DECISION SCIENCES INSTITUTE

Intention to Delegate Profile On Facebook Apps Usage

Trang Nguyen
National Cheng Kung University
Email: trangnth@uel.edu.vn

Jengchung Victor Chen
National Cheng Kung University
Email: victor@mail.ncku.edu.tw

ABSTRACT

To go along with the Digital Age, Facebook has created Facebook apps in order to enhance users' engagement on social network. The underlying motive of apps creation is to collect more information from their users. Based on dual factors of the privacy trade-off and theory of communication privacy management, this study investigates the role of privacy concern and social rewards as potential contributors to user's intention to delegate profile on SNSs apps. Survey and experiment will be conducted to collect data. Partial least squares (PLS), a second-generation causal modeling technique, is used to test the theoretical model.

KEYWORDS: Profile delegation, Privacy concern, Social rewards.

INTRODUCTION

The introduction of third-party developed applications (Facebook apps) has significantly captured the attention of people around the global and now Facebook users can easily download it from any Apps providers. The aim of Facebook apps is to increase the usage of online social networks and intensify users' social engagements. In fact, an implicit purpose of any mobile app or service is that passively collect users' personal information. For example, before using Facebook apps, it is required user to log in by Facebook profile or Gmail, then the app provider can gather users' profile information. Some researches show that Facebook apps take advantages for user to express their exhibitionism (S. S. Wang & Stefanone, 2013). In particular, Facebook apps often attach an impersonation feature that automatically post information without users' permission whenever they install the app in their device.
It is said that this action possibly attracts attention of individuals; however, sometimes they might feel irritated because of privacy invasions (Hart, Ridley, Taher, Sas, & Dix, 2008). Besmer and Lipford (2010) studies show that their personal information is being revealed more than they realized to applications. Wang and her coauthors (N. Wang, Xu, & Grossklags, 2011); (N. Wang, Grossklags, & Xu, 2013) decided to embark on taking on a research related to users' privacy behaviours and perceptions when they installed Facebook apps.
Whereas several recent reports on Information Systems (IS) has mainly concentrated on problems created by users' personal information collection ((Malhotra, Kim, & Agarwal, 2004), Son and Kim (2008)), little is known about the privacy concern regarding to extended scope of information collection. Dissimilar to traditional online commercial transactions and online social interactions, Facebook apps nowadays do not only require revelation of profile information during installation but also involve delegating profile control to the app. By delegating profile control, static information is collected during installation, and furthermore, Facebook apps acquired extended access to user profiles. The ability to access to users' profile beyond

installation enables Facebook applications to continue monitoring user profile information changes over an extended period of time.

The disclosure of the high granularity of personal information possibly increases the risk of compromising or misusing personal information (Awad & Krishnan, 2006). The paradox of enjoying personalized services and the risk of losing personal information is evident in social networks. In order to encounter to such paradox, Facebook app producers are seeking solutions to show users that they would receive more benefits than the potential cost caused by inappropriate manner. Previous researches on the privacy calculus model addressed two path of the direct effects on perceived benefits and risks inducing the ultimate intention to disclose personal information (Posey, Lowry, Roberts, and Ellis (2010); T. Wang, Duong, and Chen (2016); Zhao, Lu, and Gupta (2012), Keith, Thompson, Hale, Lowry, and Greer (2013)). Existing studies on delegation profile to Facebook apps only focus on the interaction between general privacy concern and transactional privacy concern (Choi & Land, 2016) . As the best of my knowledge, lack of research working on the integration of privacy concern and social rewards in an extended scope of information collection. To fill this gap, this study aims to examine the impact of dual factors of the privacy trade-off on profile delegation intention in order to provides a holistic view of the positive and negative forces that influence behavior beyond disclosure management.

This paper is organized as follows: the next section clarifies the theoretical foundations of the study. The third section explains the research model and hypotheses. The fourth section describes the research methodology.

