THE EFFECT OF ONLINE PRIVACY INFORMATION ON PRIVACY EVALUATIONS IN USING MOBILE FITNESS APPLICATIONS

Joseph Tam, School of Information Systems, Technology, and Management, UNSW Australia Business School, UNSW Australia, Australia, joseph.tam@student.unsw.edu.au

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

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

This paper proposes an investigation on the effect of online privacy information on privacy evaluation in using mobile fitness applications. Drawing on the justice framework, we identify three key types of annotated privacy information, namely social rating, profile control, and security conformity, to be particularly important to users' transactional privacy trade-off in evaluating mobile fitness applications. To reflect the unique context of mobile fitness applications, we conceptualize profile delegation privacy risks as the transactional cost whereas physical fitness improvements as the transactional benefit in users' privacy trade-off. More importantly, this proposal attempts to elucidate the distinction between dispositional privacy concerns and transactional privacy trade-off. To do so, we plan to investigate the way dispositional privacy concerns moderate the effect of transactional trade-off on disclosure behaviour. The hypothesized research model will be tested by a laboratory experiment. Expected contributions are discussed.

Keywords: Mobile Fitness Applications, Transactional Privacy Trade-off, Dispositional Privacy Concerns.

1 INTRODUCTION

In recent years, in attempts to enhance user's experience, third party application developers have increasingly begun to synergise with Online Social Networks (OSNs) such as Facebook and Twitter to integrate the social function of these OSNs with the features of their applications. Indeed, according to a study performed by IBM, almost 9 out of 10 global marketers had developed and published mobile applications with OSN integrations. Among the diverse types of mobile applications, evidence suggests that mobile fitness applications have undergone the greatest growth in this emerging mobile application market. In recent market survey, over 6,800 mobile fitness applications were identified (Tyler and Blader 2003). More importantly, in terms of usage sessions in a six month period, the study reported that usage of mobile fitness applications was up 62 per cent whereas the overall usage of all the identified mobile applications underwent a 33 per cent growth.

Yet the skyrocketing growth of mobile fitness application usage is not without issues. The ubiquitous use of these fitness applications presents the major threat of unsolicited information exposure, which often transcends traditional online exposures. In particular, the usage of mobile fitness application involves not only involuntary dissemination of personal information, such as names and contact numbers, but also revelation of sensitive health-related information, such as height, weight, and heart-rate. More worryingly, the closely-coupled integration with social media has further exacerbated the privacy threats associated with using mobile fitness applications. Whereas traditional fitness applications typically collect personal information through tracking exercise performance data (i.e., exercise duration, calories burnt, and ambient temperature), mobile fitness applications often leverage the integration with social media to collect not just users' personal information but also acquire the information of their online social networks. The substantial increase in information acquisition ability and ubiquitous monitoring has alerted users about the privacy risks associated with mobile fitness application usage (Smock et al. 2011).

The Information System (IS) literature has substantially advanced understanding towards information privacy. Recent IS research has gone beyond the rim of conceptualization and scale development. In particular, substantial attempts have been put forth to identify unique factors that influence individuals' privacy concerns in the online environment (e.g., Jiang et al. 2013) and classify individuals' behavioural responses after online security issues (e.g., Son and Kim 2008). Overall, past studies reveal that privacy concerns significantly inhibit online exchange, which can be highly detrimental to the survivability and sustainability of online businesses. In attempts to address this challenging issue, IS research has exerted considerable efforts in developing mitigation strategies, such as posting privacy policies, displaying privacy seals, and providing tangible as well as intangible benefits (Chellappa and Sin 2005; Culnan and Williams 2009; Hann et al. 2005; Tsai et al. 2011). However, ample evidence suggests that these mitigation strategies are largely ineffective because individuals typically do not fully understand the policies and protection mechanisms (Moores 2005). Therefore, to address this gap, we propose to investigate whether annotated privacy information will help individuals better understand the way their privacy is handled in using mobile technologies. In particular, this research sets to identify the key annotated privacy information that is crucial to individuals' privacy evaluation in using mobile fitness applications.

