An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective

Mehrdad Koohikamali[a], Aaron M. French[b], Dan J. Kim[c],*

[a] Computer Information Systems, College of Business Adminstration, California State Polytechnic University, Pomona, United States of America
[b] Information Systems, Anderson School of Management, University of New Mexico, United States of America
[c] Information Technology & Decision Sciences, G. Brint Ryan College of Business, University of North Texas, 1155 Union Circle #305249, Denton, TX 76203-5249, United States of America

ARTICLE INFO

ABSTRACT

This study examines the dynamic relationship between perceived privacy concerns and use behaviors of a new social networking application (SNA) over time. By integrating the theory of belief updating and an extended privacy trade-off model from a longitudinal perspective as the basis for theoretical underpinning, this study proposes a privacy trade-off model showing the role of initial use and initial self-disclosure on updating users' pre-perceptions of using a new SNA to initial perceptions of using it. The trade-off between pre-privacy concern and pre-perceived benefit determines the initial SNA usage and self-disclosure behaviors. Then, initial privacy trade-off determines the continued use behavior and continued self-disclosure. Using an empirical data collected three phases from actual mobile app users, this study validates the proposed model and hypotheses. Including the proposed dynamic model of privacy trade-off, this study provides important contributions to theory and practice in the privacy literature.

1. Introduction

Mobile computing devices such as smartphones and tablets are the leading personal computing technologies dominating the digital landscape with roughly 77% of Americans owning smartphones [1]. The evolution of smartphones has transformed cell phones from simple communication tools to sophisticated multi-tasking platforms. Especially now, with the variety of mobile applications (apps), mobile devices are considered to be the *Swiss army knives* of technology [2]. One prominent feature of mobile apps involves social networking services, reported to reach an estimated 2.95 billion users by 2022, encompassing approximately one-third of the global population [3].

In contrast to mobile web sites' access via web browsers, mobile apps can access device functionality and personal data. The continuous use of mobile apps increases privacy concerns because of the access of personal information, including address books, calendars, photos, and even location information via GPS data [4].[1] With persistent access to mobile apps, privacy concerns become a critical factor with the continued use decisions of these apps [5,6]. While users may have initial privacy concerns, those privacy concerns may change with different

experience of smartphone technology [7]. In other words, users' privacy concerns are not static and are subject to change based on different factors such as experience, understanding of context, and policy modifications in legislation [8].

In the context of social networking mobile apps (SNAs), users experience social interactions as a result of a mental trade-off between their concerns for privacy and rewards (benefits), or simply, the privacy trade-off [6]. Most prior studies examine privacy concerns as a static factor that influences usage intention or disclosure behavior [5,9,10]. In this study, we explore a dynamic view of privacy trade-off by addressing the following research questions: (1) *What are the relationships among privacy concern, perceived benefit, and self-disclosure in a new SNA? (2) How does the privacy trade-off change over time in SNAs due to update of privacy concern and perceived benefit beliefs?*

By integrating the privacy trade-off model [6] and the theory of belief updating process [11,12], this study aims 1) to propose a dynamic privacy trade-off model which explains the change in privacy concern and perceived benefit across three phases (i.e., pre-, initial, and after-use phases), 2) to empirically test the proposed model using the data collected from users of a new mobile app at three phases (i.e., pre-,

---

initial, and after-use phases), and 3) to provide theoretical contributions to literature and practical insights to mobile app communities. The results of the study offer new insights to the decision-making process as it relates to social networking usage in the context of mobile apps and change in users' perceptions after gaining some experience on a new SNA.

The remainder of this paper is organized as follows. First, we review literature related to the theories of privacy trade-off, self-disclosure behavior, and the belief updating process in social networking context. Then, we propose a research model integrating privacy trade-off and theory of belief updating. Following the proposed research model and hypotheses, we present the details of the methodology, including data collection and analysis. After presenting the analysis results, we conclude the paper with a discussion of the findings and the implications of research and practice, along with limitations and future directions.

2. Literature review and background theories

2.1. Longitudinal studies in IT and social networking apps

In the IS field, various research evaluate the adoption of new IT with longitudinal perspectives. The success of an information system depends on its adoption, growth, and continued use over time, which can be measured at the pre-adoption, post-adoption, and continued use stages of an information systems life-cycle. Cross-sectional studies are useful for comparing different groups at a single point in time but often fall short in capturing changes in the variables required to produce a desired outcome. The use of longitudinal studies in the evaluation of information systems is crucial for capturing changes in perceptions, behaviors, and attitudes which are necessary in evaluating the success of an information system. By determining the change in characteristics of the same sample group at different points in time, researchers can identify factors that influence the outcome variables. For example, Warkentin et al. [13] evaluates the effects of changes in perceptions over time and their influence on continuance of security-related behaviors. The effects of continued use have also been evaluated to identify ways that habitual use affects perceptions over time [14]. Another study conducted a longitudinal evaluation of the change in privacy concerns at three different points in time mixed with a cross-sectional analysis during the third data collection [15].

With millions of mobile apps available, understanding factors that influence the selection, adoption, and continued use of a specific app becomes increasingly important. The lifecycle of mobile apps revolves around five distinct events that consist of installing, updating, opening, closing, and uninstalling the app [16]. The life cycle begins with installing the app – i.e., the initial adoption stage of a mobile app. After the adoption, mobile users start to use the app – i.e., the initial usage stage. Based on the experience of initial use, they can continually use the app or discontinue using the app, or even uninstalling the app. User satisfaction of the app, and even marketing strategies employed influence the decision of continued usage [17].

Previous research on social networking sites (SNS) identifies prior experience as an important factor in determining user behavior in pre-adoption and post-adoption comparisons [18]. Variations in attitudes toward information systems are attributed to experiential and situational factors during adoption and use [9]. More specifically, privacy concern is a significant determinant of SNS continuance [10]. In the context of mobile apps (e.g., SNAs), short usage life cycles, dynamism of situational factors, and low switching costs result in an increased need to evaluate the change of behavioral factors. While previous research has evaluated pre-adoption and post-adoption across numerous factors, there is still much more to be done. Current research contributes to longitudinal work by evaluating the change in privacy trade-off from a pre-adoption, post-adoption, and continuance longitudinal perspective.

2.2. Privacy trade-off

While previous research has identified privacy concern as an important determinant of SNS use [10], actual behavior to protect one's privacy does not always match his or her desire [19]. In the context of SNS, privacy concern has been viewed as an individual's desire to control their information and interaction with others, which can be overridden when certain perceived benefits such as socialization, self-expression, and pleasing others is present [20]. This trade-off between privacy concern and perceived benefits is likely to influence various states of adoption and use based on the perceptions of the technology being used and the user's experience. The perceptions of risk and reward will continue to shift from individuals' initial perception prior to adopting the app and throughout the life cycle of usage until discontinuance takes place. The current research evaluates privacy trade-off from a pre-adoption to post-adoption perspective by evaluating the changes in privacy concerns and perceived benefits and their longitudinal effects on SNA continuance.

Privacy concern is a multifarious concept with its definition dependent upon the context that frames it, the culture that cultivates it, and the individual who perceives it [6]. There are three major areas that previous privacy literature has contributed most: 1) the conceptualization of information privacy, 2) the relationships between information privacy constructs and other constructs, and 3) the context that information privacy resides in [21]. Personal concepts of privacy are interwoven with values, perceptions, beliefs, and experience [22]. Privacy can have different meanings and connotations across different groups of the same culture, resulting in contrasting expectations among individuals to protect their privacy [23]. Personal information privacy is the optimal level of control over personal information [24] with privacy concerns reflecting the desire for sufficient control and fairness of personal information [24,25]. Concern for information privacy (CFIP) is multidimensional [26], consisting of four dimensions of CFIP that include collection, improper access, errors, and unauthorized use [26]. In the context of SNAs, users' privacy is influenced by their network, the app provider policies, and the users themselves. Following this view, the current study modifies CFIP in the context of SNAs as a reference to privacy concerns for conducting the analysis.

Perceived benefit is a multidimensional construct that consists of a range of benefits depending on the context, expectations, and use of the technology being evaluated. The direct and indirect advantages of adopting information technologies/services comprise of the two main types of perceived benefits identified as utilitarian and hedonic benefits [27]. Utilitarian benefits refer to the functional and practical benefits, whereas hedonic benefits reflect the aesthetic and gratification (enjoyment) benefits [28]. Previous research identifies perceived usefulness as a measure for capturing utilitarian benefit and perceived enjoyment to capture hedonic benefit [29]. In the context of SNAs, users are provided constant connectivity to the network and their SNA contacts anytime and anywhere. The ubiquity and immediacy of these apps provide utilitarian benefits of constant connectivity to others in a timely manner. Hedonic benefits generate a feeling of excitement [30], resulting in increased satisfaction through interaction with others [6] and social rewards facilitating relationship building [31]. Based on previous literature, the hedonic benefits of social rewards and enjoyment [6,32] are integrated into the current research along with the utilitarian benefits of ubiquity and timeliness as part of the privacy trade-off.

2.3. Self-disclosure behavior in social networks

Information sharing in SNSs is a natural phenomenon occurring as a post-adoption behavior [33]. The content that SNS users generate can be classified as personal information (e.g., age, home address, phone number, personal views, and personal images) and other diverse content (e.g., news and entertainment information) [34]. *Self-disclosure* refers to the intentional and voluntary sharing of personal information

[35] such as personal photos, videos, [35,36], home address, phone number, email, [37] or a variety of other information related to the sharer. Previous literature identifies various factors that influence self-disclosure such as perceived benefits, perceived risks, privacy concerns, information control, and sensitivity [38]. SNS research evaluating self-disclosure identifies usage rate as a positive influence on disclosure extent, whereas privacy concern demonstrates a negative effect on self-disclosure [39]. Information dissemination and exposure of personal information is shown to have a strong effect on perceptions of privacy invasion [40]. During the usage of a social network service, users do not always have sufficient control over their information, and privacy concern could increase due to others' sharing behavior or the lack of users' awareness about privacy practices [34]. As a result, studying self-disclosure behavior in social networks should be an integrated approach, considering the privacy trade-off as well as usage experiences.

