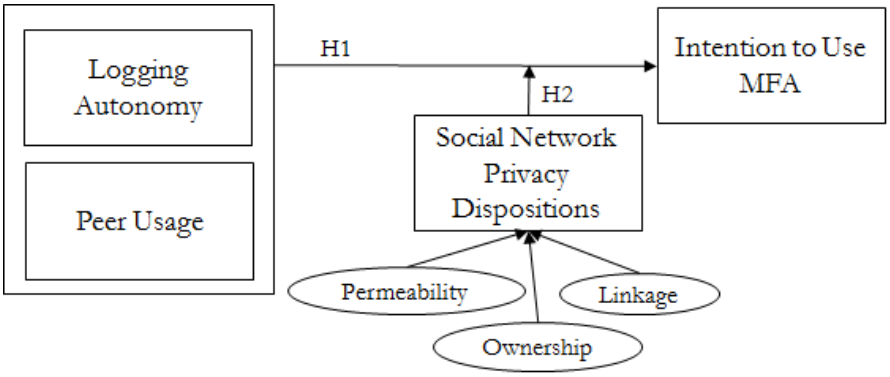

Figure 1. Research model

This study focuses on two important antecedents of mobile application usage when individuals' personal information is concerned. Specifically, previous research has demonstrated that users' intention to use mobile applications are influenced by autonomy and relatedness (e.g., McMillan et al. 2013). Therefore, to reflect the importance of autonomy, this study examines two modes of logging autonomy, namely autonomous logging and delegated logging. Whereas autonomous logging allows users' control over archiving of their usage activities, delegated logging denies users' control over the logging mechanism. Furthermore, to reflect the importance of relatedness, this study examines the extent of peer usage, which depicts the extent of consensus among a user's online social network friends specific to the mobile application. The information privacy literature suggests that when individuals evaluate information exchange, their dispositional privacy concerns play an important role in privacy assessment. Therefore, to reflect the differential impact of dispositional privacy concerns, this study examine the way social network privacy dispositions moderate the effects of logging autonomy and peer usage on mobile application usage.

According to privacy regulation theory (Altman 1993), individuals desire to avoid being manipulated, dominated, or exposed by others. In particular, privacy related behaviors are pertinent to individuals' ability to control over 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 profile information integrity, which triggered privacy concerns.

A general consensus in the privacy literature shows that the ability to control personal information entices technology usage intention (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). This implies that logging autonomy will influence their intention to use mobile applications. While users in general are able to manage information disclosure on their personal profiles, mobile applications might expose private information and hence reduce their personal profile integrity. This is because posting made by mobile applications are typically seen as unsolicited disseminations, which could

potentially violate users' "right to be left alone" (Moore and Benbasat 1991). Therefore, we expect that autonomous logging would lead to higher intention to use mobile applications.

H1a: Compared to autonomous logging, delegated logging will lead to lower intention to use mobile application.

The social influence perspective provides the theoretical explanation on the effect of peer usage on intention to use mobile application (King 2012). According to this perspective, 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 (i.e., wide adoption by peers and positive word-of-mouths from friends) regarding a mobile application, these individuals will develop stronger usage intention.

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 (Parboteeah et al. 2009). Nevertheless, many explanations of social influence are built upon the conformity principle, which contends that individuals change their behaviors to match the behavior of others (Wang and Stefanone 2013). Evidence suggests that conformity is contingent on individuals' perceptions of the level of consensus for the beliefs held by others. In particular, the Social Impact Theory (SIT) (Banker et al. 2006) 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 networks, the majority's attitude towards a mobile 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 a user's friends have not adopted the mobile application. Therefore, without a convergent attitude towards the application, the user will develop lower usage intention. On the contrary, when peer usage is high, the majority of the individual's social network has adopted the mobile application. As a result, according to the SIT, the user is likely to conform to his or her friends' convergent attitude towards the application. Thus, we hypothesize

H1b: Compared to low peer usage, high peer usage will lead to higher intention to use mobile application.

According to the enhanced APCO model (Dinev et al. 2015), privacy-related behaviour might not be an entirely deliberative outcome. Rather privacy behaviors could be affected by the level of cognitive effort being expended in processing privacy-related information. In particular, whereas privacy unconcerned individuals might neglect scrutinizing privacy situations, privacy fundamentalists could be motivated to thoroughly process privacy-related information. Recent IS research has formally recognized the existence of such moderated relationship. For instance, Xu et al. (2012) showed that individuals' dispositional privacy concerns reflect their inherent needs and attitudes toward maintaining privacy, whereas privacy-related behaviour focus on specific assessments of privacy in which their privacy needs are evaluated against information disclosure in a transaction. In essence, dispositional privacy concerns reflect individuals' dispositional privacy beliefs, which are typically stable across various encounters with technologies. Privacy-related behavior, however, focuses on individuals' privacy evaluation in a specific online exchange which involves personal information. Hence, privacy behavior is typically the outcome of context-specific evaluation and formulated in accordance to each unique privacy encounter.