LITERATURE REVIEW

Communication privacy management theory

This study uses Communication Privacy Management Theory (CPMT) that was proposed by (Petronio, 2012). By the ground of privacy theory (Altman, 1975), CPMT developed that privacy is a process of closing and opening boundaries to others (Zlatolas, Welzer, Heričko, & Hölbl, 2015)

This theory demonstrates Facebook apps users' decision making towards the social information interaction. Specifically, CPM theory reaffirm that people put up privacy boundaries above all in order to make sure their privacy protected. And in case of their information ownership is confronted, consequently, these boundaries would be threatened. Based on that theory, this study exploits three application-specific attributes that dispute information ownership in the contexts of using Facebook apps, called information collection, information relevance and profile control. While information collection concentrates on the profile information acquisition before app adoption, the management of information encompasses profile control that exposure after app adoption.

Privacy calculus model

Privacy calculus model (Laufer & Wolfe, 1977) is classical model to analyze the privacy perceptions and behaviors of IT users. Privacy calculus is an attribute that reveals how users decide to disclose their private information, based on the consideration between the disclosure needs and privacy concerns in a specific information-disclosure context (H. Xu, Teo, Tan, & Agarwal, 2009).

In fact, privacy calculus play an functional role of consumers' expectations toward the positive and negative results, before deciding to what kind of information they are willing to disclose and how much (T. Li & Unger, 2012). Several recent reports show the benefits and risks of privacy calculus in common activities such as traditional transactions (Culnan & Armstrong, 1999), online transactions (Dinev & Hart, 2004), government surveillance (Dinev, Hart, & Mullen, 2008), and location-aware marketing (H. Xu, Luo, Carroll, & Rosson, 2011).

As such, users maybe disclose personal information Facebook apps when they perceive more benefits than risks. In support, the success of mobile service personalization strongly depends on the collection of information as well as the analysis of data. When receiving personalized services, users also encounter the threat of having their personal information as compromised as a consequence of the lack of security control across servers and/or client sites. Therefore, the perception of benefits and risks must be take into account simultaneously in order to get to know the users' intention to disclose their personal information via Facebook apps usage. Combining two approaches for examining both benefits and risks of delegating personal information via Facebook apps, this study proposes perceived benefits as social rewards derived from self-presentation and personalized services and perceived risk as privacy concern with three factors of included information collection, profile control and information relevance.

HYPOTHESES/MODEL

Information collection and Privacy concern

According to CPM theory, in evaluating private situations, individual pays strong attention to confront to information ownership, which illustrates the rights to control the privacy boundary to conceal or reveal personal information (Petronio & Altman, 2002). In essence, despite of being shared with the others, users expect to retain full ownership of their privacy boundaries. The previous research also finds that individuals always consider the importance of how personal information is collected and they also often feel that they should take over its subsequent usage (Malhotra et al. (2004), Smith, Dinev, and Xu (2011), Stewart and Segars (2002)). Applying the CPM theory in the Facebook apps usage settings, information collection could threat information ownership (Dinev & Hart, 2006). Information collection consists of two important kinds, which are global and local scope. In detail, global scope refers to information that beside users' own profile information, there are other information that also relates to the profiles of user's online social media (N. Wang et al., 2011). On the other hand, local information collection is a wide range of profile information such as email addresses, birthdays, profile names (Choi, Lee, & Land, 2015). Moreover, when we only considers individuals' personal information in information collection, such information would threaten only our personal privacy,hence, compose a risk to their personal boundary ownership in a particular transaction (Petronio & Altman, 2002).

In the research context, the scope of information collection might range from a local scope to a global scope. Regarding to local information collection scope, individual users' profile information is obtained by Facebook apps. As a result, the Intention to install the application predominantly challenges users' personal boundary ownership in information transaction. In contrast, a global scope of information collection broadens the extent of information acquisition beyond users' profile information by acquiring the profile information of their online social network friends. Consequently, in the installation apps, a global information collection scope does not only challenge individual personal boundary ownership but also confronts the collective privacy boundary. Therefore, compared to a local scope of information collection, a global scope of information collection would escalate privacy threats to the entire online social network, and hence elevating users' privacy concerns. Thus, the researcher posits:

H1. Compared to a local scope of information collection, a global scope of information collection will increase privacy concern.