2.4. Privacy trade-off during usage of social networks

Privacy concern is an elastic construct that varies in response to people's experiences and perceptions [8,21] with the regular impact of new regulations and technology advancements [21,41]. In a given context, prior experience has shown a significant impact on privacy concerns, with negative experiences resulting in heightened awareness of privacy-related issues and increased privacy concern. [42]. Based on these findings from literature, the current research evaluates pre-adoption and post-adoption privacy trade-off dynamics to analyze the experiential effects on user privacy trade-off perceptions in the context of SNA usage. The theory of belief updating (TBU) process is used to explain this adjustment in beliefs (i.e., privacy trade-off) in response to interaction with information (i.e., use of the SNA) [11].

In IS research, TBU is used to explain post-adoption behaviors such as continued use. The adjustment of perceptions based on prior knowledge and new information gathered through experience define the main principles of TBU [11]. The process of adopting and using new technology involves the TBU principles as users form a pre-conception of the technology based on prior knowledge, which is then adjusted based on experience with the new technology. In the context of SNS/SNA, experience is based on three levels of involvement identified as discovery, superficial involvement, and true commitment [43]. In the discovery phase, people become aware of the new SNA and are faced with the adoption decision prior to initial use. The superficial involvement phase is where users decide to try the new SNA and create content for the first time to gain experience with the SNA. In the true commitment phase, users get actively involved in seeking relationships with others and sharing personally created content through the SNA. As a user spends more time using the SNA, his or her perception toward the app (i.e., privacy trade-off) will adjust based on the individual's experience. In this study, the discovery phase is identified as the pre-use phase, superficial involvement relates to initial use phase, and the true commitment is the continued use phase. TBU is used to evaluate the change in privacy trade-off and use behaviors as users progress through

these three phases over time while gaining experience with the new SNA. Table 1 summarizes the definition of each construct across the phases used in this study. Fig. 1 provides the conceptual model used for the current study with all three phases and the time line of the research that was conducted.

It is expected that privacy trade-off will change from phase 1 to phase 2 as users experience using the app initially, and the adjusted perceptions after initial use will influence their continued use behaviors. To conduct the longitudinal study, phase 1 consists of the introduction to the new SNA, followed by an evaluation of the user's initial use experience in phase 2 one week later. Three weeks after capturing initial use perceptions and behaviors, continued use and disclosure behaviors are measured to determine the change in use behaviors based on initial privacy trade-off perceptions.

3. Research model and hypotheses development

The privacy trade-off dynamic is the internal perceptions of the privacy concerns and perceived benefits related to an artifact that influences individual behavior. While privacy trade-off influences behavior [47], privacy concerns also shift as people gain experience with a given technology over time [11]. This study evaluates the relationship between privacy trade-off and usage behaviors from a longitudinal perspective in the context of SNA. Fig. 2 presents the research model evaluating privacy trade-off and continued use behaviors with the proposed hypotheses at all three phases.

The underpinning logic of the proposed model is based on the culmination of privacy trade-off and TBU across the three time-frames (i.e., pre-, initial-, and continued use). Pre-adoption (t0) stage is the discovery phase where people learn about the new SNA and form their pre-adoption privacy trade-off perceptions. At this phase, individuals perceive expected benefits and privacy concerns that influence their decision to adopt the new SNA. Initial-use (t1) stage is the superficial involvement phase, which consists of activities such as downloading and using the app for the first time. After initial experience with the app, an individual's perceptions about perceived benefits and privacy concerns may shift as identified by TBU. The continued use (t2) stage is a commitment phase based on the evaluation of multiple use experiences.

3.1. Relationship between privacy trade-off and social network usage behaviors

Social network usage behavior can be evaluated based on the dichotomy of active usage and passive usage [48]. Active usage pertains to social interaction of users on the network [48] that requires self-disclosure. Passive usage is classified by lurker behaviors that include searching, following, and viewing shared content by others [48] with a lower level of self-disclosed information. Based on this distinction, the current research evaluates use behavior as the actual use of the SNA and the sharing of information referred to as self-disclosure. When

Table 1
Construct definition.

Construct	Definition
Pre-privacy concern [24,26]	The individual's subjective view of control over personal information shared with other people at the pre-use stage of the SNA (t0).
Initial privacy concern [24,26]	The individual's subjective view of control over personal information shared with other people after the initial use stage of the SNA (t1).
Pre-perceived benefits [38,44]	The individual's subjective view of value expected from use of the SNA at the pre-use stage of the SNA (t0).
Initial-perceived benefits [38,44]	The individual's subjective view of value expected from use of the SNA after the initial use stage of the SNA (t1).
Pre-privacy trade-off [6]	The psychological trade-off between privacy concerns and perceived benefits at the pre-use stage of the SNA (t0).
Initial privacy trade-off [6]	The psychological trade-off between privacy concerns and perceived benefits after the initial use stage of the SNA (t1).
Initial use [45]	The total amount of time the user spent using the SNA during the initial use stage after installing the SNA (t1).
Continued use [45]	The total amount of time the user spent using the SNA during the on-going use stage of the SNA (t2).
Initial self-disclosure [35,46]	The voluntary sharing of personal information during the initial use stage after installing the SNA (t1).
Continued self-disclosure	The voluntary sharing of personal information during the on-going use stage of the SNA (t2).

Time: t0 = phase 1: pre-use (Week 1); t1 = phase 2: initial use (Week 2); t2 = phase 3: on-going use (Week 5).
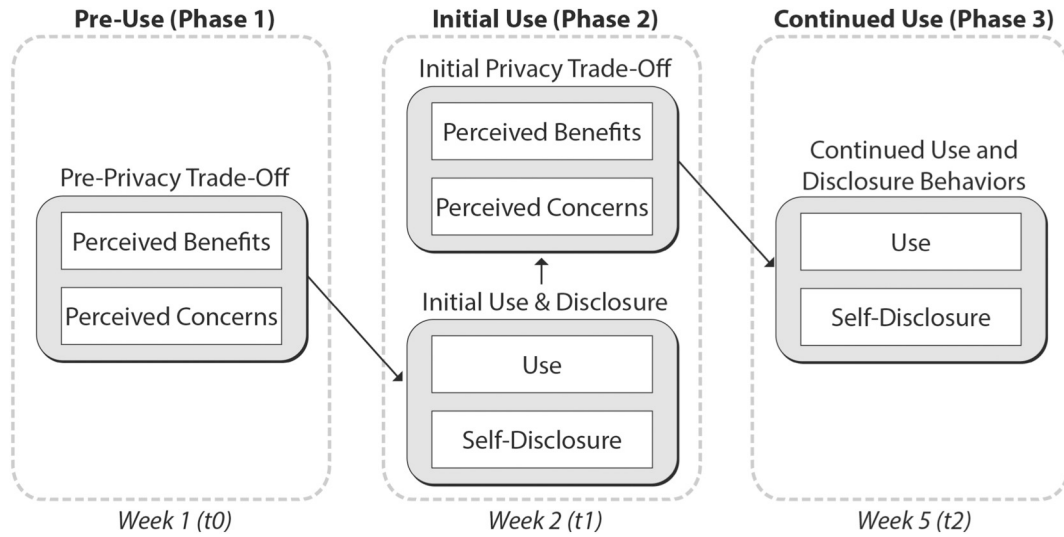
Fig. 1. The conceptual model of dynamic privacy trade-off.

presented with a new technology (e.g., SNA), individuals internalize their perceptions about the technology based on their personal experiences with similar technology to determine their adoption behavior. Upon initial use, pre-perceptions will shift based on their initial experience with the app. The theory of belief updating (TBU) encompasses the dynamics of this change in perceptions in relation to behaviors over time. Integrating TBU with privacy trade-off theory, the current research evaluates the change in privacy perceptions post adoption and their effect on continued use.

Privacy trade-off refers to the mental trade-off between an individual's privacy concerns and perceived benefits gained through social interaction [6]. Perceived benefits relate to an individual's perception of the benefits gained by engaging in a specific action [38,44]. The current research evaluates the actions of initial use and continued use behaviors in the context of SNAs, consisting of actual use and self-disclosure. Prior to adoption, an individual discovers a new technology and forms perceptions about the benefits of adopting and using the technology based on the information available and experience with similar technologies. The pre-perceived benefits refer to the pre-conceived value an individual expects to receive from using a technology (i.e., *Sociabile* mobile app). When presented with a new technology, an individual perceives the expected benefits to determine their adoption and initial use behavior. It has been shown that perceived benefits significantly influence technology adoption [49]. In the context of social networking, perceived benefits may consist of hedonic or utilitarian

values [32] stemming from feelings of enjoyment [50], excitement [51], social reward from interactions with others [6], or various other benefits. Previous research has demonstrated a positive effect of perceived benefits on usage behaviors in the context of social network sites [19]. Based on TBU, perceptions have been shown to shift over time as users gain more experience with a given technology. Therefore, the current research evaluates the post-adoption perceptions of initial perceived benefits referred to as the expected reward an individual expects to receive from continued use of a particular technology after initial use. There is an abundance of research supporting the positive effect of perceived benefit on using an IT [38]. Based on previous literature, it is predicted that the positive relationship between perceived benefit and use behavior will produce similar results in the context of SNAs at the pre-adoption and post-adoption stages of analysis. Considering a longitudinal perspective and consistent with the prior literature, we propose that:

H1a. Pre-perceived benefit is positively related to the initial use a new SNA.

H1b. Initial perceived benefit is positively related to the continued use a new SNA.

