Information & Management xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage

Ben C.F. Choi *, Lesley Land

The University of New South Wales, UNSW Business School, School of Information Systems, Technology and Management, Sydney, Australia

ARTICLE INFO

Article history:
Received 29 August 2015
Received in revised form 21 January 2016
Accepted 12 February 2016
Available online xxx

Keywords:
General privacy concerns
Transactional privacy concerns
Information control

ABSTRACT

This study elucidates the role of control in the context of information privacy to develop a better understanding of the interactions between general privacy concerns and transactional privacy concerns. We posit that general privacy concerns moderate the effects of information collection and profile control on transactional privacy concerns, which in turn, influence willingness to delegate profile to Facebook apps. We test the research model in the context of Facebook apps installation. Results support our propositions. Theoretical contributions and practical implications for service providers and users are discussed.

1. Introduction

In recent years, Facebook has introduced third-party developed applications (Facebook apps), which have attracted massive usage across the globe. Facebook apps are available to all Facebook users through the Facebook App Center; they are designed to intensify social interactions and usage of online social networks. Usage of Facebook apps typically requires users to install the app on their Facebook profile and in doing so, users expose some of their profile information to the app provider. Previous studies found that Facebook apps usage facilitates exhibitionism, which may manifest in show-off behaviours on online social networks [47]. In particular, Facebook apps often incorporate an impersonation feature, which allows posting of app usage on behalf of users. While individuals might be attracted by the attention generated from Facebook apps postings, individuals are at times deterred by privacy invasions triggered by these automated postings [19].

This paper has three objectives. First, this research aims to enrich the IS literature by developing and testing a model that explains Facebook app usage in order to provide a richer conceptual description of information privacy. More specifically, our study focuses on users' initial evaluation of a Facebook app. Past Information Systems (IS) research has substantially advanced our understanding of information privacy (e.g., Refs. [8,22,41]). While IS literature has explored several aspects of information privacy, its primary focus has been on issues triggered by personal information collection (e.g., Refs. [28,42]). As a result, to the best of our knowledge, there is limited research done to elucidate privacy issues associated with an extended scope of information collection. Drawing on Communication Privacy Management (CPM) theory [33], we examine how extended information collection (such as the collection of network information) and profile control (such as impersonated posting) influence users' evaluation of privacy.

Second, this paper attempts to shed light on the interplay between general privacy concerns and transactional privacy concerns in driving Facebook apps usage behaviour. Ample IS research has focused on the importance of general privacy concerns in driving disclosure behaviour and technology usage (e.g., Refs. [5,45]) and emerging studies have revealed the importance of transactional privacy concerns (e.g., Refs. [23,49]). Hence, following past research examining transactional concerns for privacy, this study emphasizes the distinction between general privacy concerns and transactional privacy concerns.

Lastly, this study examines the impact of privacy evaluation on profile delegation in order to enrich our understanding of privacy-related behaviour beyond disclosure management. Past IS research has identified several important privacy-related behaviours, such as self-disclosure and misrepresentation (e.g., Refs. [22,42]). While extant studies have extended understanding of the prevalence of information provision, rarely has past research explored the importance of continued exposure. Unlike traditional online commercial transactions and online social interactions, Facebook apps do not only require revelation of profile information during installation but they also involve delegating profile control to the app. By delegating profile control, static information is collected

* Corresponding author. Tel.: +61 65423161205.
E-mail addresses: chun.choi@unsw.edu.au (Ben C.F. Choi), l.land@unsw.edu.au (L. Land).

http://dx.doi.org/10.1016/j.im.2016.02.003
0378-7206/

during installation, and furthermore, Facebook apps acquire extended access to user profiles. The ability to access user profile beyond installation enables Facebook apps to continue monitoring user profile information changes over an extended period of time. More critically, a majority of Facebook apps go beyond merely collecting information by making posting on behalf of users. Hence in this study, we address how privacy evaluation impacts profile delegation.

This paper is organized as follows: the next section explicates the theoretical foundations of the study. The third section explains the research model and hypotheses. The fourth section describes the research methodology. The fifth section reports the tests of the research hypotheses. This paper concludes with a discussion of its contributions, limitations, and future research directions.

2. Literature review

2.1. Communication privacy management theory

Communication privacy management (CPM) theory posits that because privacy is an inherent need, individuals will erect boundaries around their personal information and regulate access based on implicit privacy rules [32]. Personal privacy boundaries might be transformed to collective privacy boundaries when individuals' personal information is shared among friends. Collective privacy boundaries are constructed to protect information privy to a group, such as a dyad, organization, or social network. Be it personal privacy boundaries or collective privacy boundaries, theorists agree that these privacy boundaries are governed by some implicit rules, which can typically be implied by the types of information and social context in which the boundaries are challenged. More important, Petronio [33] considers information ownership as the key factor in individuals' assessment of privacy situations.

CPM theory has been widely drawn upon as the theoretical basis in investigating IT usage behaviour. For example, in a study examining privacy issues in e-health, Zohar and Tenne-Gazit [51] found that individuals' e-health website evaluations drove their disclosure of medical histories. More important, preliminary evidence underscores the relevance of CPM theory in explaining individuals' behaviour when collective privacy is challenged. Although the disclosure of personal information often triggers privacy concerns, in general, the exposure of others' personal information is known to be viewed as betrayal and selfish [39]. On one hand, the disclosure of personal information is typically a voluntary decision in which individuals reveal personal information, at their own privacy costs, for personal gains [16]. On the other hand, when disclosure exposes information about friends, individuals are essentially gaining benefits at the privacy costs of others.

2.1.1. Challenges to information ownership – information collection

According to CPM theory, in assessing private situations, individuals pay special attention to challenges to information ownership, which describes the rights to control the privacy boundary to conceal or reveal personal information [33]. Indeed, individuals expect to retain full ownership of the privacy boundaries even though their personal information has been shared with others. In fact, evidence suggests that individuals place importance in how personal information is handled and often feel that he or she should have total control of its subsequent usage, despite having shared the information with others [28,40,44].