Profile control and Privacy concern

In the context of Facebook app usage, personal privacy boundaries are able to be confronted by the losing control over personal profiles from users. This study thereby tests the way posting control can be threatened when Facebook apps make postings on behalf of users. Previous IS research has identified exposure control as the major consideration in personal evaluation of technology. For instance, Son and Kim (2008) states that IT users occasionally do not disclose their personal information because of privacy concern. Similarity, Hui, Teo, and Lee (2007) demonstrates that people do not individuals did not only utilize exposure control by limiting the amount of disclosed information, but also manipulate information to protect their privacy in any information transaction. Furthermore, when users keep controlling over posting, they might feel less concerned about privacy invasions and more appreciated to the value that obtains from the information transaction. On the other hand, in case of that users are not given such options (i.e., applications make posting on their behalf), the exposure becomes compulsory, hence, users turn out to be more anxious about their private data in the installation transaction. Moreover, the information privacy research found out that the ability to utilize authority over posting can improve users' benefit analysis. In fact, control is about one's ability to take charge of subsequent usage of its personal information (Malhotra et al., 2004). Previous studies reveal the essential of control by emphasizing on confidentiality and secondary usage, latest research have pointed out control as one of the essential factors. It is suggested that accessible and usable problems are more appropriately managed by ''controlling over who has access to personal data, how personal data are used'' (Phelps, Nowak, & Ferrell, 2000). In the online settings, individuals could be conferred by information control functionally and environmentally. Specifically, functional control is about the enforcement of integrity for personal information (Hu, Pavlou, & Zhang, 2007). With the right information, users can make sure that the impression is devised for them properly. Moreover, environmental control is about the ability to manage unintentional self-exposure (Olivero & Lunt, 2004). In fact, the feeling of vulnerable is evoked by the loss of environmental control, and it turns out to be uncomfortable in transactions (Goffman, 1959).

In the context of Facebook apps usage, by allowing users to have autonomous control over posting made by applications, they could better control over disclosing information about themselves, hence making sure that the posting is consistent with their desired social images in online transactions. On the other hand, by impersonating profile control, users not only capitulate functional control but also lack of their environmental control in managing information exposure in online settings. Thus, the second hypothesis is stated:

H2. Compared to autonomous profile control, impersonated profile control will increase transactional privacy concerns.

Information Relevance and Privacy concern

A website requesting user's information if those information would be relevant to and beneficial for the purpose or function of the website itself (Zimmer, Arsal, Al-Marzouq, & Grover, 2010) . State-of-the-art research singles out several types about information science that have related to subjective relevance. The first is affective relevance (the emotional response), topicality relevance (the way it defines the subject of interest), cognitive relevance (the influence of that to state of knowledge), and situational relevance (pragmatic utility) (Y. Xu, 2007).

By and large, among those factors having positive influence on user attitude toward information revealing, information relevance plays an significant role (Zimmer et al., 2010). The past study reveals that the information that requests to the users would eliminate the risk of perception of information disclosure. Zimmer et al. (2010) illustrates that employees feel invaded in their

privacy when irrelevant information of themselves have been collected. Moreover, the user's choice is affected by the relevance of the information while making intention collected (Zimmer et al., 2010)(Zimmer et al., 2010).
When using Facebook apps, if the information is related to the function to the apps, privacy concern will be eliminated in users and vice versa. Therefore, the following hypothesis will be:

*H3: Lower relevance of information will increase higher privacy concern***.**

Self-presentation and social rewards

Based on privacy calculus theory, consumers carry out a risk–benefit analysis when deciding to disclose personal information in a digital context. The most of users recognize the dangers of disclosing personal information without sufficient assurance, and the risk–benefit analysis turns out to be a common practice in the digital world (Milne, Rohm, & Bahl, 2004). It is true that users occasionally analyze the potential benefits as well as risk that they maybe receive or encounter before disclosing their private information to app providers.
Taking a broader view, self-presentation is the first perceived benefits (social rewards). Self-presentation implies to the behavior of consumers to intentionally regulate their personal image in the eyes of others. In the context of Web 2.0, users might control over their own information by showing, editing , and managing for the sake of self-presentation such as online personal brands (Labrecque, Markos, & Milne, 2011). Consequently, the stranger can see these private information, including demographic profiles, photos, selfies, videos, and friends lists (E. Lee, Ahn, & Kim, 2014). In fact, this digital information may offer more social cues than ones revealed by body language. For instance, the main Facebook's function are check-in, like, comment, and share that allow Facebook users to present and manage their identity and image (E. Lee et al., 2014). Self-presentation also is characterized by an initiative of communication behavior that triggers individuals' motivation to disclose or share personal information, as well as support them in building and reserving their public self-image (Lee-Won, Shim, Joo, and Park (2014); Rui and Stefanone (2013)). BY sharing app's results, for example about their personalities or future predictions, individual can realize the behavior of presenting their self-presentation on Facebook apps. Based on the preceding discussion, the researcher proposes the following hypothesis:
H4. Self-presentation behavior is positively related to perceived social rewards to delegate profile to Facebook apps

Personalized services and social rewards

Together, the second driving force is personalization. Personalization requires collecting and exploiting personal information to customize services and contents to the right target consumers. In fact, consumers are generally willing to reveal their personal information to receive personalized services, such as birthday coupons and recommended books (Y. Li (2014); Taylor, Davis, and Jillapalli (2009)). Research shows that customers often greeting the services or product that is personalized, for example offering an ad in exchange for a specific product for which they have been looking. These personalized facts of immediacy can improve the intentions of disclose embarrassing and descriptive information among users (Bandura (1986); D. Lee and LaRose (2011)).
After customers provide the apps providers their personal information, those providers will use them to analyze and create a personalized service for users. For instance, Facebook app has been offered several of personalized services such as fortune telling, games, comics, fun animation for the benefits of users.

H5. Personalized services are positively related to perceived social rewards to delegate profile to Facebook apps

Privacy Concern to Willingness to delegate profile

Information privacy concern is security of information interaction, being in control of information, and whether the collector of information will behave properly**.** Information privacy can be defined as user being able to control their personal information revelation (Bélanger and Crossler (2011)). In other word, privacy reflects the right of deciding and managing what personal information is offered to other side (Bansal, Zahedi, & Gefen, 2016). Before the invention of computers, privacy has become sensitive concern for a long time (Wu, Huang, Yen, & Popova, 2012).