Most social networks are based on sharing information where users voluntarily choose to disclose their personal information [52]. Self-disclosure is referred to as the intentional sharing of self-information to
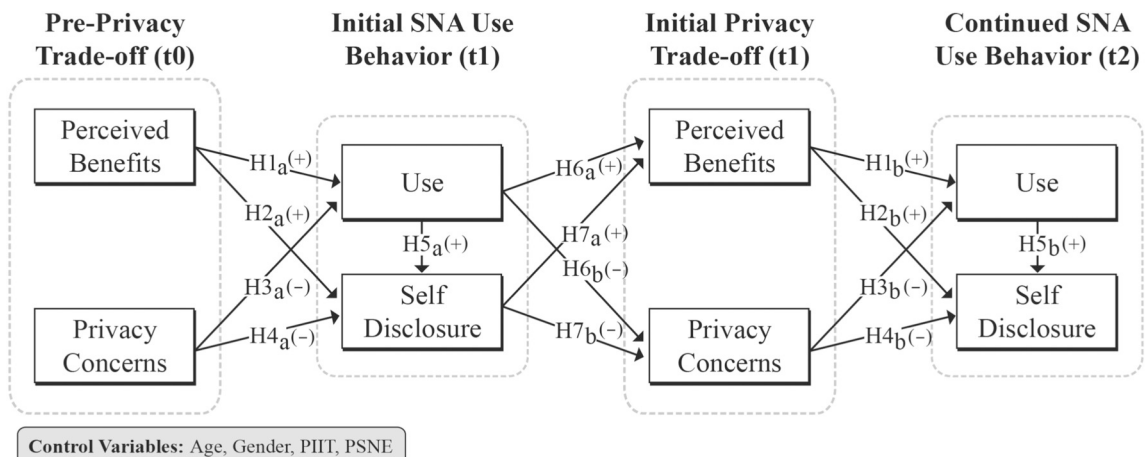

Fig. 2. The proposed research model on privacy trade-off.

others in a social environment [46]. The current study evaluates initial self-disclosure when the user adopts the SNA and uses it for the first time and continued self-disclosure to describe their ongoing disclosure behavior over time. Previous research has shown that users are more likely to disclose information via the social network when their perceptions of perceived benefits are high [47,53]. When using a social networking service for the first time, the psychological assessment of benefits determines the disclosure of personal information, because users want to be able to grow the network, to change settings, to express openly, to build identity, and to enjoy [38]. Social interaction is a fundamental benefit of social networking use causing individuals to disclose personal information to other in order to interact with other in the network [38]. Based on the fundamental tenets of TBU, perceptions of social benefits will shift over time due to experience with the network. Based on existing research identifying a positive relationship between perceived benefits and self-disclosure [53,54], it is predicted that this relationship will be significant in the current study at both the pre-adoption and post adoption stages of use behavior.

H2a. Pre-perceived benefit is positively related to the initial self-disclosure.

H2b. Initial perceived benefit is positively related to the continued self-disclosure.

Personal concepts of privacy are linked with values, perceptions, beliefs, and experiences [21,22]. Privacy is related to amount of information that an individual chooses to share with others [55]. Privacy-related perceptions originate from an individual's information processing during their engagement with a technology [56]. People with higher concerns regarding their privacy may exhibit lower intentions to adopt technologies that require disclosure of their personal information. Prior research shows that SNS usage increases threats to privacy of users [42]. Privacy experiences form users' privacy perceptions are typically built on automatic cognitive heuristics [56]. Initial privacy concerns have been shown to influence the intention of new technology adoption (e.g., SNA). According to the conceptual model of dynamic privacy trade-off, SNS users gain initial usage experiences when they use a service. TBU shows that a shift in beliefs regarding privacy concerns influence the continued use of a given technology. For example, users who have experienced privacy invasions would generally have higher privacy concerns compared to others [40]. Based on the inverse relationship shown between privacy concern and use behaviors, it is predicted that privacy concern will contain a negatively relationship with use behavior at both the initial use and continued use stages.

H3a. Pre-privacy concern is negatively related to the initial use a new SNA.

H3b. Initial privacy concern is negatively related to the continued use a new SNA.

Disclosure of self- information in SNSs poses possible risks to a user [53]. Previous research has shown a negative relationship between privacy concern and self-disclosure [57,58]. Possible future risks of self-disclosure make people more hesitant to disclose personal information [59]. As a result, prior privacy concerns influence the future disclosure on a new SNA. It has been shown that privacy concerns influence self-disclosure behaviors in social networking [47]. However, findings of prior literature are not clear whether updated privacy-related beliefs during a continued usage, have similar effect on self-disclosure. Based on previous finding of privacy concerns and its relationship with self-disclosure, the current research posits that the negative relationship between these constructs will exist at both the initial and continued use stages.

H4a. Pre-privacy concern is negatively related to the initial self-disclosure.

H4b. Initial privacy concern is negatively related to the continued self-disclosure.

3.2. Usage behaviors and updated privacy trade-off

Self-disclosure is one of user behaviors in the process of usage mobile apps and building social relationships [60]. Disclosure personal information is the first step in using social network apps and making relationships with other members in online social network [61]. To build relationship with others in social networks, people need to initially disclose personal information and build their identity [62]. For example, to connect to friend or family members users should use their name or personal photo to make themselves known to another person. During the usage of new social networks, people continuously share personal information as a result of the time they spend on the app or the type of features they use. If users want to be invited to an event, they need to disclose their personal information as a result. During communications of users in SNAs, self-disclosure behavior occurs regularly [63]. Usage and self-disclosure happen almost at the same time. When a user experiences a messaging option or commenting, personal information is also shared at that moment. In social networks, self-disclosure is generally beneficial because it builds intimacy in relationships [63]. When individuals use a SNA for the first time, their initial perceptions could change due to their actual experience. Positive experiences have been shown to result in a higher level of information disclosure behavior [64]. As a result, if users invest more time during their first experience with a SNA and use more functions, they are likely to disclose more personal information. Thus, we posit that:

H5a. Initial use is positively related to the initial self-disclosure on a new SNA.

H5b. Continued use is positively related to the continued self-disclosure on a new SNA.

As illustrated by TBU, perceptions may shift over time as individuals gain experience with a given technology [41,65]. Prior research has shown significant distinctions between pre-adoption and post-adoption perceptions [65,66]. The changes in perceptions after adoption of a new IT (i.e., the new SNA) can be attributed to the knowledge gained through initial experience [65,67]. Prior to adoption, and individual conceives internal beliefs about the new app that are confirmed or disconfirmed through initial use and experience [67]. As a result, prior perceptions that influenced initial use may shift after adoption once new information is discovered. In accordance with TBU, we argue that adoption and initial use behaviors will result in a shift in privacy trade-off perceptions. Once an individual adopts the SNA and uses it, their perceived benefits and privacy concerns are likely to shift after processing the new information gathered. Engaging in behaviors influencing the future perceptions of future benefits [68]. Individuals with positive experiences from initial use of the SNA will perceive an increase in the benefits from the SNA [27]. However, just as positive experiences influence perceived benefits, negative experience are likely to result in an increase of privacy concerns about the SNA. Usage intensity is shown to be associated with the privacy concern [69]. Users with a positive first experience are likely to use the app more, resulting in a higher perceived benefits and decreased privacy concerns. Based on these arguments, we posit that:

H6a. Initial use is positively related to the initial perceived benefit.

H6b. Initial use is negatively related to the initial privacy concern.

Prior to initial use, individuals internalize pre-perceptions about an app due to uncertainty [66]. Personal feelings, experience with similar technologies, or other factors may influence their pre-privacy trade-off perceptions. However, once an individual has adopted the app and used it, they may experience confirmation to their prior beliefs or update their beliefs based on the new information processed from use [67]. As TBU presented, perceptions shift over time as individuals gain experience with a given technology [65,67]. To fully experience benefits of social networks, individuals need to participate in self-disclosure [70].

As users begin disclosing their personal information on the SNA, they start building their identify on the app, increasing the number of connections, obtaining social rewards, and enjoying using the app [34]. As users disclose more information, the full range of benefits become apparent to them increasing their positive feeling toward the app resulting in an increase of perceived benefits. However, initial experience may also have a negative impact on the user causing them to not disclose information due to perceived risks or lack of control of their information [59]. These negative initial experiences can result in an increase of privacy concerns with the app. Based on the arguments above, we hypothesize that:

H7a. Initial self-disclosure is positively related to the initial perceived benefit.

H7b. Initial self-disclosure is negatively related to the initial privacy concern.

3.3. Control variables

In addition to the proposed hypotheses, we propose several controls variables that may influence the usage behaviors. The control variables include age, gender, prior social networking experience (PSNE), and personal innovativeness in IT (PIIT) [6]. PIIT is an enduring trait that every individuals possess [71] and has an effect on the usage of new technology [72]. While privacy trade-off perceptions may shift during the adoption of a new technology, personal innovativeness is stable situation-specific [73].

4. Methodology

To test the proposed model, a longitudinal approach is necessary to evaluate the changes in privacy trade-off perceptions (perceived benefits and privacy concern) over time and their relationship with use behaviors (actual use and self-disclosure) during the pre-use (t0), initial use (t1), and continued use (t2) periods of a new SNA.

4.1. Measurement development

Three surveys were conducted in three different times (i.e., t0, t1 and t2) to capture privacy trade-off perceptions and usage. Self-reported app usage and information disclosure behaviors were used to capture use behaviors in phase 1 and 2. Appendix A summarizes the measurement items. We adopted most measurement items from previously validated scales in related literature and modified for the context of the current [74]. Most items were measured using 7-point Likert scales ranging from 1 (strongly disagree) to 7 (strongly agree) to increase the reliable for capturing respondent perceptions [75].

4.2. Data collection procedures

A new privacy-based SNA called Sociabile was used to conduct this study.[2] Survey questionnaires were distributed to students at a major university in the US. Students are typical users of social networks and mobile apps and thus are representative of the population of users to predict disclosure behavior during the adoption of a new SNA. Furthermore, Sociabile is a startup company that had no users to sample from at the time of this study. Sociabile's target market for launching the new app is college students. By introducing Sociabile to students, we followed the marketing strategy laid out by Sociabile and capturing a representative sample of the population of its target users. The sample used was not a random sample due to the use of students in classes that

the app was introduced to. However, based on previous research on generalizability, it can be argued that a representative sample is generalizable suitable for research [76].