Another challenge faced in understanding information privacy is the diversity of privacy trade-off, considered in prior research. For instance, in a study on mobile applications, Sutanto et al. (2013) examined the effectiveness of privacy-safe features and revealed that these features were instrumental in users' evaluation of privacy intrusion and personalization benefits, which were key determinants of their willingness to use the mobile applications. Overall, while IS research has substantiated the role of privacy trade-off, ample evidence underscores the importance of developing contextualized understanding on individuals' cost and benefit evaluation when information privacy is concerned (e.g., Awad and Krishnan 2006; Jiang et al. 2013). Hence, to develop better understanding of users' privacy trade-off, this research explicitly identifies the cost and benefit components which are pertinent to their evaluations in using mobile fitness applications.

Finally, although the IS field has made substantial contributions to the understanding of information privacy, past research has predominately focused on dispositional privacy concerns. Consequently, there is a lack of attention towards transaction-specific privacy concerns. Given the prevalence of privacy trade-off in the IS literature, it is surprising that the transaction nature of a privacy cost and privacy benefit evaluation has been largely ignored. The importance of transaction-specific privacy concerns has received substantial emphasis in other disciplines (Ackerman and Mainwaring 2005; Margulis 2003; Solove 2006). More important, some recent IS studies have revealed preliminary evidence on the unique role of transaction-specific privacy concerns (e.g., Xu et al. 2012). Towards this end, this study extends the information privacy literature by highlighting the distinction between dispositional privacy concerns and transactional privacy concerns and empirically evaluating the respective impacts on usage of mobile fitness applications.

2 LITERATURE REVIEW

2.1 Justice Framework

The information privacy literature suggests that the justice framework is a useful theoretical perspective for examining types of privacy information, which are important to help individuals better understand the way their privacy is handled in using technologies (Culnan and Bies 2003; Son and Kim 2008). The justice framework is typically about how fairly individuals are treated in an information exchange (Colquitt 2001). The justice framework has been widely drawn upon to understand individuals' behaviours in the context of information privacy (e.g., Xu et al. 2011a). More important, vast empirical evidence has substantiated the validity and robustness of the justice framework in guiding the identification of antecedents of privacy-related perceptions across a variety of contexts.

The justice framework identifies several types of justice which are particularly important in individuals' privacy evaluations, namely distributive, procedural, and informational justice (Colquitt 2001; Greenberg 1993). Distributive justice refers to the perceived fairness of outcomes that one receives from the disclosure of private information. In particular, past research has established distributive justice through the equality aspect (Patient and Skarlicki 2010). Distributive justice is often promoted when outcomes are coherent with implicit norms for distribution. While outcomes can vary in a number of possible criteria such as need, rights and duties, evidence suggests that distributive justice is typically formulated based on the fairness of outcomes.

Procedural justice refers to the perceived fairness of the procedures that enabled individuals control over the disclosed information. Whereas distributive justice emphasizes the importance of fair outcomes, procedural justice formalizes the prominence of control in addressing privacy concerns in online transactions. For example, in a study on online social interactions, Jiang et al. (2013) substantiated the central role of control in mitigating privacy concerns through regulating self-disclosure and misrepresentation. Overall, past studies demonstrate the unique role of procedural justice in diluting the detrimental effects of privacy concerns on technology usage.

Informational justice refers to the extensiveness of explanations in the context of privacy violation (Greenberg 1993). Past IS research has revealed substantial evidence on the role of explanations in regulating privacy concerns. For example, Xu et al. (2011b) examined the effectiveness of corporate privacy strategies and found that privacy assurance is not only a mechanism to induce privacy awareness but also helps explain organizational privacy policies.

2.2 Dispositional Privacy Concerns and Transactional Privacy Trade-off

Past IS research has made strong strides towards comprehending and understanding the concerns individuals have for their privacy. In particular, previous studies have focused on examining the effects of dispositional privacy concerns on technology usage behaviours (e.g. Awad and Krishnan 2006; Dinev and Hart 2006; Smith et al. 1996). Unsurprisingly, dispositional privacy concerns have received substantial attention in past IS research. For example, in a study on Internet usage intention, Dinev and Hart (2006) reported that when individuals perceived great interests in the Internet content, they could be very willing to overlook their general privacy concerns and be highly forthcoming towards revealing personal information in online commercial transactions.