Consistent with CPM theory, in the context of Facebook apps usage, information ownership can be challenged by information collection. This study focuses on two scopes of information collection, namely a local scope and global scope of information collection, which are particularly prevalent when individuals evaluate Facebook apps. A local scope of information collection refers to the acquisition of users' own profile information. When local profile information is collected, a user's personal information, which resides on his or her personal profile, is acquired by the Facebook app. Local information collection often involves the acquisition of an extensive range of profile information, such as profile names, email addresses, genders, and birthdays [48]. Users typically assume ownership of their profiles and expect to be in control over its exposure [13,37]. The collection of local information is vital to Facebook apps usage experience because profile information allows application providers to provide uniquely tailored products, content, and services to individual users [24].

Global information collection does not only involve the acquisition of a user's own profile information but also entails information collection that involves the profiles of those in his or her online social networks [48]. When global information is collected, friends' profile information (such as his or her list of friends, their profile names, email addresses, genders, and birthdays) is collected in addition to the user's own profile information. Since users are entrusted with their friends' profile information, users often assume to have a stake of ownership over such information and expect to exercise some control over the exposure of the shared information. Acquisition of global information allows Facebook apps providers to facilitate network-associated content, which is derived from the opinions and preferences of the users' online social network contacts.

2.1.2. Challenges to information ownership – posting control

In the context of Facebook app usage, individuals' privacy boundaries can also be challenged when users lose control over their personal profiles. This study examines the way posting control can be challenged when Facebook apps make postings on behalf of users. Whereas autonomous posting control represents users' full control over posting on Facebook, impersonated posting control implies that the Facebook apps could act on behalf of the users in disseminating information on Facebook.

Impersonated posting control does not only facilitate the dissemination of Facebook apps usage information, it also allows Facebook apps full control over users' profile. With impersonated posting control, Facebook apps might impersonate users in making status updates, postings, and invitations to use applications. Past information privacy research suggests that individuals manage privacy by establishing interactional boundaries (between oneself and other people) and assume control over these boundaries as part of interaction management. For instance, Hann et al. [18] noted that the management of personal information flow was an important consideration in individuals' evaluation of social exchange. Likewise, Jiang et al. [22] examined synchronous online social interactions and found that individuals managed information flow in social exchange by carefully regulating self-disclosure and misrepresentation.

2.2. General privacy concerns and transactional privacy concerns

The psychology literature has broadly recognized the important distinction between dispositional beliefs and transaction-specific beliefs. For example, Heatherton and Polivy [20] formally proposed the theoretical distinction between dispositional self-esteem and state self-esteem and developed a measurement of state self-esteem. According to the authors, state self-esteem refers to temporarily altered self-esteem, which is highly sensitive to environmental influences, whereas dispositional self-esteem represents a form of individuals' character, which is generally stable and evolves gradually over time. Likewise, McCain et al. [29] investigated transient feelings of self-worth and found that transient self-worth significantly predicted sexual attitudes and

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

behaviours, after controlling the effects of basic personality and traits. Collectively, past psychology research provides substantial evidence for the theoretical distinction between trait beliefs and transient beliefs.

Contrastingly, while making significant progress in understanding information privacy, past IS research has predominately focused on investigating the impact of individuals' general privacy concerns, which refers to individuals' overall concerns about opportunistic behaviour related to the disclosure of personal information in the online environment. For example, Dinev and Hart [15] found that individuals were more willing to self-disclose in online transactions when their general interests in the content surpassed general Internet privacy concerns. Likewise, Son and Kim [42] noted that general privacy concerns might motivate privacy-protective responses, which could manifest in several behaviours, such as negative word-of-mouth, complaints to peers, and report to third parties. In essence, past IS research has vastly broadened understanding of information privacy by deliberating on the impact of general privacy concerns.

Despite the prominent focus on general privacy concerns, emerging evidence suggests that individuals' general privacy concerns might not be entirely sufficient in explaining privacy-related behaviour in a specific transaction. Indeed, several scholars underscore the importance of considering transactional privacy concerns in explaining individuals' privacy trade-off, which is predominantly transaction specific. For example, Ackerman and Mainwaring [1] suggest that individuals develop highly divergent privacy concerns in different privacy situations. The authors point out that while individuals might have extremely high privacy concerns towards healthcare websites, they could be much insensitive towards privacy issues in social networking websites. Similarly, Angst and Agarwal [4] examined adoption of electronic health record and found that individuals' general concerns for information privacy moderated the impact of persuasive messages on attitude towards electronic health records in a specific evaluation episode.

More importantly, recent IS research has started to formally examine transactional privacy concerns. For instance, Xu et al. [49] showed that individuals' general privacy concerns reflect their inherent needs and attitudes towards maintaining privacy, whereas transactional privacy concerns focus on specific assessments of privacy in which their privacy needs are evaluated against information disclosure in a transaction. In essence, general privacy concerns reflect individuals' dispositional privacy beliefs, which are typically stable across various encounters with technologies. Transactional privacy concerns, however, focus on individuals' privacy evaluation in a specific online exchange which involves personal information. Hence, transactional privacy concerns are typically context-specific and formulated in accordance to each unique technology encounter.

Following the spirit of past research examining transactional privacy concerns, this study considers transactional privacy concerns specific to a situation where individuals evaluate their privacy prior to committing their personal information to complete the transaction. Consistent with Xu et al. [49], we posit that transactional privacy concerns are based on specifics of by whom, why, when, and what type of personal information is being collected, distributed, and used. In the context of Facebook apps evaluation, users typically develop transactional attitude based on the specific application information available. In particular, users are likely to focus on the credibility of the app provider, the reasons for information collection (e.g., to enable customization of content), the specific transaction in which information collection occurs (e.g., upon installation), and the type of profile information to be collected (e.g., basic profile information). Accordingly, we define transactional privacy concerns as users' concerns about possible loss of privacy as a result of delegating personal profile to complete a specific Facebook app installation. It is important to note that whereas general privacy concerns focus on individuals' trait privacy concerns, transactional privacy concerns represent individuals' transient privacy concerns, which is highly sensitive to the specific information-related requirement in each Facebook app evaluation episode. To illustrate, when a user evaluates an instant messaging app that requires basic profile information collection (e.g., profile name, date of birth), he or she might develop a moderate level of transactional privacy concerns specific to the app evaluation transaction. On the contrary, when another instant messaging app requires not just basic profile information but collects additional information (e.g., list of friends, friends' profile pictures), the user is likely to develop stronger transactional privacy concerns.