Data collection consisted of three phases administered at different times to measure changes in perceptions and use behaviors over time. Participants were recruited from students enrolled in various undergraduate business courses. Phase 1 introduced the new SNA to the participants and used a survey to capture pre-use perceptions and yielded 390 respondents. Respondents were then asked to install and use the Sociabile app on their smartphones. Phase 2 was conducted one week after phase 1 to capture privacy trade-off perceptions and usage experiences after adoption using a second survey and server data provided by Sociabile. The second survey captured privacy trade-off perceptions and self-reported use from 349 respondents who were adopters of the app. Based on research identifying peak abandonment rates of mobile apps being one month after adoption [77], phase 3 of the study was administered one month after phase 2 and consisted of a survey to capture self-reported use from the participants and usage data from Sociabile to evaluate self-disclosure behaviors. There were 301 respondents that participated in the phase 3 of the study. Users who completed all three phases were included in the analysis so that pre, initial, and continued evaluations could be conducted. Participants were offered extra credit for participating in the pre-use stage survey. No extra credit or compensation was provided for downloading and using the app or participation in the second and third phases of the study. This ensured that participation was completely voluntary, and expectation of rewards and compensation did not motivate respondents. Use construct was measured based on the user's self-reported usage time in each session before completing the phase 2 and phase 3 surveys.

Self-disclosure was based on aggregating information that adopters initially entered as a part of their profile creation process or later as a part of their communication and posting actions on the app. Self-disclosure is measured by the number of general information (such as nickname, hobbies, profile image, user name, email) and specific information (physical appearance, current work place, gender, DOB, time capsules, my mind posts, image posts) fields. To analyze all phases together, we provided the social network a list of users who took the survey and they matched the data and returned the non-identifying information to the researchers for analysis. The final dataset includes 290 usable responses suitable for analysis. Table 2 shows the demographic information of the final dataset.

5. Analysis and results

The proposed research model was tested using partial least squares (PLS) analysis using Smart PLS 3.2.6 because PLS employs a component-based approach for estimation that minimizes residual distributions [78], and is best suited for testing complex relationships by avoiding inadmissible solutions and factor indeterminacy [75]. A three-step analysis procedure was implemented: measurement model assessment including reliability and validity tests, common method bias checking, and evaluation of structural model.

5.1. Measurement model assessment

We evaluate the measurement model by examining the reliability (composite and indicator reliabilities), convergent validity, and discriminant validity of measurement items [79]. Since perceived benefits and privacy concerns are formative second-order constructs, calculations of AVEs for second-order constructs are performed following the guidelines provided by Becker [80]. Table 3 presents the descriptive statistics, composite reliability values, Cronbach's alpha values, and the average variance explained (AVEs) of the principal constructs. Composite reliability is established if all calculated values exceed 0.70 [81,82]. Cronbach's alpha scores of 0.70 or greater are considered

---

[2] Sociabile is a new free social networking app developed by Sociabile LLC and available on iTunes and Google play. More information related to Sociabile can be found in Appendix B.

Table 2
Demographic information.

Gender	Age	Disposable income		Academic standing	
Male: 55%	Min: 18	< 5000:	48%	Freshman:	4%
Female: 45%	Max: 41	5000–10,000:	21%	Sophomore:	14%
	Mean: 23	10,000–15,000:	21%	Junior:	65%
		15,000–20,000:	1%	Senior:	17%
		> 20,000:	9%	Graduate:	0%

Phase 1: n = 390; phase 2: n = 349; phase 3: n = 301; usable responses: n = 290.

Table 3
Descriptive statistics.

No.	Construct	Mean	SD	CA	CR	AVE
1	Initial use (t1) in minutes	5.58	1.00	n/a	n/a	1.00
2	Initial self-disclosure (t1)	5.58	2.43	0.89	0.93	0.86
3	Continued use (t2) in minutes	8.51	2.64	n/a	n/a	1.00
4	Continued self-disclosure (t2)	5.61	1.93	0.96	0.98	0.96
5	Perceived benefits: social rewards (t0)	5.60	0.98	0.78	0.90	0.82
6	Perceived benefits: enjoyment (t0)	5.66	1.03	0.81	0.91	0.84
7	Perceived benefits: ubiquity (t0)	5.77	0.78	0.92	0.96	0.93
8	Perceived benefits: timeliness (t0)	5.73	0.88	0.87	0.94	0.89
9	Perceived benefits: social rewards (t1)	4.78	1.12	0.90	0.95	0.91
10	Perceived benefits: enjoyment (t1)	4.99	1.08	0.95	0.98	0.95
11	Perceived benefits: ubiquity (t1)	4.93	1.16	0.94	0.97	0.94
12	Perceived benefits: timeliness (t1)	5.01	1.12	0.93	0.97	0.94
13	Privacy concerns: collection (t0)	6.20	1.11	0.85	0.93	0.87
14	Privacy concerns: secondary use (t0)	6.18	1.51	0.94	0.97	0.94
15	Privacy concerns: improper access (t0)	6.25	1.34	0.97	0.99	0.97
16	Privacy concerns: error (t0)	6.07	1.46	0.97	0.99	0.97
17	Privacy concerns: collection (t1)	4.75	1.08	0.91	0.96	0.92
18	Privacy concerns: secondary use (t1)	4.47	1.42	0.96	0.98	0.96
19	Privacy concerns: improper access (t1)	4.67	1.10	0.92	0.96	0.93
20	Privacy concerns: error (t1)	4.66	1.20	0.93	0.96	0.93

SD: standard deviation, CA: Cronbach's Alpha, CR: composite reliability, AVE: average variance extracted; Time: t0 = phase 1 (Week 1); t1 = phase 2 (Week 2); t2 = phase 3 (Week 5).

acceptable [82], while scores between 0.8 and 0.9 are considered satisfactory [83]. All values of composite reliabilities and Cronbach's alpha exceed 0.70, verifying the reliability of measurement items. Initial use and continued use are calculated single measure resulting in AVEs of 1.00 and no composite reliability and Cronbach's alpha. Appendix C shows correlations among constructs and AVEs and Appendix D presents factor loadings of measurement items.

Next, convergent validity was assessed by evaluating the AVEs [79]. Convergent validity is established if AVE reaches at least 0.50 or if principal hypothesized constructs load much higher than other constructs [78]. All AVEs exceed 0.50, thus establishing convergent validity. Discriminant validity is established by initially ensuring an indicator's outer loading on a construct is greater than cross loadings with other constructs, and next by ensuring for each construct the square root of AVE is higher than the outer correlations [79]. The results show all outer loadings are greater than cross loadings for each construct and squared root of AVEs are higher than outer correlations. The results affirm discriminant validity. Overall, results show high reliability and validity of the posited measurement model.

Common method bias (CMB) is a measurement error resulting in erroneous conclusions in studies implementing survey questionnaire [84]. The presence of CMB is evaluated using Harman's single factor test and the Liang et al. [85] method. CMB is present if there is a single factor from the factor analysis, or there is a single factor which accounts for the majority of the covariance among the variables [84]. First, all 38 items entered the explanatory factor analysis and the un-rotated solution outcome was eight total factors, which equals the number of latent variables in the posited model. Second, the un-rotated single factors from the explanatory factor analysis accounts for 25.8% of the variance

in the data which is less than the 50% upper bound. Eight factors emerged which accounted for 81.7% of the variance in the data with the first factor accounting for < 50% of the total variance. In addition, the threat of CMB is examined following the procedure suggested by Liang et al. [85]. The result of analysis is presented in Appendix E. According to the results, all the method factor loadings are insignificant except one. Based on Harman's single factor test and the procedures suggested by Liang et al. [85], we confirm that CMB is not an issue in the measurement model of this study.

5.2. Structural model assessment

The PLS results of the structural model show during the pre-use to initial use stages (phase 1 to phase 2), 41% variance of initial use is explained by pre-perceived benefits and pre-privacy concerns. In addition, 22% of the initial self-disclosure variance is explained by pre-privacy concerns and initial use. During the initial use stage to continued use stages (phase 2 to phase 3), 39% of continued use variance is explained by initial perceived benefits and initial privacy concerns. Also, 43% of the continued self-disclosure variance is explained by continued use. In phase 2, 29% of the variance in initial perceived benefits is explained by initial SNA use behaviors and 26% of the variance in initial privacy concerns explained by initial use behaviors. Thus, the research model demonstrates satisfactory explanatory power to capture the effect of privacy trade-off on the continued use and continued self-disclosure.

Findings demonstrate that pre-perceived benefits positively influence initial use of SNAs (b = 0.59, p < 0.001), supporting H1a. The relationship between initial perceived benefits and continued use is also significant (b = 0.20, p < 0.001), supporting H1b. While the relationship between pre-perceived benefits and initial self-disclosure (H2a) were not supported, the results demonstrated a significant relationship between initial perceived benefits and continued self-disclosure (H2b). Pre-privacy concerns exhibited insignificant results in its relationship with initial use (H3a) but a strong negative relationship between initial privacy concerns and continued use (H3b). The relationship between pre-privacy concerns and initial self-disclosure is significant (b = −0.21, p < 0.01), supporting H4a while the relationship between initial privacy concern and continued self-disclosure was not supported (H4b). The relationships between initial use and initial self-disclosure (b = 0.41, p < 0.001) and continued use and continued self-disclosure (b = 0.60, p < 0.001) are significant, supporting H5a and H5b. The relationship between initial use and initial perceived benefits is significant (b = 0.46, p < 0.001), supporting H6a while the relationship between initial use and initial privacy concerns was not significant (H6b). The relationships between initial self-disclosure and both initial perceived benefits (b = 0.14, p < 0.05) and initial privacy concerns (b = −0.27, p < 0.01) are significant, supporting H7a and H7b. Results of the research model and changes in coefficients' dimensions of perceived benefit and privacy concern are shown in Fig. 3 with a list of supported hypotheses presented in Table 4.

Based on the results, all formative indicators of perceived benefits and privacy concerns are significant, confirming the choice of formative construct. Also, changes in the coefficients of privacy trade-off prior to using a SNA (stage 1) to initial use (stage 2) show the dynamics of privacy trade-off and the effects of experience with the app. To ensure findings of analysis are not confounded by other variables, we controlled the possible effect of age, gender, prior social networking experience, and personal innovativeness in IT (PIIT) on dependent variables. All control variables were initially included in the model but then two dropped due their insignificance.