While the information privacy literature has made substantial progress in understanding privacy issues in the online environment, some evidence indicates that individuals' general privacy concerns might not be entirely sufficient in predicting their attitudes towards information exchange, and to a larger extend, willingness to use technologies (e.g., Jiang et al. 2013). Overall, emerging evidence suggests that transaction-specific privacy trade-off is an important perspective in understanding individuals' privacy-related behaviours.

Following the spirit of past research examining transactional privacy concerns, this study formally posits a transactional privacy trade-off in which individuals engage a psychological trade-off between the benefit and cost specific to an information transaction. Accordingly, to reflect the unique benefit in the context of mobile fitness application usage, this study examines *physical fitness improvements*, which refers to the extent to which an individual improves his or her athletic ability (Warburton et al. 2006). Consistent with Xu et al. (2012), in terms of transactional privacy cost, we examine *profile delegation privacy risks*, which refers to the extent to which a user is concerned about the possible loss of privacy as a result of personal profile information disclosure.

3 RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

Based on the discussion of the justice framework and information privacy literature, the proposed research model is shown in figure 1.

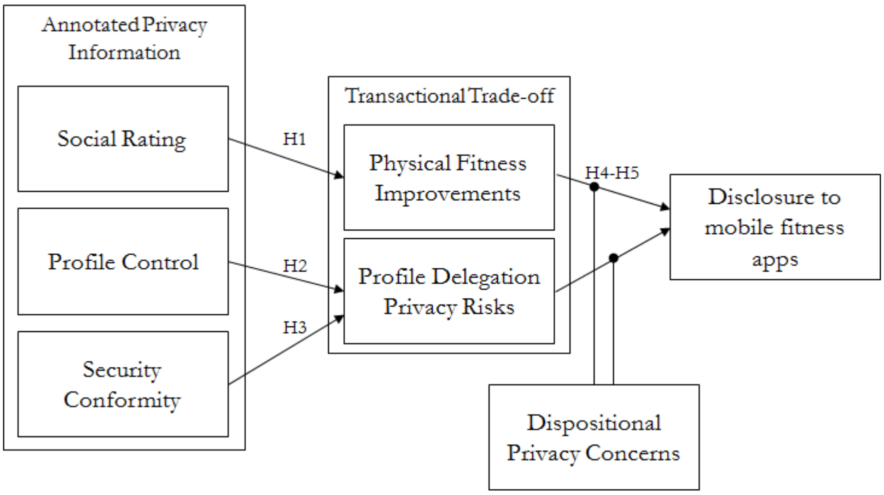
Annotated Privacy Information
Social Rating
Profile Control
Security Conformity
H1
H2
H3
Transactional Trade-off
Physical Fitness Improvements
Profile Delegation Privacy Risks
H4-H5
Disclosure to mobile fitness apps
Dispositional Privacy Concerns

Figure 1. Research Model

This study draws on the justice framework as the overarching framework in identifying three key types of annotated privacy information, which are antecedents of transactional privacy trade-off, namely social rating, profile control, and security conformity. First, according to the justice framework, individuals consider *distributive justice* to evaluate the outcome of an exchange (McNall and Roch 2007). In particular, prior to committing to an exchange, individuals focus on the potential benefits that they expect to obtain in evaluating outcomes (Roberson and Colquitt 2005; Skarlicki and Folger 1997). In mobile fitness application usage, users typically develop their expectation of benefits based on user reviews and user base. Therefore, to reflect the importance of distributive justice in individuals' transactional privacy trade-off, annotated social rating information is examined in this study. Social rating refers to the users' overall satisfaction with their mobile fitness application usage experience (Wang and Wu 2012). Whereas annotated privacy information that suggests high social rating is indicative of users' high degree of functional satisfaction in using the application, annotated privacy information that indicates low social rating is indicative of users' dissatisfaction in their application usage experience.

Second, the justice framework suggests that individuals do not only consider the outcomes but also value *procedural justice* in evaluating an exchange (Alge 2001; Tyler and Blader 2003). When personal information is concerned, individuals are particularly concerned about protecting their information from subsequent malicious usage (Hong and Thong 2013). Corresponding to the important role of procedural justice, this study pays special attention on the way annotated privacy information helps facilitate users' understanding of profile control. Specifically, this study examines annotated profile control information, which refers to the extent to which users are provisioned with control over information exposure after adopting the application. Typically, in mobile fitness applications, profile control is facilitated through autonomous profile control and impersonated profile control. Autonomous profile control allows user complete control over posting made by the application. In contrast, with impersonated profile control, mobile fitness applications assume full control over users' profile.