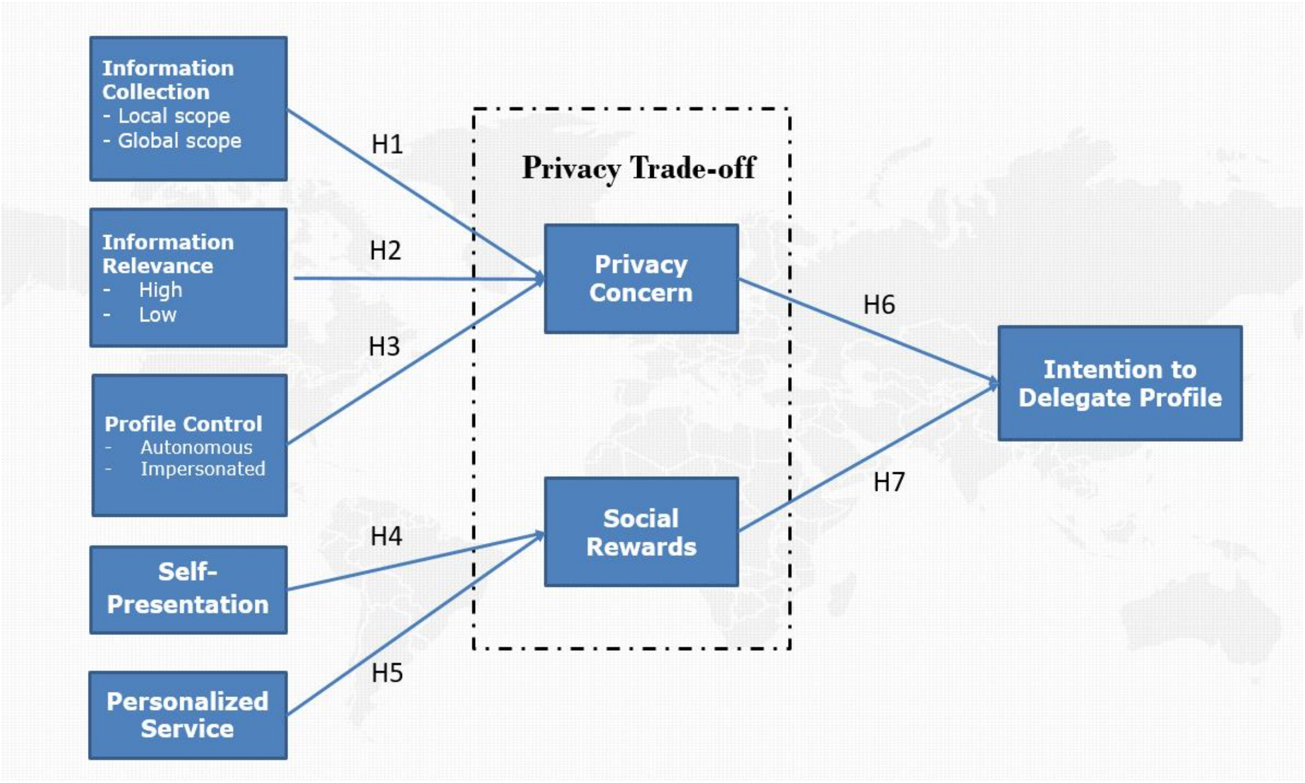
In the online settings, privacy concern is an increasingly important issue for both organizations and individuals. With the approach of innovation that upgrades information accumulation, information sharing, and information mining systems, the idea of Internet data protection has gotten to be as widespread as the information themselves. Krasnova, Kolesnikova, and Guenther (2009)) and Wu et al. (2012) demonstrates that privacy concern significantly effect on self-disclosure negatively. Moreover, self-disclose is termed as the action of exposing personal information to other side (Archer, 1980). Research from Acquisti and Grossklags (2005) illustrates that self-exposure pays little mind to their protection issues (security concern). Additionally, research from Dinev and Hart (2006) reported that privacy concerns decreases the willingness to disclose their personal information on the Internet.

This study focuses on the influence of privacy concerns on individuals' Intention to delegate profile to a Facebook app, which reflects to the extent to which person is prepared to relinquish control over their personal profiles to install the Facebook app. It is worthy to note that profile delegation goes beyond the disclosure of static profile information, which is equivalent to information provision widely investigated in past information privacy research. Rather, profile delegation involves entrusting to manage user's profile to the app, which will be authorized not only to collect static profile information but also grant permission to monitor subsequent profile information changes and make impersonated posting on behalf of users. Profile monitoring exposes users to extended surveillance. Impersonated posting goes beyond mere information collection by disseminating usage information through status updates.