5.3. A post hoc analysis: mediation test

The relationships between initial privacy concerns and continued self-disclosure were not supported, which raised the question of
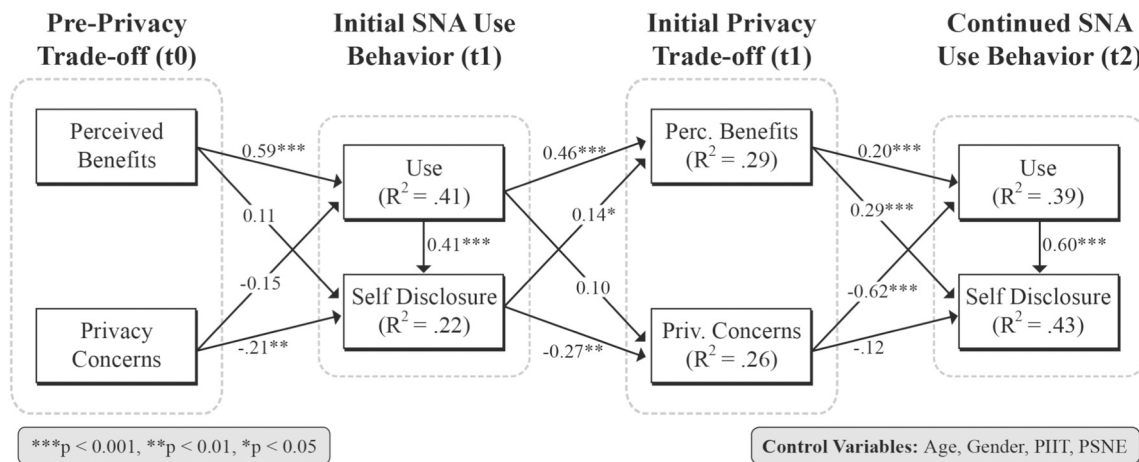
Fig. 3. The privacy trade-off model analysis.

mediation between these two constructs via continued use. To evaluate if a mediating effect exists, a post hoc analysis was conducted using Baron and Kenny's three step approach for mediation testing. First, we isolate and test the relationship between initial privacy concern and continued use, displaying a negative correlation between these two variables. Next, we isolate and test the relationship between initial privacy concern and continued self-disclosure that yield similar results with a negative correlation between the variables. After demonstrating that initial privacy concern significantly influenced continued use and continued self-disclosure independently, a third test was executed with all three variables included in the model. The results show that by including continued use into the model, the relationship between initial privacy concern and continued self-disclosure is no longer significant. Based on the results of the three-step approach, it is concluded that continued use fully mediate the relationship between initial privacy concern and continued self-disclosure. Table 5 displays the results of the mediation at all three steps.

6. Discussion

The current study evaluated changes in trade-off perceptions over time through pre-adoption, initial use, and continued use behaviors. The relationship between the theory of belief updating (TBU) and privacy trade-off perceptions was conceptualized and empirically tested using a longitudinal study conducted at three stages of adoption and use in the context of SNAs. While there was a mix of supported and unsupported hypotheses in the results, the change of significance between constructs pre- and post-adoption was the most interesting. Based on

TBU, it is expected that a change in beliefs over time will evolve as users gain experience with a given technology. These changes in beliefs are most evident from the change in relationships between privacy trade-off and use behaviors over time.

To understand how beliefs could change with experiences via individual experience with the SNAs, the relationships between privacy trade-off and use behaviors were analyzed. Pre-perceived benefits demonstrate significant results explaining initial use behavior but yield insignificant results in explaining initial self-disclosure behaviors as hypothesized. However, privacy trade-off after initial use demonstrates a change in perception, with perceived benefits significantly influencing both continued use and continue self-disclosure. Based on the results, it can be argued that the attainment of benefits prior to adoption influences usage behavior toward initial usage of the app while post-adoption perceived benefits influence both continued use and self-disclosure behaviors. Pre-privacy concerns demonstrate opposite effects with privacy concerns influencing initial self-disclosure behaviors while privacy concerns after initial use are insignificant in relation to self-disclosure but yield positive influence on continued use behavior. The switch in significance between privacy trade-off constructs and use behaviors (pre- and post-adoption) support TBU by demonstrating a change in beliefs over time in relation to experience. However, the most interesting discovery is how these relationships change and how they influence behaviors over time. Pre-adoption perceptions demonstrate that perceived benefits influence adoption and use while privacy concerns influence initial self-disclosure. The study suggests that people choose an app to use based on the perception of benefits they may receive. However, unfamiliarity of the new app can result in increased

Table 4
Hypotheses and results.

Hypotheses			Result
H1a:	Pre-perceived benefit (t0)	➔ Initial use (t1)	Supported (+)
H1b:	Initial perceived benefit (t1)	➔ Continued use (t2)	Supported (+)
H2a:	Pre-perceived benefit (t0)	➔ Initial self-disclosure (t1)	Not supported
H2b:	Initial perceived benefit (t1)	➔ Cont. self-disclosure (t2)	Supported (+)
H3a:	Pre-privacy concern (t0)	➔ Initial use (t1)	Not supported
H3b:	Initial privacy concern (t1)	➔ Continued use (t2)	Supported (−)
H4a:	Pre-privacy concern (t0)	➔ Initial self-disclosure (t1)	Supported (−)
H4b:	Initial privacy concern (t1)	➔ Cont. self-disclosure (t2)	Not supported
H5a:	Initial use (t1)	➔ Initial self-disclosure (t1)	Supported (+)
H5b:	Continued use (t2)	➔ Cont. self-disclosure (t2)	Supported (+)
H6a:	Initial use (t1)	➔ Initial perceived benefit (t1)	Supported (+)
H6b:	Initial use (t1)	➔ Initial privacy concern (t1)	Not supported
H7a:	Initial self-disclosure (t1)	➔ Initial perceived benefit (t1)	Supported (+)
H7b:	Initial self-disclosure (t1)	➔ Initial privacy concern (t1)	Supported (−)

Note: t0 = phase 1; t1 = phase 2; t2 = phase 3.

Table 5
Mediation test results.

Mediation	Relationship		Correlation
Step 1:	Initial privacy concern (t1)	→ Continued use (t2)	−0.59**
Step 2:	Initial privacy concern (t1)	→ Continued self-disclosure (t2)	−0.36**
Step 3:	Initial privacy concern (t1)	→ Continued use (t2)	−0.59**
	Continued use (t2)	→ Continued self-disclosure (t2)	0.65**
	Initial privacy concern (t1)	→ Continued self-disclosure (t2)	−0.09

Note: **Significant at 0.01 level.

privacy concerns limiting their willingness to disclose information until they have used the app more. Initial experience with the app will confirm or disprove people's initial beliefs, resulting in altering perceptions of the app as related to benefits and privacy concerns. These changes in beliefs will influence on-going use behaviors of people using the app. At this point, perceived benefits begin influencing continued self-disclosure while continuing to influence continued use. The effects of privacy concerns switch after initial use to influence continued use behavior while no longer influencing self-disclosure behavior. Logically, privacy concerns should influence an individual's self-disclosure behavior. This is where the mediation effect comes into play as privacy concerns influence self-disclosure through the mediation of continued use. Privacy concerns influence the continued use of the app, resulting in increased continued self-disclosure behaviors over time. Based on these findings, there are several implications identified that make significant contributes to both theory and practice.

6.1. Theoretical implications

There are several contributions that the current research makes to existing theories in the information systems field. The most significant one is the evaluation of privacy trade-off perceptions using a longitudinal approach, implementing TBU to determine three phases of use behaviors: pre-use (phase 1), initial use (phase 2), and continued use (phase 3). Previous research reflects a positive relationship from perceived benefits and negative relationship from privacy concerns on usage behaviors of use and self-disclosure. Findings in the current research extend this model by revealing varying relationships between privacy trade-off perceptions and use behaviors depending on the stage of adoption and use. The current research also shows the reciprocal effects of privacy trade-offs and use behaviors over time as each affect the other at different stages of adoption and use. While privacy trade-off perceptions influence use behaviors, it is shown that use behaviors influence privacy trade-off beliefs over time as users gain more experience with this technology. These changes in beliefs therein influence continue use behaviors. It can be predicted that there is a constant interaction effect over time between privacy-tradeoff beliefs and use behaviors. The current research also demonstrates the importance of longitudinal studies evaluating pre-adoption and post-adoption perceptions and behaviors as static results yield varying results at different points through the adoption life cycle.

6.2. Practical implications

The current research also has several implications for practitioners in the context of social networking apps. Perceived benefits influence adoption and initial use of SNA's while privacy concerns influence the users' initial self-disclosure behaviors. Understanding factors that influence adoption and use behaviors can help startup entrepreneurs (e.g. Sociabile in this study) when trying to attract users and build their brand. With a stronger focus on the potential benefits, new SNAs can increase adoption of their app while focusing on ways to mitigate

privacy concerns to influence initial self-disclosure. The efforts made to positively influence initial use behaviors can result in a positive change of perceived privacy trade-off after initial use, thereby increasing continued use behaviors over time. Understanding the dynamics of beliefs and behaviors can help SNAs focus on the functionality needed to instill confidence in users that their information is protected while taking measures to help users realize the value of the app, post-adoption, resulting in continued use. Although it is important to understand factors that help build the SNA community, long-term success depends on sustainability of the network. Hence, the longitudinal results of the current research provide valuable findings, helping SNAs understand the shift in privacy trade-off perceptions over time and their influence on use behaviors.