Lastly, the justice literature underscores the importance of *informational justice* in evaluating an exchange (e.g., Fang and Chiu 2010; Patient and Skarlicki 2010). When online privacy is concerned, users typically evaluate informational justice by considering online companies' security policies and privacy-protection arrangement. Past research examining information privacy suggests that users typically do not entirely understand security policies and privacy-protection arrangement, despite the availability of security statements and privacy seals (e.g., Xu et al. 2012). Therefore, to help users better evaluate the security and privacy protection implemented in mobile fitness applications, we examine annotated security conformity information in this study. Security conformity is defined as whether the mobile fitness application provides security and privacy policies that conform to established legal standards (Liang et al. 2013). While applications in general provide some forms of security and privacy arrangement, the arrangement might not entirely conform to established standard. In general, applications with security conformity provide clear and easily accessible statements of its privacy practices and policies. Furthermore, security conformity is achieved when the purpose of collection and usage of personal information is clearly communicated. In contrast, security unconformity is often realized in applications which provide no privacy statements.

3.1 Determinants of Physical Fitness Improvements

Past research suggests that annotated social rating information is important in reducing users' uncertainty in technology adoption (Gu et al. 2012). In evaluating mobile fitness application, users might be challenged with a huge collection of mobile applications with similar functionalities. Consequently, it becomes highly challenging for users to fully understand all the functionalities and conduct an encompassing evaluation in choosing an application. In such a case, social rating provides users an explicit indication of the quality of the mobile fitness applications (Forman et al. 2008). Research suggests that users tend to rely on social rating in making technology adoption decision in the online environment (e.g., Li and Hitt 2008). In particular, social rating is often considered a collective evaluation of a technology or service, which is objective and unbiased. Therefore, when the annotated information indicates a low social rating, users will be alerted that this could be an indication of poor usage experience, which typically suggests inadequate application quality. Accordingly, users are less likely to expect the application beneficial in helping improve their physical fitness.

However, when the annotated information indicates a high social rating, users might consider the social opinion as an assurance for physical fitness improvements. Indeed, ample evidence substantiates the impact of high social rating on expectation of benefits in using technologies (Dou et al. 2013). Therefore, we expect annotated information that indicates high social rating will induce users' perception of physical fitness improvements in using the mobile fitness app. More important, high social rating also provides users with concrete evidence about the substantial potential in helping them improve their physical fitness.

In sum, we posit:

H1: Compared to annotated information that indicates low social rating, annotated information that indicates high social rating will lead to higher level of perceived physical fitness improvements.

3.2 Determinants of Profile Delegation Privacy Risks

Past research examining self-determinations suggests that autonomy is a key consideration when individuals evaluate the costs of engaging prolonged physical exercises (Ryan and Deci 2000). A high degree of autonomy allows individuals a sense of control in reducing the potential risks. In evaluating mobile fitness applications, annotated information that indicates autonomous profile control is particularly important because autonomy allow users to develop self-organize usage experience and perform activities concordant with their sense of self (Deci and Ryan 1991). Similarly, when personal information is concerned, ample information privacy research has highlighted the importance of control in addressing privacy issues (e.g., Son and Kim 2008; Xu et al. 2010). Drawing on the self-determination literature and past privacy research, it is reasonable to expect that when annotated information indicates autonomous profile control, users are likely to expect a high degree of control over their profile information. As a result, they might expect less risk in delegating their profile to the application.

On the contrary, when annotated information indicates impersonated profile control, users would not expect to have much control over their profile. This is because annotated information that indicates impersonated profile control is not only a clear signal of limited users control over their profile but also is an indication of lack of restriction in improving physical fitness, which is an essential aspect of healthy human functioning (Deci and Ryan 2000). Therefore, we expect annotated information that indicates impersonated profile control will lead to higher level of privacy risks compared to annotated information that indicates autonomous profile control.

Annotated information that indicates security conformity is not only an indication of privacy protection but also implies the commitment of the application providers in delivering high quality mobile applications. In evaluating mobile fitness applications, annotated information that indicates security unconformity suggests a lack of dedicated design in developing the mobile application. Hence, users are likely to deem the application ineffective in protecting their private information.