3. Research model and hypotheses development

The overarching theory that guides the development of the research model is the CPM theory [32], which was derived from past works examining the dyadic boundary model of information provision (e.g., Refs. [2,12]). This theory was proposed to explain Facebook apps users' decision making towards information disclosure in social exchange. In particular, CPM theory posits that individuals erect privacy boundaries to protect their privacy and these boundaries can be threatened when their information ownership is challenged. Accordingly, this study examines two application-specific privacy attributes that challenge information ownership in using Facebook apps, namely information collection and profile control. Whereas information collection focuses on the scope of profile information acquisition prior to app adoption, profile control subsumes the management of information exposure after app adoption.

Furthermore, CPM theory presumes challenges to information ownership are the key considerations in individuals' privacy evaluation. More important the theory suggests that individuals construct their privacy evaluation based on some privacy rules, which are established based on their general privacy beliefs. Therefore, this study pays special attention on the interplay between general privacy beliefs and privacy evaluation specific to a transaction. Specifically, in terms of general privacy beliefs, we focus on general privacy concerns, which underscore users' dispositional belief associated with privacy challenges in the online environment. Corresponding to the importance of transaction-specific privacy evaluation, this study centres on transactional privacy concerns. Furthermore, consistent with past information privacy research, we posit that transactional privacy concerns determine users' willingness to delegate profile to Facebook app.

On the basis of CPM theory and the information privacy literature, the research model is represented in Fig. 1.

3.1. Information collection

Information collection is known to exacerbate individuals' concerns about privacy in social transactions [15]. Specifically, when information collection only concerns individuals' personal information, information collection would threaten only their personal privacy and hence constitute a threat to their personal boundary ownership in a particular transaction [33]. On the contrary, when information collection concerns not only personal information but also the information of others, information collection would threaten the privacy of a collective and hence constitute a threat to the collective boundary ownership in a transaction.

In the context of Facebook apps usage, the scope of information collection might range from a local scope to a global scope. In the

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

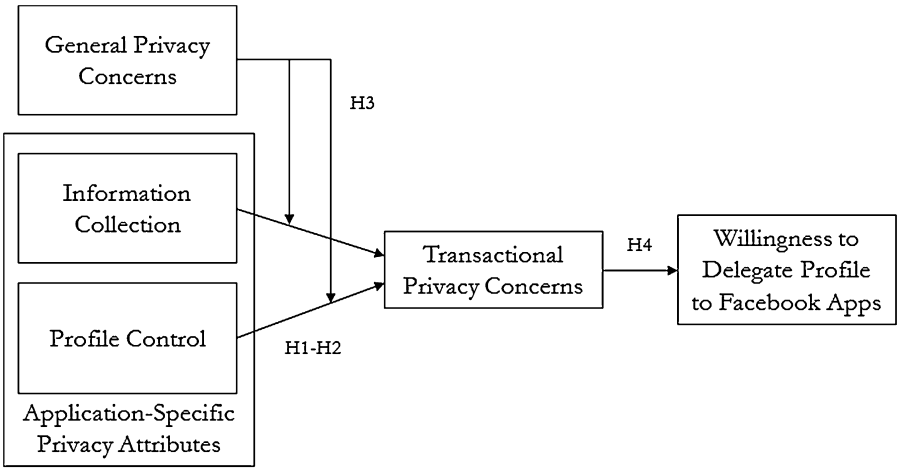

Fig. 1. Research model.

case of a local information collection scope, individual users' profile information is acquired by Facebook apps. As a result, the decision 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 transaction, 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' transactional privacy concerns. Thus, we posit:

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

3.2. Profile control

Past IS research has identified exposure control as the main consideration in individuals' evaluation of technology. For example, Son and Kim [42] revealed that online consumers typically reduced disclosure of personal information to protect privacy. Likewise, Hui et al. [21] reported that individuals did not only exercise exposure control by limiting disclosure but also reveal falsified information to protect their privacy in an information transaction. Similarly, in Facebook app usage, when users retain control over posting, they might be less concerned about privacy invasions and become more appreciative to the value derived from the installation transaction. In contrast, when they are not given such options (i.e., applications make posting on their behalf), the exposure becomes compulsory and hence they could become more apprehensive about their privacy in the installation transaction.

Furthermore, the information privacy literature suggests that the ability to exercise control over posting can enhance individuals' benefit analysis. Control is about individuals' ability to manage subsequent usage of their personal information [28]. While earlier privacy studies hint at the importance of control through their emphasis on confidentiality and secondary usage, recent studies have singled out control as one of the essential factors. Evidence suggests that issues with access and usage are more appropriately managed through "control over who has access to personal data, how personal data are used" ([36], p. 29). In the online environment, individuals could be bestowed with information control functionally and environmentally. Functional control is related to the enforcement of integrity for personal information [31]. With accurate information, individuals can ensure that proper impression is formed about them. Environmental control is about the ability to regulate unintentional self-exposure [30]. The loss of environmental control causes individuals to feel vulnerable and become uncomfortable in transactions [17].

In the context of Facebook apps usage, by allowing users to have autonomous control over posting made by applications, they could better regulate disclosure about themselves and hence ensure the posting is consistent with their desired social images in online transactions. In contrast, with impersonated profile control, users do not only surrender functional control but also lose their environmental control in regulating information exposure in online social networks. Thus, we hypothesize:

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

3.3. General privacy concerns

This study pays special focus on the moderating effect of general privacy concerns on the relationship between application-specific privacy attributes and transactional privacy concerns. The Elaboration Likelihood Model (ELM) provides the theoretical basis for the moderating role of general privacy concerns in this study [34,35]. According to ELM, when individuals are presented with privacy information (i.e., information collection and profile control), individuals will vary in how much cognitive energy they devote to elaborate the information in accordance to their involvement. In the context of privacy evaluation, individuals are typically more involved when they have high dispositional privacy concerns. Therefore, individuals with high dispositional privacy concerns are more likely to read, cognitively process, and carefully consider the privacy information. In contrast, when individuals are less concerned about privacy in general, they will be less involved in the evaluation. Consequently, the privacy information could be ignored altogether. In essence, compared to individuals with low general privacy concerns, the effects of the privacy information on transactional privacy concerns are stronger for individuals with high general privacy concerns.