Recent evidence suggests that individuals with higher dispositional concerns are particularly sensitive to privacy-intrusive stimulus and environments (Bassili 1996; Boritz and No 2006). Scholars suggest that individuals with high dispositional privacy concerns are especially susceptible to losses or risks incurred in online information transactions (Angst and Agarwal 2009). For example, in a study examining the adoption of electronic health records, Angst and Agarwal (2009) reported that dispositional privacy concerns moderated the effects of source expertise on opt-in intention. On the

whole, past research suggests that dispositional privacy concern plays a vital moderating role on the relationships between technological characteristics and individuals' intention to use technologies.

Consistent with this logic, this study pays special attention on the moderating roles of social network privacy dispositions. To illustrate, users who have high social network privacy dispositions would be particularly sensitive towards delegated logging and low peer usage. As a result, they would develop a lower intention to use mobile applications. Therefore, we hypothesize:

H2a: There is an interaction effect between logging autonomy and social network privacy dispositions on intention to use mobile application, i.e., autonomous logging has a stronger effect on intention to use mobile application in the high social network privacy dispositions condition than in the low social network privacy dispositions condition.
H2b: There is an interaction effect between peer usage and social network privacy dispositions on intention to use mobile application, i.e., peer usage has a stronger effect on intention to use mobile application in the low social network privacy dispositions condition than in the high social network privacy dispositions condition.

4 METHODOLOGY

4.1 Experimental Design

We plan to conduct two empirical studies to develop and test a new scale of SNPD. The purpose of Study 1 is to develop objective measures for the three dimensions of SNPD (i.e., permeability, ownership, and linkage). Specifically, we plan to first identify the major profile privacy regulation features on Facebook. Using the list of key features, a card sorting exercise will be conducted (Moore and Benbasat 1991). In the exercise, participants will be asked to categorize the features into four groups, namely permeability, linkage, ownership, and others. They will be provided with the descriptions of each of the group names. An expected list of categorized features is provided in Table 1.

Permeability (Disclosed vs. Not disclosed)	*Ownership (Disclosed vs. Not disclosed)*	*Linkage (Allowed vs. Not allowed)*
Profile photo	Status updates	Friend requests
Cover photo	Tagged content	Searchable via email
Mobile phones	Photos	Searchable via phone number
Address	Places	Searchable via search engines
Email	Likes	
Gender		
Relationship		

Table 1. Expected list of sorted features

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. A laboratory experiment with 2 (Logging Autonomy: Autonomous Logging vs. Delegated Logging) x 2 (Peer Usage: Low vs. High) factorial design will be conducted to test the proposed hypotheses. Logging Autonomy will be manipulated by the availability (unavailability) of control over posting made by the mobile application. Whereas autonomous logging will be represented by the provision of control over each posting, delegated logging will be administrated through enabling the application to post on behalf of the subject. Peer usage will be facilitated by manipulating the number of the subject's friends who are using the application. Specifically, in this study, we plan to use 3 friends to represent low peer usage and 35 friends to represent high peer usage.

4.2 Sample and Experimental Procedures

Subjects in this experiment will be students at a large public university. Prior to the experiment, subjects will be asked to provide information about demographics, Internet experience, Facebook experience,

Facebook application experience, and dispositional privacy concerns. At least 128 subjects will be recruited to participate in the experiment. Subjects will be randomly assigned to one of the four experimental conditions. They will be presented with a hypothetical scenario in which they will be asked to evaluate an imaginary mobile application that allows users to keep track of their physical exercise activities and show off their performance with Facebook friends. Subjects will be told that this application requires (or not require) delegating their profiles to the application in making posting on their behalf and the application has been adopted by 3 Facebook friends (or 35 Facebook friends). Subjects will be told to imagine that the scenario is real and read through it carefully. Afterwards, subjects will be instructed to complete a questionnaire that contained manipulation checks and measurement items of the research variables. Finally, subjects will be debriefed and thanked.

5 EXPECTED CONTRIBUTIONS AND LIMITATIONS

Drawing on the information privacy literature and the CPM theory, this study puts forth a theoretical conceptualization to explain the dimensions of users' social network privacy dispositions. Specifically, we offer discussions on (1) the permeability principle, (2) the ownership principle, and (3) the linkage principle, and established the three principles in guiding the formation of social network privacy dispositions – "the extent of static profile disclosure" (permeability), "the extent of dynamic profile disclosure" (ownership), and "the extent of profile searchability" (linkage). We believe that our theory-driven approach to objective social network privacy dispositions will complement existing scales which focus on subjective measurements. The construct social network privacy dispositions is developed to reflect the notion of dispositional privacy concerns because of the widespread use of mobile applications with social media integration. It is strongly rooted in a general conceptual framework drawing on the CPM theory. Therefore, under an assumption that personal profiles are constructed to reflect users' privacy space in online social networks, our scale is expected to be generalizable to other privacy contexts.