In contrast, when annotated information indicates security conformity, the thorough considerations in security protection would emphasize the meticulosity in developing the mobile fitness application. As a result, users are likely to deem the application effective in protecting their personal information. Furthermore, past research on uncertainty reduction suggests that detailed explanations are instrumental in reducing individuals' perception of risks in information exchange (e.g., Pavlou and Gefen 2004). Likewise, in evaluating mobile fitness applications, when the annotated information suggests that the application is developed with conformity to security standards, users would expect using the application as less risky, compared to an application with inconformity with established privacy requirements.

In sum, we hypothesize:

H2: Compared to annotated information that indicates autonomous profile control, annotated information that indicates impersonated profile control will lead to higher level of profile delegation privacy risks.
H3: Compared to annotated information that indicates security conformity, annotated information that indicates security unconformity will lead to lower profile delegation risks.

3.3 Impacts of Physical Fitness Improvements and Profile Delegation Privacy Risks

Prior privacy literatures have empirically investigated and verified the negative relationship profile delegation privacy risks have on an individual's willingness to disclose their information (Joinson et al. 2006; Malhotra et al. 2004). Usage of mobile fitness applications not only exposes individuals' profile information to the service provider but also makes them vulnerable to other privacy invasions. Past studies suggest that individuals' perceptions of privacy invasion reduce the intention to disclose personal information in the online environment. For instance, Youn (2005) examined online privacy-protective behaviour and revealed that internet users coped with privacy invasions by limiting participation in online transactions. Accordingly, we propose that the benefit and cost analysis performed by users on perceived physical fitness improvements and profile delegation risks will ultimately determine whether they disclose their information and use the application. Therefore we propose:

H4a: Higher perceived physical fitness improvements are positively related to disclosure of personal information in using mobile fitness applications.
H4b: Higher profile delegation privacy risks are negative related to disclosure of personal information in using mobile fitness applications.

3.4 Moderating Effects of Dispositional Privacy Concerns

Past IS research reveals that individuals would be better able to focus on the benefits of information exchange when their concerns over privacy risk is low (e.g., Dinev et al. 2006). Indeed, users with low dispositional privacy concerns are typically more tolerant to risks in conducting online information exchange (Westin 1996). As a result, they might entirely ignore the potential risks and focus on the potential benefits they could derive in exchange of their personal information. In particular, users who are largely privacy indifferent might simply consider their privacy worthless and hence would be highly sensitive to any benefits they might obtain by disclosing personal information (Joinson et al. 2006). Therefore, when users are of low dispositional privacy concerns, the effect of perceived physical fitness improvement on personal information disclosure will be stronger than when users are of high dispositional privacy concerns.

In contrast, we expect the effect of profile delegation privacy risks on disclosure of personal information will be weaker with users of low dispositional privacy concerns than with users of high dispositional privacy concerns. To illustrate, users who have high dispositional privacy concerns would place the majority of their attention in evaluating information collection and profile control. Consequently, they are highly sensitive and susceptible to the loss of personal information and profile control in using fitness based applications.

Based on these findings, we hypothesize:

H5a: The effect of perceived physical fitness improvements on disclosure of personal information is stronger in the low dispositional privacy concerns condition than in the high dispositional privacy concerns conditions.
H5b: The effect of profile delegation privacy risks on disclosure of personal information is weaker in the low dispositional privacy concerns condition than in the high dispositional privacy concerns conditions.

4 METHODOLOGY

We plan to conduct a 2 (Social Rating: low vs. high) x 2 (Profile Control: autonomous profile control vs. impersonated profile control) x 2 (Security Conformity: security conformity vs. security unconformity) factorial-design laboratory experiment in which subjects will be asked to "test a new privacy enhancement application." The experiment will be designed in such a way that subjects will face a privacy challenging situation in evaluating a mobile fitness application.

Our experiment involved a hypothetical scenario in which subjects evaluate a mobile fitness app. Past IS and privacy research have vastly adapted hypothetical scenarios (e.g., Anderson and Agarwal 2011). While a field experiment could better resemble the reality; however it is not feasible to effectively control and facilitate the experimental conditions in the actual environment. Therefore, a laboratory experiment involving a hypothetical scenario method is deemed relevant for this study.