Past literature substantiates the existence of such moderated relationships [46]. Ample evidence suggests that individuals with higher general concerns are particularly sensitive to privacy-intrusive stimulus and environments [7,10,25]. Scholars suggest

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

that individuals with high general privacy concerns are especially susceptible to losses or risks incurred in online information transactions. For example, Angst and Agarwal [4] examined electronic health record adoption and found that persuasive messages shaped individuals' attitudes towards usage. More important, the authors reported that individuals' general privacy concerns had a differential effect on the motivating influence of persuasive message on attitudes towards using electronic health records. In particular, individuals with strong general privacy concerns were highly sensitive to the persuasive messages whereas those with weak general privacy concerns reported less attitude change caused by the persuasive messages.

Following past information privacy research, we expect general privacy concerns to moderate the effect of information collection and profile control on transactional privacy concerns. Individuals with high general privacy concerns are typically more sensitive to information collection when privacy is scrutinized. Accordingly, individuals with high general privacy concerns are likely to be more attentive to information collection and profile control when evaluating the Facebook app. Consequently, compared to a local scope of information collection, when the Facebook app requires a global scope of information collection, individuals will be especially concerned about threats to both personal privacy boundary and collective privacy boundary. Likewise, compared to autonomous posting control, when the installation involves impersonated profile control, individuals with high general privacy concerns will become highly anxious about the loss of functional control and environmental control in regulating information exposure. Consequently, they become highly susceptible to the loss of information and profile control when installing the Facebook app.

In contrast, low general privacy concerns imply individuals' indifference towards privacy issues. Past information privacy research has broadly classified individuals with low general privacy concerns as privacy-insensitive users, who largely ignore, if not neglect threats to privacy in online transactions [26]. Extending this logic, individuals with low general privacy concerns are more likely to neglect information collection and profile control when evaluating the Facebook app. As a result, despite the apparent difference in privacy boundary implications, individuals with low general privacy concerns might consider the scopes of information collection irrelevant in the evaluation. Likewise, being largely indifferent towards privacy in general, individuals are less likely motivated to prudently estimate the potential reputational damages caused by different types of profile control. Based on this logic, we posit:

H3a. The relationships between information collection and transactional privacy concerns are moderated by general privacy concerns such that the relationships are stronger for individuals with high general privacy concerns.

H3b. The relationships between profile control and transactional privacy concerns are moderated by general privacy concerns such that the relationships are stronger for individuals with high general privacy concerns.

3.4. Willingness to delegate profile to Facebook apps

This study focuses on the impact of transactional privacy concerns on individuals' willingness to delegate profile to a Facebook app, which refers to the extent to which individuals are 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 control over user 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 [43]. The theory posits that individuals form privacy spaces around themselves and protect the spaces by erecting psychological boundaries. More important, researchers suggest that these boundaries play important roles in individuals' willingness to disclose information in online transactions [33]. Similarly, in the context of Facebook apps evaluation, when transactional 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.

Ample past research has identified the relationships between privacy concerns and intention to disclose personal information to use technologies. For instance, Sheehan and Hoy [38] found that individuals with higher privacy concerns in transactions were more likely to provide incomplete information or turn down the particular transaction. On the contrary, evidence suggests that individuals with lower privacy concerns in transactions had higher tendency to being profiled or identified [9]. Therefore, we test:

H4. Higher transactional privacy concerns lead to lower willingness to delegate profile to Facebook apps.

4. Research methodology

4.1. Experimental design

A scenario-based experiment with 2 (information collection: local scope vs. global scope) × 2 (profile control: autonomous vs. impersonated) factorial design was conducted to test the proposed hypotheses. Information collection was manipulated by the type of profile information collected by the Facebook app. In our manipulation, we used 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 was chosen to represent the global scope of information collection. Profile Control was facilitated by manipulating the extent of subject's control over profile impersonation. Autonomous profile control was facilitated by providing subject control over posting made by the application. In contrast, impersonated profile control was administrated by enforcing posting-on-behalf by the application.

Our experiment involved a stimulation of an application evaluation incident using a hypothetical scenario [11]. Hypothetical scenarios have been used in previous IS and privacy research [3].

4.2. Experimental procedures

A total of 284 subjects completed this study. Subjects were public university students. One week prior to the experiment, subjects were asked to provide information about demographics, Internet experience, Facebook experience, Facebook applications experience, and general privacy concerns.

Subjects were presented with a hypothetical scenario (see Fig. 2) in which they evaluated an imaginary Facebook app. Subjects were told that this application acquires local (or global) profile information and the application would impersonate (would not impersonate) them in making status update. Subjects were told to imagine that the scenario was real and read through it carefully.