6.3. Limitations and future research

While the current research provides several implications for theory and practice, there are limitations that must be acknowledged and opportunities for future research. The use of student participants in the study coincides with the goals of the SNA used and their target market creating a representative sample for generalization. However, future growth of SNA startups such as *Sociabile*, and more established SNAs, are likely to have a broader range of users in relation to demographic, geographic, and sociographic characteristics. Future researchers should evaluate the growth of SNAs as the community grows and reaches a wider audience with varying characteristics. With continued globalization, the findings of this study should also be included into cross-cultural contexts to increase the generalizability of the results. Another limitation relates to the context of the study and the niche focus on the SNA evaluated. *Sociabile* is a privacy-based SNA focused on personal networks and close tie connections. Many other SNAs consist of open platforms designed to increase the number of friend connections with the disclosure of information in order to increase marketing capabilities. Because of this factor, the findings in the current study are only applicable to privacy based social networking apps. Future research should extend the current study to evaluate change in behaviors as they affect the privacy trade-off and use behavior dynamic in public and open SNAs. In addition, future studies can extend the current study by including additional constructs not evaluated in the current research such as risk aversion, trust, social capital, ease of use, and an expansion of perceived benefits evaluating various hedonic and utilitarian benefits.

7. Conclusion

The goal of the current research was to evaluate the relationship between the privacy trade-off/use behaviors dynamic/and the change in beliefs over time. Based on the literature, a research model was derived and tested using a longitudinal approach at three points in time, consisting of pre-adoption, initial use, and on-going use stages. The results revealed the change in privacy trade-off perceptions and their influence on use behaviors at different stages of adoption and use.

While perceived benefits only influenced self-disclosure behavior during the ongoing use phase, the relationship between privacy concerns and use behaviors was the most interesting. In the pre-adoption stage, privacy concerns significantly influenced initial self-disclosure but had no effect on adoption and initial use. During the ongoing use stage, privacy concerns significantly influenced on-going use and demonstrated a relationship with self-disclosure through the mediating effect of use. With the extension of privacy trade-off and TBU theories based on a longitudinal approach, the current research established varying effects of the relationships at different points in time, creating a strong foundation for future studies and solidifying the importance of longitudinal work in the IS research.

Acknowledgments

Appendix A. Measurement instrument

Construct	Code	Items	Reference
Privacy concern[a]	COL1	I am concerned [if/that] I am asked to provide my personal information on this app.	[26,86]
	COL2	I am concerned [if/that] this app stores too much of my personal information.	
	ACC1	I am concerned [if/that] there is the possibility of unauthorized access to databases that contain my information on this app.	
	ACC2	I am concerned [if/that] unauthorized people can access my personal information on this app.	
	ERR1	I am concerned [if/that] this app does not have thorough procedures to prevent errors in my personal information.	
	ERR2	I am concerned [if/that] there are not enough features to double-check the accuracy of my personal information on this app.	
	SEC1	I am concerned [if/that] this app uses my personal information for other purposes without getting my authorization.	
	SEC2	I am concerned [if/that] this app shares my information without my consent.	
Perceived benefit[a]	UBQ1	I can access to the relevant services everywhere.	[87,88]
	UBQ2	I am able to access to the relevant information at the right place.	
	TIM1	I can get the just-in-time information/services.	
	TIM2	I can get an answer to my questions right away.	
	SR1	The interaction with other users [will fulfill/fulfills] my social needs in some way.	[6,32]
	SR2	The interaction with other users [will help/helps] me cultivate a good relationship with the other party.	
	ENJ1	The use of this app [will give/gives] me pleasure.	
	ENJ2	Using this app [will make/makes] me feel good.	
Personal innovativeness in IT	PIIT1	I like to experiment this app.	[71,89]
	PIIT2	Among my peers, I am usually the first to use this app.	
	PIIT3	I would look for ways to experiment this app.	
	PIIT4	I am not hesitant to use this app.	
Initial use/continued use	Use	Total time in minutes that a user has spent on the app at the end of each phase.	[45]
Self-disclosure	DISC1	Number of general personal information fields filled (e.g., such as nickname, hobbies, profile image, user name, email, etc.).	New
	DISC2	Number of specific personal information fields filled (e.g., physical appearance, current work place, gender, DOB, time capsules, mind posts, image posts, etc.).	

 [a] Note. For privacy concern and perceived benefit, questions are modified using different verb tense to appropriately capture user responses before and after using the app for phase 1 and phase 2.
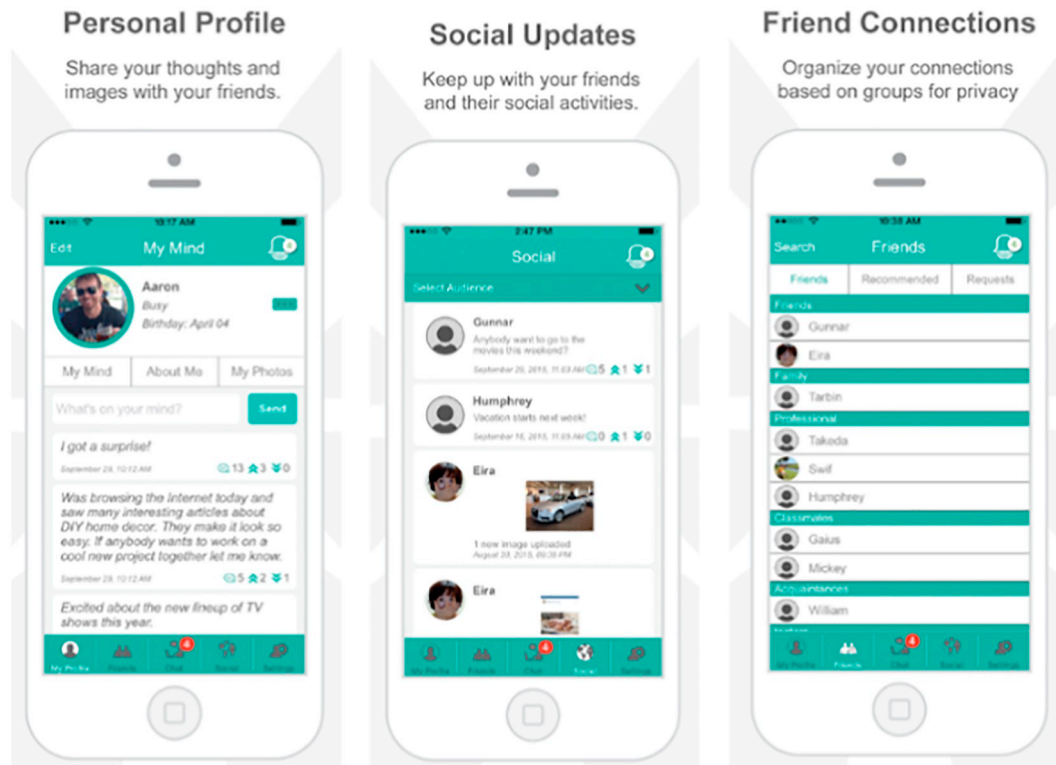
Appendix B. Sociabile app

Sociabile is a new free social networking app developed by Sociabile LLC and available on iTunes and Google play.[3] This app redefines the social networking paradigm by providing a privacy-based networking specifically allowing users to control who they connect and who can view their information. Areas that differentiate Sociabile include privacy, innovation, and an ad free environment. Time capsules are the first of many innovations that added to the platform. Some of the important features of Sociabile include:

- <u>Privacy:</u> To connect to others a user must know the phone number or unique user ID. Names are not searchable, which allows users to only connect to others they choose to connect to. Once connected, user is placed in groups that are used to grant access to posted content. Custom privacy settings can be used to grant permission groups or individuals for content posted.
- <u>Animated emoticons:</u> Animated emoticons bring users' chat conversations to life.
- <u>Time capsules:</u> Time capsules are a new way to send messages that transcend space and time. These are message containing text and images that can only be opened at the designated date and time set by the sender.

Below are examples of the app user interface. More information about Sociabile LLC and the mobile app can be found on their website at www.scble.com.

---

 [3] Sociabile LLC is a startup social networking company that developed a privacy-based application that was used for the current study. Sociabile is a portmanteau of the words 'social' and 'mobile' that differentiates itself from traditional social networks (e.g., Facebook, Instagram, Twitter, etc.) due to their focus on privacy and protection of user data. Members can only add other members as friends if they know the user's specific user ID or phone number. Friend connections are organized by groups, which are used for privacy settings to control who has access to information posted on the user's profile. Groups and individual users can be granted access to specific content rather than having new posts broadcast to everybody and blocking those who are not permitted. Sociabile does not push advertisements to users or sell user data in according to their focus on privacy. Furthermore, when posts are deleted from a user's account, the data is also deleted permanently from Sociabile's servers. The SNA is available on iTunes and Google Play as a free download and free to register. The company's revenue model revolves around selling digital content, such as the animated emoticons available for purchase through the app.

Personal Profile
Share your thoughts and images with your friends.

Social Updates
Keep up with your friends and their social activities.