Information Boundary Theory (IBT) provides the theoretical explanation on the relationship between transactional privacy concerns and individuals' willingness to delegate profile to Facebook apps (Stanton, Stam, Mastrangelo, & Jolton, 2005). The theory posits that individuals form privacy spaces around themselves and protect the spaces by erecting psychological boundaries. More importantly, researchers suggest that these boundaries play important roles in individuals' willingness to disclose information in online transactions (Petronio & Altman, 2002). Similarly, in the context of Facebook apps evaluation, when privacy concerns are high, individuals will be motivated to protect their privacy spaces and hence they will be less willing to delegate their personal profile to the Facebook app. In this way, the sixth hypothesis is:

H6: Higher privacy concern will decrease willingness to delegate profile

Based on proposed hypothesis, this research comes up with a research framework as showed below:



METHODS

Experimental design

Stage 1

An online survey with 350 participants is employed to collect data for hypothesis testing regarding to self-presentation, personalized services, social rewards in the first survey. All questionnaire items are adapted from the existing literature to fit the current research context and are assessed with a seven-point Likert scale ranging from 1 (“strongly disagree”) to 7 (strongly agree”).

Stage 2

A scenario-based experiment with 2 (information collection: local scope vs. global scope) x 2 (profile control: autonomous vs. impersonated) x 2 (information relevance: high vs. low) factorial design is conducted to test the proposed hypotheses. Participant will be presented with a hypothetical scenario in which they evaluate an imaginary Facebook app. Information collection is manipulated by the type of profile information collected by the Facebook app. In the manipulation, the researcher uses collection of user’s own profile information to represent the local scope of information collection. The collection of user’s own profile information as well as his or her friends’ profile information is chosen to represent the global scope of information collection. Profile Control is facilitated by manipulating the extent of subject’s control over profile impersonation. Autonomous profile control is facilitated by providing subject control over posting made by the application. In contrast, impersonated profile control is administrated by enforcing posting-on-behalf by the application. In manipulation check for ‘Information, users will be asked to provide personal information which are relevant or not relevant.

Stage 3

Participants will be asked to answer the 2nd survey for measuring intention to delegate profile to Facebook apps.

Measurement and Control variables

Self-presentation

I delegate profile to present myself in a realistic manner
I delegate profile to present my self-concept
I delegate profile to present my individual characteristics

Personalized services

Facebook apps can provide me with personalized information to my activity context
Facebook apps can provide me with more relevant personal information tailored to my preferences or personal interests
Facebook apps can provide me with the type of information that I might like

Privacy concern

I am concerned that the Facebook app is collecting too much profile information.
I am concerned that the Facebook app provider may not take measures to prevent unauthorized access to the collected profile information.
I am concerned that the Facebook app provider may not devote enough time and effort to preventing unauthorized access to the collected profile information.
I am concerned that the Facebook app provider may not well establish the procedures to correct errors in the collected profile information.
I am concerned that the Facebook app provider may not devote time and effort to verify the accuracy of the collected profile information.
I am concerned that the Facebook app provider may use the collected profile information for other purposes without notifying me or getting my authorization.
I am concerned that the Facebook app provider may sell the collected profile information to other companies.

Social rewards

Delegate profile may help to establish relationship with my friends.
Delegate profile may help to gain socio-emotional support from others
Delegate profile may help me joining in some social groups

Intention to delegate profile to Facebook apps

I am interested to have my Facebook profile delegated to the Facebook app.
It is likely that I would allow the Facebook app to take over my Facebook profile.

Control variables

Variables such as age, gender, Internet experience, Facebook experience, and Facebook applications experience, which could potentially affect Intention to delegate profile to Facebook apps are included in the research model as control variables.

Data analysis

Descriptive statistical analysis has been used to illustrate the means, and standard deviation of each research variable to have a better understanding the characteristics of each variable. Analysis of Variance (or t-test) is used to compare and determine the significance of means. If the means of the two variables compared vary significantly, that they can be said to be correlated.

The measurement that is used to purify and identify their dimensionality, principle components factor analysis was applied to condense the collected data into certain factors. In addition, item-to-total correlation and internal consistency analysis (Crobach's alpha) will be applied to confirm the reliability of each research factor.