Subjects will be told that they are looking for a mobile fitness app and find the hypothetical application. The hypothetical application is presented with annotated privacy information, which indicates the level of social rating (low social rating will be represented by zero point; whereas high social rating will be represented by five points), the type of profile control (the annotated information will explicitly indicate the type of profile control with explanations), and the presence of security conformity (the annotated information will explicitly indicate the presence of security conformity/unconformity with explanations).

To ensure sufficient explanatory power (0.8) with a medium effect size (f = 0.25), we plan to recruit 200 subjects to participate in this experiment. One week prior to the main experiment, we plan to administrate online surveys to participants to capture their demographic information, Facebook usage experience, mobile application usage experience, and dispositional privacy concerns.

In the main experiment, participants will be randomly assigned to one of the eight experimental conditions. Participations will be presented with a hypothetical mobile fitness application and a privacy report which gives details on the three experimental aspects of the fitness application. Upon viewing the privacy report, subjects will be asked to complete an online survey which measures the research variables.

5 EXPECTED CONTRIBUTION

This study is expected to make important contributions to three bodies of literature, namely the information privacy literature and technology usage behaviour studies. First, drawing on the justice theory, this study proposes a theoretical framework to explain the role of three annotated privacy-related information and how they combine to affect an individual's willingness to disclose personal information. Specifically, we discuss the notions of annotated social rating, annotated profile control and annotated security conformity and tie them to the three key dimensions of the justice framework – "How do users evaluate the benefits of information exchange?" (social rating), "how is my information exposure controlled?" (profile control), "how relevant and accessible is the information provided?" (Security conformity). We believe that our theoretical approach to how privacy-related information influences personal privacy concerns will build upon existing information privacy research.

Utilising the foundation of the privacy calculus perspective, profile delegation privacy risks and perceived physical fitness improvements are identified as the cost and benefit items influencing the trade-off decision when evaluating their intentions to disclose information on mobile fitness applications. As identified per our literature review, this study is one of the first attempts to investigate a specific privacy trade-off for mobile fitness applications. Finally, in terms of contributing to the information privacy literature, this study is one of the first attempts that investigate the unique roles of dispositional privacy concerns and transactional privacy concerns in the context of fitness application evaluation.

6 CONCLUSION

Overall, this study advances the IS literature by elucidating the distinction between dispositional privacy concerns and transactional privacy concerns. Furthermore, this study explores novel ways of providing privacy information to users in the context of mobile fitness application usage.

7 ACKNOWLEDGEMENTS

The authors would like to thank the Ministry of Education, Singapore (Project No.: T1 251RES1304) for its financial support.

References

Ackerman, M. S. and Mainwaring, S. D. (2005). Privacy issues and human-computer interaction. Computer, 27(5), 19-26.

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, 86(4), 797–804.

Anderson, C. L. and Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Information Systems Research, 22(3), 469-490.

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), 339-370.

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), 13-28.

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), 637.

Boritz, J. E. and No, W. G. (2006). Internet privacy research: Framework, review and opportunities. Review and Opportunities (June 14, 2006).

Chellappa, R. K. and Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 6(2).

Colquitt, J. A. (2001). On the dimensionality of oJustice: A construct validation of a measure. Journal of Applied Psychology, 86(3), 386-400.

Culnan, M. J. and Bies, R. J. (2003). Consumer privacy: balancing economic and justice considerations. Juornal Social Issues, 59(2), 323-342.

Culnan, M. J. and Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX datab. MIS Quarterly, 4(6), 673-687.

Deci, E. L. and Ryan, R. M. 1991. "A motivational approach to self: Integration in personality," in *Nebraska Symposium on Motivation: Perspectives on motivation,* R. Dienstbier (ed.), University of Nebraska Press: Lincoln, pp. 237-288.

Deci, E. L. and Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. Psychological inquiry, 11(4), 227-268.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. European Journal of Information Systems, 15(4), 389-402.

Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 1(17), 2006.

Dou, Y., Niculescu, M. F., and Wu, D. (2013). Engineering optimal network effects via social media features and seeding in markets for digital goods and services. Information Systems Research, 24(1), 164-185.

Fang, Y.-H. and Chiu, C.-M. (2010). In justice we trust: Exploring knowledge-sharing continuance intentions in virtual communities of practice. Computers in Human Behavior, 26(2), 235-246.