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

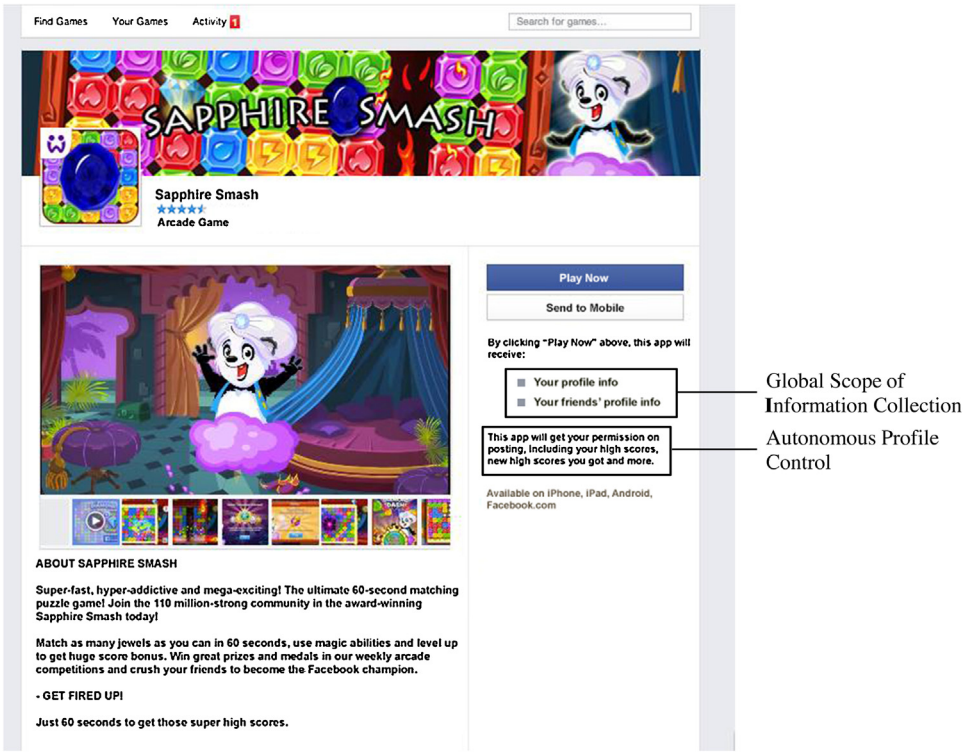

Fig. 2. Hypothetical scenario.

Afterwards, subjects were instructed to complete a questionnaire that contained manipulation checks and measurement items of the research variables. Finally, subjects were debriefed and thanked.

5. Data analysis

5.1. Subject demographics and background analysis

Among the 284 subjects, 135 were females. The age of the subjects ranged from 17 to 25, with average Internet experience and average Facebook experience being 8.7 years and 3.8 years, respectively. The average Facebook applications experience was 2.52 years. On average, a subject spent 32.58 min to complete the entire experiment.

No statistical significant difference was found among subjects randomly assigned to each of the four experimental conditions with respect to age, gender, Internet experience, Facebook experience, and Facebook applications experience, indicating that subjects' demographics were quite homogeneous across different conditions.

5.2. Measurements

The manipulation check for information collection was performed by asking subjects 3 true/false questions on whether their friends' profile information would be collected by the Facebook app. All subjects in the local scope information acquisition answered "false" to the three questions and all those in the global scope information acquisition answered "true", hence suggesting that the manipulation for information collection was successful.

Manipulation check for profile control was performed by asking subjects 3 true/false questions on whether the Facebook app would impersonate them in making status updates via their profiles. All subjects in the autonomous profile control condition answered "false" to the three questions and all those in the impersonated profile control condition answered "true", hence suggesting that the manipulation for profile control worked as anticipated.

General privacy concerns was captured using measurement items adapted from Dinev and Hart [14]. Following Xu [49], we adapted the scale of CFIP development by Smith et al. [40] to measure transactional privacy concerns. Willingness to delegate profile to Facebook apps was assessed based on the measurement items adapted from Dinev and Hart [14]. The measurement items are shown in Table 1.

5.3. Results on transactional privacy concerns

ANOVA with transactional privacy concerns as dependent variable reveals the significant effects of information collection (F (1, 284) = 48.29, $p < 0.01$), profile control (F (1, 284) = 195.23, $p < 0.01$), and general privacy concerns (F (1, 284) = 165.23, $p < 0.01$) (see Table 2). The significant interaction effects suggest that the effect of information collection on transactional privacy concerns is moderated by general privacy concerns (F (1, 284) = 10.55, $p < 0.01$) and the effect of profile control on transactional privacy concerns is moderated by general privacy concerns (F (1, 284) = 16.87, $p < 0.01$).

Simple main effect analysis reveals that (1) a global scope of information collection is associated with significantly higher transactional privacy concerns than a local scope of information collection when general privacy concerns are high (F (1, 139) = 60.47, $p < 0.01$), and (2) a global scope of information collection and a local scope of information collection are not different from each other in affecting transactional privacy concerns when general privacy concerns are low (F (1, 143) = 1.94, $p = 0.17$) (see Table 2). Therefore, H1 and H3a are supported.

Additionally, simple main effect analysis reveals that (1) impersonated profile control is associated with significantly higher transactional privacy concerns than autonomous profile control when general privacy concerns are high (F (1, 139) = 36.41, $p < 0.01$), and (2) impersonated profile control and autonomous

Table 1
Measurement items.

Information collection (True/False)	
IC1	The Facebook app requires me to surrender not just my personal profile information but my Facebook friends' profile information.
IC2	The Facebook app collects both my personal profile information as well as my Facebook friends' profile information.
IC3	Both my personal profile information and my Facebook friends' profile information will be acquired by the Facebook app.
Profile control (True/False)	
PC1	The Facebook app will make status update on my behalf.
PC2	The Facebook app will be able to make posting using my Facebook account.
PC3	The status update made by the Facebook app will look like those that I have made myself.
General privacy concerns	
GPC1	In general, I am concerned that the information I submit on the Internet could be misused.
GPC2	In general, I am concerned that a person can find private information about me on the Internet.
GPC3	In general, I am concerned about submitting information on the Internet, because of what others might do with it.
GPC4	In general, I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.
Transactional privacy concerns	
TPC1	It bothers me to give profile information to the Facebook app.
TPC2	I am concerned that the Facebook app is collecting too much profile information.
TPC3	I am concerned that the Facebook app provider may not take measures to prevent unauthorized access to the collected profile information.
TPC4	I am concerned that the Facebook app provider may not devote enough time and effort to preventing unauthorized access to the collected profile information.
TPC5	I am concerned that the Facebook app provider may not well establish the procedures to correct errors in the collected profile information.
TPC6	I am concerned that the Facebook app provider may not devote time and effort to verify the accuracy of the collected profile information.
TPC7	I am concerned that the Facebook app provider may use the collected profile information for other purposes without notifying me or getting my authorization.
TPC8	I am concerned that the Facebook app provider may sell the collected profile information to other companies.
Willingness to delegate profile to Facebook apps	
WDP1	I am interested to have my Facebook profile delegated to the Facebook app.
WDP2	It is likely that I would allow the Facebook app to take over my Facebook profile.

Note: Unless otherwise indicated, the anchors for all items are 1 = strongly disagree to 7 = strongly agree.

profile control are not different from each other in affecting transactional privacy concerns when general privacy concerns are low ($F(1, 143) = 0.55$, $p = 0.29$) (see Table 2). Therefore, H2 and H3b are supported.

5.4. Results on willingness to delegate profile to Facebook apps

The Partial Least Squares (PLS) regression was used to test the right-hand side of Fig. 1. The measurement model was assessed by examining: (1) individual item reliability, (2) internal consistency, and (3) discriminant validity [6].