Partial least squares (PLS), a second-generation causal modeling technique (Chin (1998); Fornell and Bookstein (1982); Wold, Martens, and Wold (1983)), is used to test the research model. A multigroup PLS analysis was conducted by comparing differences in coefficients of the corresponding structural paths for each research sites.

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26-33.

Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

Archer, R. L. (1980). Self-disclosure. *The self in social psychology*, 183-205.

Awad, N. F., & 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*, 13-28.

Bandura, A. (1986). Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *Mis Quarterly, 35*(4), 1017-1042.

Besmer, A., & Lipford, H. R. (2010). *Users'(mis) conceptions of social applications.* Paper presented at the Proceedings of Graphics Interface 2010.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295-336.

Choi, B. C., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management, 53*(7), 868-877.

Choi, B. C., Lee, N. T., & Land, L. P. W. (2015). *The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage.* Paper presented at the Pacific Asia Conference on Information Systems.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science, 10*(1), 104-115.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research, 17*(1), 61-80.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214-233.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of marketing research*, 440-452.

Goffman, E. (1959). The moral career of the mental patient. *Psychiatry, 22*(2), 123-142.

Hart, J., Ridley, C., Taher, F., Sas, C., & Dix, A. (2008). *Exploring the facebook experience: a new approach to usability.* Paper presented at the Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges.

Hu, N., Pavlou, P. A., & Zhang, J. J. (2007). Why do online product reviews have a J-shaped distribution? Overcoming biases in online word-of-mouth communication.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *Mis Quarterly*, 19-33.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). " It won't happen to me!": self-disclosure in online social networks.

Labrecque, L. I., Markos, E., & Milne, G. R. (2011). Online personal branding: processes, challenges, and implications. *Journal of Interactive Marketing, 25*(1), 37-50.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues, 33*(3), 22-42.

Lee, D., & LaRose, R. (2011). The impact of personalized social cues of immediacy on consumers' information disclosure: A social cognitive approach. *Cyberpsychology, Behavior, and Social Networking, 14*(6), 337-343.

Lee, E., Ahn, J., & Kim, Y. J. (2014). Personality traits and self-presentation at Facebook. *Personality and Individual Differences, 69*, 162-167.

Lee-Won, R. J., Shim, M., Joo, Y. K., & Park, S. G. (2014). Who puts the best “face” forward on Facebook?: Positive self-presentation in online social networking and the role of self-consciousness, actual-to-total Friends ratio, and culture. *Computers in Human Behavior, 39*, 413-423.

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems, 21*(6), 621-642.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision support systems, 57*, 343-354.

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

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers’ protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217-232.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*: Suny Press.

Petronio, S., & Altman, I. (2002). Boundaries of privacy.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

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

Rui, J. R., & Stefanone, M. A. (2013). Strategic image management online: Self-presentation, self-esteem and social network perspectives. *Information, Communication & Society, 16*(8), 1286-1305.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *Mis Quarterly, 35*(4), 989-1016.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: a taxonomy and a nomological model. *Mis Quarterly*, 503-529.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security, 24*(2), 124-133.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information systems research, 13*(1), 36-49.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203-223.

Wang, N., Grossklags, J., & Xu, H. (2013). *An online experiment of privacy authorization dialogues for social applications.* Paper presented at the Proceedings of the 2013 conference on Computer supported cooperative work.

Wang, N., Xu, H., & Grossklags, J. (2011). *Third-party apps on Facebook: privacy and the illusion of control.* Paper presented at the Proceedings of the 5th ACM symposium on computer human interaction for management of information technology.

Wang, S. S., & 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), 437-457.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542.

Wold, S., Martens, H., & Wold, H. (1983). The multivariate calibration problem in chemistry solved by the PLS method. *Matrix pencils*, 286-293.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889-897.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). 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., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Xu, Y. (2007). Relevance judgment in epistemic and hedonic information searches. *Journal of the American Society for Information Science and Technology, 58*(2), 179-189.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce, 16*(4), 53-90.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management, 47*(2), 115-123.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*, 158-167.