Friend Connections
Organize your connections based on groups for privacy

Appendix C. Construct correlations with square root of AVEs (bold)

No.	Principal construct	AVE	Mean	SD	1	2	3	4	5	6	7	8
1	Pre-perceived benefit	0.87	5.69	0.92	**0.93**							
2	Initial perceived benefit	0.94	4.93	1.12	0.44	**0.97**						
3	Initial self-disclosure	0.86	5.58	2.43	0.34	0.31	**0.93**					
4	Continued self-disclosure	0.96	5.61	1.93	0.38	0.49	0.72	**0.98**				
5	Initial use	1.00	5.58	1.00	0.74	0.42	0.40	0.54	**1.00**			
6	Pre-privacy concern	0.94	6.18	1.36	0.26	0.28	0.28	0.27	0.27	**0.97**		
7	Initial privacy concern	0.94	4.64	1.20	0.08	0.50	0.05	0.14	0.22	0.48	**0.97**	
8	Continued use	1.00	8.51	2.64	0.48	0.55	0.61	0.79	0.50	0.27	0.23	**1.00**

Appendix D. Factor loadings

	Item	PB (t0)	PB (t1)	DISC (t1)	DISC (t2)	USE (t1)	PC (t0)	PC (t1)	USE (t2)
1	ENJ1_1	0.87	0.50	0.39	0.46	0.70	0.28	0.11	0.59
2	ENJ2_1	0.82	0.36	0.30	0.28	0.63	0.00	-0.01	0.33
3	SR1_1	0.73	0.29	0.16	0.12	0.45	0.34	0.11	0.16
4	SR2_1	0.77	0.38	0.28	0.34	0.64	0.26	0.15	0.43
5	TIM1_1	0.88	0.32	0.26	0.32	0.67	0.17	0.01	0.37
6	TIM2_1	0.81	0.35	0.32	0.34	0.55	0.30	0.08	0.43
7	UBQ1_1	0.90	0.37	0.30	0.32	0.65	0.26	0.07	0.43
8	UBQ2_1	0.88	0.34	0.26	0.33	0.65	0.17	0.01	0.43
9	ENJ1_2	0.29	0.89	0.31	0.48	0.39	0.26	0.50	0.53
10	ENJ2_2	0.38	0.89	0.35	0.44	0.42	0.33	0.43	0.44
11	SR1_2	0.49	0.93	0.24	0.48	0.44	0.35	0.44	0.52
12	SR2_2	0.35	0.87	0.29	0.42	0.34	0.25	0.44	0.47
13	TIM1_2	0.42	0.93	0.25	0.46	0.37	0.24	0.44	0.49
14	TIM2_2	0.42	0.91	0.32	0.37	0.34	0.24	0.46	0.41
15	UBQ1_2	0.40	0.93	0.30	0.43	0.34	0.16	0.44	0.52
16	UBQ2_2	0.44	0.90	0.20	0.48	0.37	0.23	0.46	0.61
17	DISC1 (t1)	0.34	0.40	0.91	0.60	0.45	-0.04	-0.08	0.30
18	DISC2 (t1)	0.20	0.16	0.83	0.73	0.27	-0.10	-0.34	0.41
19	DISC1 (t2)	0.31	0.21	0.54	0.98	0.30	-0.11	-0.34	0.48
20	DISC2 (t2)	0.37	0.29	0.52	0.98	0.38	0.03	-0.30	0.63
21	USE1 (t1)	0.42	0.39	0.36	0.31	1.00	0.23	0.24	0.48
22	USE2 (t2)	0.49	0.56	0.41	0.29	0.50	0.28	0.25	1.00
23	ACC1_1	0.18	0.22	0.24	0.21	0.19	0.95	0.45	0.20
24	ACC2_1	0.19	0.20	0.24	0.20	0.19	0.93	0.40	0.20
25	COL1_1	0.29	0.28	0.30	0.31	0.40	0.87	0.46	0.24
26	COL2_1	0.15	0.30	0.30	0.34	0.22	0.82	0.40	0.38
27	ERR1_1	0.24	0.25	0.28	0.25	0.24	0.96	0.44	0.24
28	ERR2_1	0.26	0.32	0.31	0.32	0.27	0.95	0.47	0.36
29	SEC1_1	0.37	0.28	0.22	0.16	0.24	0.90	0.46	0.23
30	SEC2_1	0.19	0.21	0.20	0.17	0.20	0.94	0.45	0.16
31	ACC1_2	0.11	0.44	0.10	0.17	0.24	0.53	0.94	0.17
32	ACC2_2	0.06	0.44	0.01	0.11	0.18	0.38	0.94	0.24
33	COL1_2	0.12	0.41	-0.05	-0.01	0.15	0.46	0.85	0.11
34	COL2_2	0.06	0.46	0.00	0.07	0.20	0.48	0.94	0.12
35	ERR1_2	0.06	0.33	0.06	-0.09	0.11	0.45	0.75	-0.08
36	ERR2_2	0.06	0.37	0.05	0.01	0.16	0.49	0.84	0.01
37	SEC1_2	0.08	0.45	0.07	0.29	0.25	0.29	0.83	0.48
38	SEC2_2	0.00	0.46	0.14	0.33	0.17	0.25	0.73	0.49

Time: *t0 = Phase 1 (Week 1); t1 = Phase 2 (Week 2); t2 = Phase 3 (Week 5)*
Perceived Benefit Dimensions are *SR: Social Rewards, ENJ: Enjoyment, UBQ: Ubiquity, TIM: Timeliness*
Privacy Concern Dimensions are *COL: Collection, SEC: Secondary Use, ACC: Improper Access, ERR: Error*

Note. Shaded cells indicate within construct factor loadings.

Appendix E. Common method bias analysis

Item	Substantive factor loading (R1)	R1^2	Method factor loading (R2)	R2^2
ENJ1_1	0.80**	0.64	0.26	0.07
ENJ2_1	0.83**	0.69	0.59*	0.35
SR1_1	0.91**	0.83	0.11	0.01
SR2_1	0.80**	0.64	−0.27	0.07
TIM1_1	0.89**	0.79	−0.01	0.00
TIM2_1	0.87**	0.76	−0.05	0.00
UBQ1_1	0.89**	0.79	−0.28	0.08
UBQ2_1	0.83**	0.69	−0.35	0.12
ENJ1_2	0.90**	0.81	0.05	0.00
ENJ2_2	0.84**	0.71	−0.10	0.01
SR1_2	0.90**	0.81	0.06	0.00
SR2_2	0.92**	0.85	0.08	0.01
TIM1_2	0.84**	0.71	0.14	0.02
TIM2_2	0.88**	0.77	0.13	0.02
UBQ1_2	0.86**	0.74	−0.18	0.03
UBQ2_2	0.86**	0.74	−0.19	0.04
DISC1 (t1)	0.87**	0.76	0.05	0.00
DISC2 (t1)	0.87**	0.76	−0.05	0.00
DISC1 (t2)	0.79**	0.62	0.13	0.02

DISC2 (t2)	0.80**	0.64	−0.13	0.02
USE1 (t1)	0.97**	0.94	0.19	0.04
USE2 (t2)	1.00**	1.00	0.12	0.01
ACC1_1	0.92**	0.85	−0.10	0.01
ACC2_1	0.90**	0.81	−0.11	0.01
COL1_1	0.74**	0.55	−0.03	0.00
COL2_1	0.92**	0.85	−0.15	0.02
ERR1_1	0.80**	0.64	−0.01	0.00
ERR2_1	0.85**	0.72	−0.03	0.00
SEC1_1	0.84**	0.71	−0.14	0.02
SEC2_1	0.77**	0.59	−0.04	0.00
ACC1_2	0.94**	0.88	−0.06	0.00
ACC2_2	0.88**	0.77	−0.03	0.00
COL1_2	0.91**	0.83	0.06	0.00
COL2_2	0.80**	0.64	0.17	0.03
ERR1_2	0.89**	0.79	0.01	0.00
ERR2_2	0.88**	0.77	0.17	0.03
SEC1_2	0.92**	0.85	−0.17	0.03
SEC2_2	0.88**	0.77	0.10	0.01
Average	0.87	0.76	−0.002	0.03

* $p < 0.05$.

** $p < 0.01$.

References

[1] A. Smith, Record shares of Americans now own smartphones, have home broadband, Pew Research Center. (2017) 1–3 http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

[2] C. Christensen, P. Prax, Assemblage, adaptation and apps: smartphones and mobile gaming, Continuum: Journal of Media & Cultural Studies. 26 (2012) 731–739.

[3] Statista, Mobile Social Media - Statistics & Facts, Mobile App Usage, https://www.statista.com/topics/2478/mobile-social-networks/, (2018).

[4] J. Gu, Y. (Calvin) Xu, H. Xu, C. Zhang, H. Ling, Privacy concerns for mobile app download: an elaboration likelihood model perspective, Decision Support Systems. 94 (2017) 19–28, https://doi.org/10.1016/j.dss.2016.10.002.

[5] N. Gerhart, M. Koohikamali, Social network migration and anonymity expectations: what anonymous social network apps offer, Computers in Human Behavior 95 (2019) 101–113.

[6] Z. Jiang, C.S. Heng, B.C.F. Choi, Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions, Information Systems Research. 24 (2013) 579–595.

[7] Y. Xu, M. Lin, H. Lu, G. Cardone, N. Lane, Z. Chen, A. Campbell, T. Choudhury, Preference, context and communities: a multi-faceted approach to predicting smartphone app usage patterns, Proceedings of the 2013 International Symposium on Wearable Computers, ACM, 2013, pp. 69–76.

[8] W. Hong, J.Y.L. Thong, Internet privacy concerns: an integrated conceptualization and four empirical studies, MIS Quarterly. 37 (2013) 275–298.

[9] T. Dinev, J. Goo, Q. Hu, K. Nam, User behaviour towards protective information technologies: the role of national cultural differences, Information Systems Journal. 19 (2009) 391–412.

[10] S. Choi, The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: social presence and privacy concern, Computers in Human Behavior 65 (2016) 325–333.

[11] R.M. Hogarth, H.J. Einhorn, Order effects in belief updating: the belief adjustment model, Cognitive Psychology. 24 (1992) 1–55.

[12] S.S. Kim, N.K. Malhotra, A longitudinal model of continued IS use: an integrative view of four mechanisms underlying postadoption phenomena, Management Science. 51 (2005) 741–755.

[13] M. Warkentin, A.C. Johnston, J. Shropshire, W.D. Barnett, Continuance of protective security behavior: a longitudinal study, Decision Support Systems. 92 (2016) 25–35.

[14] C. Wang, M.K.O. Lee, Z. Hua, A theory of social media dependence: evidence from microblog users, Decision Support Systems. 69 (2015) 40–49.

[15] L. Kelly, G. Kerr, J. Drennan, Privacy concerns on social networking sites: a longitudinal study, Journal of Marketing Management. 33 (2017) 1465–1489.

[16] M. Böhmer, B. Hecht, J. Schöning, A. Krüger, G. Bauer, Falling asleep with angry birds, Facebook and kindle: A large scale study on mobile application usage, Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, ACM, 2011, pp. 47–56.

[17] M. Kranz, L. Murmann, F. Michahelles, Research in the large: challenges for large-scale mobile application research - a case study about NFC Adoption using gamification via an app store, International Journal of Mobile Human Computer Interaction. 5 (2013) 45–61.