Forman, C., Ghose, A., and Wiesenfeld, B. (2008). Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets. Information Systems Research, 19(3), 291-313.

Greenberg, J. 1993. "The social side of fairness: Interpersonal and informational classes of organizational justice," in *Justice in the workplace,* R. Cropanzano (ed.), Lawrence Erlbaum Associates: Hillsdale, NJ, pp. 79-103.

Gu, B., Park, J., and Konana, P. (2012). Research note-the impact of external word-of-mouth sources on retailer sales of high-involvement products. Information Systems Research, 23(1), 182-196.

Hann, I., Hui, K., Lee, T. S., and Png, I. P. L. (2005). Analyzing online information privacy concerns: An information processing theory approach.

Hong, W. and Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empiricals. MIS Quarterly, 37(1), 275-298.

Hui, K. L., Teo, H. H., and T, L. S. Y. (2007). The value of privacy assurance: An exploratory field experiment, MIS Quarterly, 31 (1), 19-33.

Jiang, Z., Heng, C. S., and Choi, B. C. F. (2013). Privacy concerns and privacy-protective behavior in synchronous online social onteractions. Information Systems Research, 24(3), 579-595.

Joinson, A. N., Paine, C., Buchanan, T., and Reips, U.-D. (2006). Watching me, watching you: privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. Journal of Information Science, 32(4), 334-343.

Li, X. and Hitt, L. M. (2008). Self-selection and information role of online product reviews. Information Systems Research, 19(4), 456-474.

Liang, H., Xue, Y., and Wu, L. (2013). Ensuring employees' IT compliance: Carrot or stick? Information Systems Research, 24(2), 279-294.

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), 336-355.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. Journal of Social Issues, 59(2), 243-261.

McNall, L. A. and Roch, S. G. (2007). Effects of electronic monitoring types on perceptions of procedural justice, interpersonal justice, and privacy. Journal of Applied Social Psychology, 37(3), 658-682.

Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? Communications of the ACM, 48(3), 86-91.

Patient, D. L. and Skarlicki, D. P. (2010). Increasing interpersonal and informational justice when communicating negative news: The role of the manager’s empathic concern and moral development. Journal of Management, 36(2), 555-578.

Pavlou, P. A. and Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research, 15(1), 37 - 59

Roberson, Q. M. and Colquitt, J. A. (2005). Shared and configural justice: A social network model of justice in teams. Academy of Management Review, 30(3), 595-607.

Ryan, M. R. and Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American Psychologist, 55(1), 68-78.

Skarlicki, D. P. and Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. Journal of Applied Psychology, 82(3), 434-443.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: Measuring individuals’ concerns about organizational practices. MIS Quarterly 20(2), 167-196.

Smock, A. D., Ellison, N. B., Lampe, C., and Wohn, D. Y. (2011). Facebook as a toolkit: A users and gratification approach to unbundling feature use. Computers in Human Behavior, 27(6), 2322-2329.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-564.

Son, J.-Y. and Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly, 32(3), 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), 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), 1141-1164.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254-268.

Tyler, T. R. and Blader, S. L. (2003). The group engagement model: Procedural justice, social identity, and cooperative behavior. Personality and social psychology review, 7(4), 349-361.

Van Slyke, C., Shim, J., Johnson, R., and Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7(1), 16.

Wang, H.-F. and Wu, C.-T. (2012). A strategy-oriented operation module for recommender systems in E-commerce. Computers & Operations Research, 39(8), 1837-1849.

Warburton, D. E., Nicol, C. W., and Bredin, S. S. (2006). Prescribing exercise as preventive therapy. Canadian Medical Association Journal, 174(7), 961-974.

Westin, A. F. (1996). Privacy in the workplace: How well does american law reflect american values. Chi.-Kent L. Rev., 72, 271.

Xu, H., Dinev, T., Smith, J., and Hart, P. Year. "Information privacy concerns: linking individual perceptions with institutional privacy assurances," Journal of the Association for Information Systems, Citeseer2011a.

Xu, H., Luo, X., Carroll, J., and Rosson, M. B. (2011b). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42-52.

Xu, H., Teo, H.-H., Tan, B. C. Y., 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), 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), 135-174.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach, Journal of Broadcasting & Electronic Media, 49(1), 86-110.