Measurement items factor loadings are presented in Table 3. As all items loadings are above 0.7, the requirement for individual item reliability is met [6]. Furthermore, the composite reliabilities of the different measures range from 0.75 to 0.85 and Cronbach's Alpha ranges from 0.76 to 0.85 (as shown in Table 4), all indicating high internal consistency.

Off-diagonal elements in Table 4 represent correlations of all latent variables, while the diagonal elements are the square roots of the Average Variances Extracted (AVE) of the latent variables. As an indicator of adequate discriminant validity, the square roots of Average Variance Extracted (AVE) of any latent variable should be greater than the correlations shared between the latent variable and other latent variables [6]. Our results satisfied this requirement. Another criterion of discriminant validity is that the loadings of indicators on their respective latent variables should be higher than loadings of other indicators on these latent variables and the loadings of these indicators on other latent variables. As presented in Table 3, the loading and cross-loading scores also suggested good discriminant validity.

To examine path significance on the structural model, bootstrap resampling was performed. Results shown in Fig. 3 indicate that transactional privacy concerns has a significant and negative effect on willingness to delegate profile to Facebook app ($p < 0.05$), and hence H4 is supported.

Table 2
ANOVA and analysis of simple main effects.

Source	Type III sum of squares	Df	Mean square	*F*	Sig.
Overall sample					
IC	21.66	1	21.46	48.29	0.000
PC	70.18	1	84.22	195.23	0.000
GPC	71.51	1	60.11	165.23	0.000
IC*GPC	6.75	1	4.26	10.55	0.003
PC*GPC	7.85	1	8.87	16.87	0.000
Error	126.15	276	0.46		
Total	5098.22	284			
GPC = low					
IC	2.48	1	2.48	1.94	0.165
Error	169.46	142	1.84		
Total	171.94	143			
PC	1.67	1	1.67	0.55	0.287
Error	115.48	142	0.80		
Total	117.15	143			
GPC = high					
IC	22.38	1	22.38	60.47	0.000
Error	38.57	138	0.28		
Total	60.95	139			
PC	19.93	1	19.93	36.41	0.000
Error	58.66	138	0.38		
Total	78.59	139			

Notes: Dependent variable: transactional privacy concerns.
IC = information collection; PC = profile control; GPC = general privacy concerns.
R squared = 0.45 (adjusted *R* squared = 0.41).

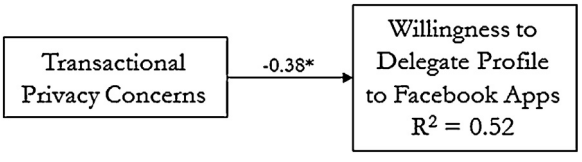

Fig. 3. Path significance.

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

Table 3
Item loadings and cross-loadings.

	GPC	TPC	WDP
GPC1	0.84	0.43	-0.28
GPC2	0.82	0.38	-0.26
GPC3	0.88	0.41	-0.26
GPC4	0.87	0.35	-0.23
TPC1	0.44	0.76	-0.27
TPC2	0.47	0.76	-0.32
TPC3	0.42	0.78	-0.29
TPC4	0.33	0.76	-0.42
TPC5	0.47	0.75	-0.44
TPC6	0.44	0.77	-0.41
TPC7	0.43	0.76	-0.28
TPC8	0.41	0.80	-0.37
WDP1	-0.29	-0.39	0.89
WDP2	-0.33	-0.37	0.92

Notes: GPC: general privacy concerns; TPC = transactional privacy concerns; WDP = willingness to delegate profile to Facebook apps. The gray shaded values are all significant at 0.05 level.

Table 4
Construction correlation matrix.

	M	SD	CR	CA	GPC	TPC	WDP
GPC	4.76	1.15	0.83	0.85	0.86		
TPC	4.97	1.36	0.75	0.76	0.40	0.81	
WDP	4.54	1.45	0.85	0.84	−0.25	−0.33	0.90

Notes: M = mean; SD = standard deviation; CR = composite reliability; CA = Cronbach's alpha.

6. Discussion and concluding remarks

6.1. Discussion of results

The results are in support of our hypotheses. We seek to explain the different roles of general privacy concerns and transactional privacy concerns in affecting individuals' willingness to delegate profile to Facebook app. We establish that information collection and profile control powerfully influence users' transactional privacy concerns, which in turn, influence their willingness to delegate profile. More important, we enhance the information privacy literature by clarifying the distinct role of general privacy concerns. Our findings reveal that general privacy concerns alter the impact of application-specific privacy attributes on transactional privacy concerns.

6.2. Theoretical contributions

6.2.1. Profile delegation in using Facebook apps

This study provides an in-depth understanding of profile delegation by taking on a privacy perspective which is drawn from the information privacy literature. In particular, it presents the importance of transactional privacy concerns in influencing individuals' willingness to delegate personal profile to Facebook apps. The findings of this study in general reveal that transactional privacy concerns play an important role in affecting individuals' decision to expose profile information. Our results show that a global scope of information collection induces higher transactional privacy concerns compared to a local scope of information collection. Furthermore, we show that impersonated profile control leads to an elevated level of transactional privacy concerns compared to autonomous profile control. Overall, we expect that the finding will serve as a useful insight for further examination of Facebook apps usage behaviour.

6.2.2. Interplay between general privacy concerns and transactional privacy concerns

To the best of our knowledge, this is one of the first studies to formally examine the interplay between general privacy concerns and transactional privacy concerns. Given the transactional nature of privacy trade-off, it is surprising that past research has paid little attention beyond general privacy concerns. Drawing on Xu et al. [49] and Li et al. [27], we proposed that transactional privacy concerns and general privacy concerns are independent concepts. Our findings show that transactional privacy concerns are indeed distinct from general privacy concerns. More important, our results reveal that the impact of information collection and profile control on transactional privacy concerns is moderated by general privacy concerns. We believe that our approach to the two concepts of privacy concerns is effective not only in examining Facebook apps usage but also in understanding individuals' psychological trade-off when their privacy is concerned.