It is worthy to note that past research typically operationalizes privacy concerns through subjective measurement items. As a result, respondents could be somewhat promoted about privacy issues and their privacy sensitivity could be elevated. More critically, since respondents must explicitly rate on the measurement items, it could be difficult, if not entrely impossible, to capture respondents' privacy disposition without explicit intrusion or interruption. The objective mesurement scale, which we named social network privacy dispositions, could help assess individuals' privacy dispositions specific to the online social networking environment without explciitly promoting them about potential privacy issues.

Some limitations of this study should be mentioned. It is plausible that individuals' reactions to mobile applications 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 networking platforms and utilities provided by application providers.

6 ACKNOWLEDGEMENT

The authors would like to thank the National University of Singapore (Suzhou) Research Institute (NUSRI) (Project No.: NUSRI2011-005) and UNSW Business School (Business School Research Grant: FBS201, OP001, PS37805) for financial support. This research is partially supported by the Digital Enablement Research Group, UNSW Business School.

7 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.

Altman, I., and Taylor, D. 1973. *Social Penetration: The Development of Interpersonal Relationships*, (Holt, Rinehart & Winston: Oxford, England.

Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *Management Information Systems Quarterly* (33:2), pp 339-370.

Banker, R. D., Kalvenes, J., and Patterson, R. A. 2006. "Information Technology, Contract, Completeness, and Buyer-Supplier Relationships," *Information Systems Research* (17:2), pp 180-193.

Bansal, G., and Gefen, D. 2010. "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems* (49:2), pp 138-150.

Bassili, J. N. 1996. "Meta-judgmental versus operative indexes of psychological attributes: The case of measures of attitude strength," *Journal of personality and social psychology* (71:4), p 637.

Boritz, J. E., and No, W. G. 2006. "Internet Privacy Research: Framework, Review and Opportunities," *Review and Opportunities (June 14, 2006)*).

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* (26:4), pp 639-655.

Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp 451-474.

Flurry Analytics 2014. "Health and Fitness Apps Finally Take Off, Fueled by Fitness Fanatics," Flurry.

Gefen, D., and Ridings, C. M. 2002. "Implementation Team Responsivenss and User Evaluation of Cusomter Relationship Management: A Quasi-Experimental Design Study of Social Exchange Theory," *Journal of Management Information Systems* (19:1), pp 47-69.

Hann, I. H., Hui, K. L., Lee, S. Y. T., and Png, I. P. 2007. "Overcoming online information privacy concerns: An information-processing theory approach," *Journal of Management Information Systems*, *24*(2), pp 13-42.

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.

Jiang, Z., Heng, C. S., and Choi, B. C. F. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp 579-595.

King, R. 2012. "Facebook Reveals Guide for Dealing with Spam, Explicit Content Reports," retrieved from http://www.zdnet.com/article/facebook-reveals-guide-for-dealing-with-spam-explicit-content-reports/

Ma, H., Zhou, D., Liu, C., Lyu, M. R., and King, I. Year. "Recommender Systems with Social Regularization," The Fourth ACM International Conference on Web Search and Data Mining, WSD '11, Hong Kong, China, 2011, pp. 287-296.

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.

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

McMillan, D., Morrison, A., and Chalmers, M. 2013. "Categorised ethical guidelines for large scale mobile HCI," In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 1853-1862.

Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp 192-222.

Parboteeah, D. V., Valacich, J. S., and Wells, J. D. 2009. "The Influence of Website Characteristics on a Consumer's Urge to Buy Impulsively," *Information Systems Research* (20:1), pp 60-78.
Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure.*, (State University of New York Press: Albany, NY.
Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumers Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1).
Shen, X., Tan, B., and Zhai, C. Year. "Implicit User Modeling for Personalized Search," Proceedings of the 14th ACM international conference on Information and knowledge management2005, pp. 824-831.
Sheng, H., Nah, F. F.-H., and Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalizaiton and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), pp 344-376.
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.
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.
Sutanto, J., Palme, E., Tan, C.-H., and Phang, C. W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly* (37:4), pp 1141-1164.
Wang, S. S., and Stefanone, M. A. 2013. "Showing Off? Human Mobility and the Interplay of Traits, Self-disclosure, and Facebook Check-Ins," *Social Science Computer Review* (31:4), pp 437-457.
Westin, A. F. 1967. "Privacy and freedom,").
Xu, H., Teo, H.-H., Tanzer, N., and Agarwal, R. 2012. "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp 1342-1363.
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.