6.2.3. Determinants of transactional privacy concerns

Emerging evidence has shown the importance of privacy boundary management in conceptualizing privacy concerns and understanding privacy-related behaviours. Yet most of these studies have focused on investigating the general impact of privacy concerns on self-disclosure behaviours. While exceptional studies have recently attempted to identify factors pertinent to privacy concerns in the online environment (e.g., Ref. [22]), rarely has research focused on identifying the privacy-related technical attributes in social media. Our study is meaningful in that it examines two key technical attributes of Facebook apps that challenge privacy boundaries. Specifically, this study demonstrates that information collection is an important technical attribute that challenges individuals' information ownership in using Facebook apps. Furthermore, posting control is another key technical attribute that challenges individuals' information ownership.

6.3. Practical contributions

Our findings provide fresh insight to Facebook app developers and social media service providers on how two key application-specific privacy attributes – information collection and profile control – impact individuals' formulation of transactional privacy concerns. Our findings alert Facebook app developers that the scope of information collection and types of profile control should be strategically considered in marketing Facebook apps. While a global scope of information collection could be important in constructing personalized services and recommendations, a local scope of information collection might be more tolerable to typical users. Likewise, although impersonated profile control might allow convenience in making status updates as well as providing a creditable source of self-presentation, individuals might still prefer autonomous posting control. To this end, developers are urged to be transparent in explaining the rationale of information collection

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

and profile control. More important, to mitigate users' privacy concerns, developers might consider providing options which would allow users to adjust the scope of information collection and types of profile control.

6.4. Limitations and future research

We acknowledge some limitations in this study. This study examines usage of Facebook apps. We do not attempt to generalize the results to applications in other online social networks.

It is possible that our findings are specific to the student samples and not necessarily generalized to other populations. For instance, our respondents might feel that they had little to "lose" financially and socially in terms of their profile information as well as friends' profile information, and thus displayed more willingness to use Facebook apps. Despite this concern, university students are generally reported to represent a huge portion of the actual population engaging actively in online social network related usage. Moreover, university students are found to be vulnerable to privacy issues and become targets for physical and psychological threats [50].

Our findings may also be limited through the use of a Facebook app evaluation scenario. While the mock-up application presented in the scenario resembled those of a real Facebook app, the application may not completely reflect the actual environment. However, in the actual social networking environment (i.e., Facebook App Center), it would be impossible to manipulate the experimental conditions. Therefore, despite the limitation, the employment of scenarios is necessary. We encourage researchers to verify the impact of information collection and profile control on Facebook apps in a more natural setting.

7. Conclusion

Privacy issues associated with Facebook apps usage are becoming increasingly prevalent. This study is one of the first attempts to develop a holistic understanding on these privacy issues by extending communication privacy management theory to the context of Facebook apps usage. Our results reveal that information collection, profile control and general privacy concerns interact to affect users' transactional privacy concerns, which in turn, influence their willingness to delegate profile to Facebook apps.

Acknowledgements

The authors wish to acknowledge the assistance and cooperation of participants from the organizations sponsoring this Identity Fraud Linkage Research Project and to Attorney-General's Department and the Australian Research Council for their research grant. The authors also thank the UNSW Business School [Grant: FBS201, OP001 and PS37805] for its financial support.

References

[1] M.S. Ackerman, S.D. Mainwaring, Privacy issues and human–computer interaction, Computer 27 (5), 2005, pp. 19–26.
[2] I. Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding, Brooks/Cole Publishing Company, Monterey, CA, 1975.
[3] C.L. Anderson, R. Agarwal, The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information, Inf. Syst. Res. 22 (3), 2011, pp. 469–490.
[4] C.M. Angst, R. Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, Manage. Inf. Syst. Q. 33 (2), 2009, pp. 339–370.
[5] N.F. Awad, M.S. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS Q. 30 (1), 2006, pp. 13–28.
[6] D. Barclay, C. Higgins, R. Thompson, The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration, Technol. Stud. 2 (2), 1995, pp. 285–309.
[7] J.N. Bassili, Meta-judgmental versus operative indexes of psychological attributes: the case of measures of attitude strength, J. Pers. Soc. Psychol. 71 (4), 1996, p. 637.
[8] F. Bélanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, MIS Q. 35 (4), 2011, pp. 1017–1042.
[9] B. Berendt, O. Günther, S. Spiekermann, Privacy in e-commerce: stated preferences vs. actual behavior, Commun. ACM 48 (4), 2005, pp. 101–106.
[10] J.E. Boritz, W.G. No, Internet privacy research: framework, review and opportunities, Rev. Oppor. (June), 2006.
[11] D.J. Brass, M.E. Burkhardt, Potential power and power use: an investigation of structure and behavior, Acad. Manage. J. 36 (3), 1993, pp. 441–470.
[12] V.L. Derlega, A.L. Chaikin, Privacy and self-disclosure in social relationships, J. Soc. Issues 33 (3), 1977, pp. 102–115.
[13] J.M. DiMiCCo, D.R. Millen, Identity management: multiple presentations of self in Facebook, GROUP '07 Proceedings of the 2007 international ACM conference on Supporting Group Work, 2007, pp. 383–386.
[14] T. Dinev, P. Hart, Internet Privacy Concerns and Trade-Off Factors: Empirical Study and Business Implications, Florida Atlantic University, 2002.
[15] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inf. Syst. Res. 1 (17), 2006, p. 2006.
[16] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti, Privacy calculus model in e-commerce – a study of Italy and the United States, Eur. J. Inf. Syst. 15 (4), 2006, pp. 389–402.
[17] E. Goffman, The Presentation of Self in Everyday Life, Doubleday Anchor Books, Garden City, NY, 1959.
[18] I. Hann, K. Hui, T.S. Lee, I.P.L. Png, Analyzing Online Information Privacy Concerns: An information Processing Theory Approach, 2005.
[19] J. Hart, C. Ridley, F. Taher, C. Sas, A. Dix, Exploring the Facebook experience: a new approach to usability, in: Proceedings of the 5th Nordic Conference on Human–Computer Interaction: Building Bridges, 2008, pp. 471–474.
[20] T.F. Heatherton, J. Polivy, Development and validation of a scale for measuring state self-esteem, J. Pers. Soc. Psychol. 60 (6), 1991, pp. 895–910.
[21] K.L. Hui, H.H. Teo, T. L.S.Y, The value of privacy assurance: an exploratory field experiment, MIS Q. 31 (1), 2007, pp. 19–33.
[22] Z. Jiang, C.S. Heng, B.C.F. Choi, Privacy concerns and privacy-protective behavior in synchronous online social interactions, Inf. Syst. Res. 24 (3), 2013, pp. 579–595.
[23] I.A. Junglas, N.A. Johnson, C. Spitzmüller, Personality traits and concern for privacy: an empirical study in the context of location-based services, Eur. J. Inf. Syst. 17 (4), 2008, pp. 387–402.
[24] S.Y.X. Komiak, I. Benbasat, The effects of personalization and familiarity on trust and adoption of recommendation agents, MIS Q. 30 (4), 2006, pp. 941–960.
[25] R.R. Lau, R.A. Smith, S.T. Fiske, Political beliefs, policy interpretations, and political persuasion, J. Polit. 53 (03), 1991, pp. 646–675.
[26] D.-J. Lee, J.-H. Ahn, Y. Bang, Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection, MIS Q. 35 (2), 2011, pp. 423–444.
[27] H. Li, R. Sarathy, H. Xu, The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors, Decis. Support Syst. 51 (3), 2011, pp. 434–445.
[28] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model, Inf. Syst. Res. 15 (4), 2004, pp. 336–355.
[29] J.L. McCain, P.K. Jonason, J.D. Foster, W.K. Campbell, The bifactor structure and the "dark nomological network" of the state self-esteem scale, Pers. Indiv. Differ. 72, 2015, pp. 1–6.
[30] N. Olivero, P. Lunt, Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control, J. Econ. Psychol. 25 (2), 2004, pp. 243–262.
[31] P.A. Pavlou, H. Liang, Y. Xue, Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective, MIS Q. 31 (1), 2007, pp. 105–136.
[32] S. Petronio, Boundary management: a theoretical model of managing disclosure of private information between marital couples, Commun. Theory 1 (4), 1991, pp. 311–335.
[33] S. Petronio, Boundaries of Privacy: Dialectics of Disclosure, State University of New York Press, Albany, NY, 2002.
[34] R.E. Petty, J.T. Cacioppo, Attitudes and Persuasion: Classic and Contemporary Approaches, Wm.C. Brown, Dubuque, IA, 1981.
[35] R.E. Petty, J.T. Cacioppo, Communication and Persuasion: Central and Peripheral Routes to Attitude Change, Springer-Verlag, New York, 1986.
[36] J. Phelps, G. Nowak, E. Ferrell, Privacy concerns and consumers willingness to provide personal information, J. Public Policy Mark. 19 (1), 2000.
[37] J. Rosenberg, N. Egbert, Online impression management: personality traits and concerns for secondary goals as predictors of self-presentation tactics on Facebook, J. Comput.-Mediat. Commun. 17 (1), 2011, pp. 1–18.
[38] K.B. Sheehan, M.G. Hoy, Dimensions of privacy concern among online consumers, J. Public Policy Mark. 19 (1), 2000.
[39] X. Shen, B. Tan, C. Zhai, Implicit user modeling for personalized search, in: Proceedings of the 14th ACM International Conference on Information and Knowledge Management, 2005, pp. 824–831.
[40] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. 20 (2), 1996, pp. 167–196.
[41] H.J. Smith, T. Dinev, H. Xu, Information privacy research: an interdisciplinary review, MIS Q. 35 (4), 2011, pp. 989–1016.

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003

[42] J.-Y. Son, S.S. Kim, Internet users' information privacy-protective responses: a taxonomy and a nomological model, MIS Q. 32 (3), 2008, pp. 503–529.
[43] J.M. Stanton, K.R. Stam, Information technology, privacy, and power within organizations: a view from boundary theory and social exchange perspectives, Surveill. Soc. 1 (2), 2003, pp. 152–190.
[44] K.A. Stewart, A.H. Segars, An empirical examination of the concern for information privacy instrument, Inf. Syst. Res. 13 (1), 2002, pp. 36–49.
[45] J. Sutanto, E. Palme, C.-H. Tan, C.W. Phang, Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users, MIS Q. 37 (4), 2013, pp. 1141–1164.
[46] C. Van Slyke, J. Shim, R. Johnson, J.J. Jiang, Concern for information privacy and online consumer purchasing, J. Assoc. Inf. Syst. 7 (1), 2006, p. 16.
[47] S.S. Wang, M.A. Stefanone, Showing off? Human mobility and the interplay of traits, self-disclosure, and Facebook check-ins Soc. Sci. Comput. Rev. 31 (4), 2013, pp. 437–457.
[48] N. Wang, H. Xu, J. Grossklags, Third-party apps on Facebook: privacy and the illusion of control, CHIMIT '11 Proceedings of the 5th ACM Symposium on Computer–Human Interaction for Management of Information Technology, 2011.
[49] H. Xu, H.-H. Teo, N. Tanzer, R. Agarwal, Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Inf. Syst. Res. 23 (4), 2012, pp. 1342–1363.
[50] A.T. Zhang, L.P.W. Land, G. Dick, Key influences of cyberbullying for university students, PACIS, 2010, p. 83.
[51] D. Zohar, O. Tenne-Gazit, Transformational leadership and group interaction as climate antecedents: a social network analysis, J. Appl. Psychol. 93 (4), 2008, pp. 744–757.

Ben C.F. Choi is a lecturer in Information Systems at the UNSW Australia Business School, University of New South Wales, Australia. He has a Ph.D. and B.S. in Information Systems (National University of Singapore). His research interests focus on information privacy, social media, and mobile applications. He has published multiple papers in premier information systems journals including, Information Systems Research and Journal of Management Information Systems. He has served as Associate Editor for major information systems conferences.

Lesley Land is a senior lecturer in the Information Systems at the UNSW Australia Business School, University of New South Wales, Australia. She has a B.Sc. from the University College London, an M.Sc. from Brunel University, and a Ph.D. from UNSW. Her research interests include understanding the impact of IT (such as social media and organizational systems) – their benefits and/or abuse, and IT implementation issues (including project management).

Please cite this article in press as: B.C.F. Choi, L. Land, The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.02.003