[18] Y.P. Chang, D.H. Zhu, Understanding social networking sites adoption in China: a comparison of pre-adoption and post-adoption, Computers in Human Behavior 27 (2011) 1840–1848.

[19] D.M. Boyd, N.B. Ellison, Social network sites: definition, history, and scholarship, Journal of Computer-Mediated Communication. 13 (2007) 210–230.

[20] T.L. James, M. Warkentin, S.E. Collignon, A dual privacy decision model for online social networks, Information and Management. 52 (2015) 893–908.

[21] H.J. Smith, T. Dinev, H. Xu, Information privacy research: an interdisciplinary review, MIS Quarterly. 35 (2011) 989–1016.

[22] D.J. Solove, A taxonomy of privacy, University of Pennsylvania Law Review. 154 (2006) 477–564.

[23] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems. 22 (2013) 295–316.

[24] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Information Systems Research. 15 (2004) 336–355.

[25] G. Bansal, F.M. Zahedi, Trust violation and repair: the information privacy perspective, Decision Support Systems. 71 (2015) 62–77.

[26] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Quarterly. 20 (1996) 167–196.

[27] M.-C. Lee, Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and perceived benefit, Electronic Commerce Research and Applications. 8 (2009) 130–141.

[28] R. Chitturi, R. Raghunathan, V. Mahajan, Delight by design: the role of hedonic versus utilitarian benefits, Journal of Marketing. 72 (2008) 48–63.

[29] D. Li, P.Y.K. Chau, H. Lou, Understanding individual adoption of instant messaging: an empirical investigation, Journal of the Association for Information Systems. 6 (2005) 102–129.

[30] C. Grange, I. Benbasat, Explaining customers' utilitarian and hedonic perceptions in the context of product search within social network-enabled shopping websites, in: Thirteenth Annual Workshop on HCI Research in MIS (SIGHCI 2014), Auckland, New Zealand, 2014.

[31] P.J. Bateman, J.C. Pike, B.S. Butler, To disclose or not: publicness in social networking sites, Information Technology & People. 24 (2011) 78–100.

[32] Z. Zhou, X.-L. Jin, Y. Fang, D. Vogel, Toward a theory of perceived benefits, affective commitment, and continuance intention in social virtual worlds: cultural values (indulgence and individualism) matter, European Journal of Information Systems. 24 (2015) 247–261.

[33] C.M.K. Cheung, M.K.O. Lee, A theoretical model of intentional social action in online social networks, Decision Support Systems. 49 (2010) 24–30.

[34] M. Koohikamali, D.A. Peak, V.R. Prybutok, Beyond self-disclosure: disclosure of information about others in social network sites, Computers in Human Behavior 69 (2017).

[35] C. Posey, P.B. Lowry, T.L. Roberts, T.S. Ellis, 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 (2010) 181–195.

[36] M. Koohikamali, N. Gerhart, M. Mousavizadeh, Location disclosure on LB-SNAs: the role of incentives on sharing behavior, Decision Support Systems. 71 (2015) 78–87.

[37] M. Taddicken, The 'Privacy Paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure, Journal of Computer-Mediated Communication. 19 (2014) 248–273.

[38] F. Xu, K. Michael, X. Chen, Factors affecting privacy disclosure on social network sites: an integrated model, Electronic Commerce Research. 13 (2013) 151–168.

[39] R. Chen, S.K. Sharma, Learning and self-disclosure behavior on social networking sites: the case of Facebook users, European Journal of Information Systems. 24 (2015) 93–106.

[40] B.C.F. Choi, Z.J. Jiang, B. Xiao, S.S. Kim, Embarrassing exposures in online social networks: an integrated perspective of privacy invasion and relationship bonding, Information Systems Research. 26 (2015) 675–694.

[41] H.-G. Chen, C.C. Chen, L. Lo, S.C. Yang, Online privacy control via anonymity and pseudonym: cross-cultural implications, Behaviour & Information Technology. 27 (2008) 229–242.

[42] H. Xu, H.-H. Teo, B.C.Y. Tan, R. Agarwal, Research note-effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Information Systems Research. 23 (2012) 1342–1363.

[43] A. Vasalou, A.N. Joinson, D. Courvoisier, Cultural differences, experience with social networks and the nature of "true commitment" in Facebook, International Journal of Human Computer Studies. 68 (2010) 719–728.

[44] J.W. Overby, E.-J. Lee, The effects of utilitarian and hedonic online shopping value

on consumer preference and intentions, Journal of Business Research. 59 (2006) 1160–1166.

[45] J.C.-C. Lin, H. Lu, Towards an understanding of the behavioural intention to use a web site, International Journal of Information Management. 20 (2000) 197–208.

[46] R. Lin, S. Utz, Self-disclosure on SNS: do disclosure intimacy and narrativity influence interpersonal closeness and social attraction? Computers in Human Behavior 70 (2017) 426–436.

[47] Z.D. Ozdemir, H. Jeff Smith, J.H. Benamati, Antecedents and outcomes of information privacy concerns in a peer context: an exploratory study, European Journal of Information Systems. 26 (2017) 642–660.

[48] P. (2013) Krasnova, H., Wenninger, H., Widjaja, T., & Buxmann, Envy on Facebook: A hidden threat to users' life satisfaction?, in: International Conference on Wirtschaftsinformatik, Leipzig, Germany, 2013: p. 16.

[49] R.C. Beatty, J.P. Shim, M.C. Jones, Factors influencing corporate web site adoption: a time-based assessment, Information and Management. 38 (2001) 337–354.

[50] N. Chung, C. Koo, The use of social media in travel information search, Telematics and Informatics. 32 (2015) 215–229.

[51] T. Hu, W.J. Kettinger, R.S. Poston, The effect of online social value on satisfaction and continued use of social media, European Journal of Information Systems. 24 (2015) 391–410.

[52] B. Contena, Y. Loscalzo, S. Taddei, Surfing on Social Network Sites: a comprehensive instrument to evaluate online self-disclosure and related attitudes, Computers in Human Behavior 49 (2015) 30–37.

[53] C. Cheung, Z.W.Y. Lee, T.K.H. Chan, Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence, Internet Research 25 (2015) 279–299.

[54] S. Dekhane, X. Xu, M.Y. Tsoi, Mobile app development to increase student engagement and problem solving skills, Journal of Information Systems Education. 24 (2013) 299.

[55] A.F. Westin, Social and political dimensions of privacy, Journal of Social Issues. 59 (2003) 431–453.

[56] T. Dinev, A.R. McConnell, H.J. Smith, Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box, Information Systems Research. 26 (2015) 639–655.

[57] H. Krasnova, S. Spiekermann, K. Koroleva, T. Hildebrand, Online social networks: why we disclose, Journal of Information Technology. 25 (2010) 109–125.

[58] Z. Liu, Q. Min, Q. Zhai, R. Smyth, Self-disclosure in Chinese micro-blogging: a social exchange theory perspective, Information and Management. 53 (2016) 53–63.

[59] G. Bansal, F. Zahedi, D. Gefen, The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decision Support Systems. 49 (2010) 138–150.

[60] H.-Y. Huang, Examining the beneficial effects of individual's self-disclosure on the social network site, Computers in Human Behavior 57 (2016) 122–132.

[61] I. Altman, D. Taylor, Social Penetration Theory, Holt, Rinehart &Winston, New York, 1973.

[62] N.B. Ellison, J. Vitak, R. Gray, C. Lampe, Cultivating social resources on social network sites: Facebook relationship maintenance beahviors and their role in social capital processes, Journal of Computer-Mediated Communication. 19 (2014) 855–870.

[63] P.B. Lowry, J. Cao, A. Everard, Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures, Journal of Management Information Systems. 27 (2011) 163–200.

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

[65] E. Karahanna, D.W. Straub, N.L. Chervany, Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs, MIS Quarterly. 23 (1999) 183–213.

[66] A.R. Montazemi, H. Qahri-Saremi, Factors affecting adoption of online banking: a meta-analytic structural equation modeling study, Information & Management. 52 (2015) 210–226.

[67] H. Sun, A longitudinal study of herd behavior in the adoption and continued use of technology, MIS Quarterly. 37 (2013) 1013–1041.

[68] J. Min, B. Kim, How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost, Journal of the Association for Information Science and Technology. 66 (2015) 839–857.

[69] S.W. Lin, Y.C. Liu, The effects of motivations, trust, and privacy concern in social networking, Service Business. 6 (2012) 411–424.

[70] M. Tsay-Vogel, J. Shanahan, N. Signorielli, Social media cultivating perceptions of privacy: a 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users, New Media & Society 20 (1) (2018) 141–161.

[71] J.D. Jackson, Y.Y. Mun, J.S. Park, An empirical test of three mediation models for the relationship between personal innovativeness and user acceptance of technology, Information & Management. 50 (2013) 154–161.

[72] R. Agarwal, J. Prasad, A conceptual and operational definition of personal innovativeness in the domain of information technology, Information Systems Research. 9 (1998) 204–215.

[73] P. Zhang, The affective response model: a theoretical framework of affective concepts and their relationships in the ICT context, MIS Quarterly. 37 (2013) 247–274.

[74] M.R. Lynn, Determination and quantification of content validity, Nursing Research 35 (1986) 382–386.

[75] R. Chen, J. Wang, T. Herath, H.R. Rao, An investigation of email processing from a risky decision making perspective, Decision Support Systems. 52 (2011) 73–81.

[76] G. Gobo, Sampling, representativeness and generalizability, Qualitative Research Practice. (2004) 435–456.

[77] J. Perro, Mobile Apps: What's A Good Retention Rate?, Localytics, http://info.localytics.com/blog/mobile-apps-whats-a-good-retention-rate, (2017).

[78] W. Chin, Commentary: issues and opinion on structural equation modeling, MIS Quarterly. 22 (1998) vii–xvi.

[79] J.F. Hair Jr, G.T.M. Hult, C. Ringle, M. Sarstedt, A primer on partial least squares Structural Equation Modeling (PLS-SEM), SAGE Publications, Incorporated, 2013.

[80] J.M. Becker, K. Klein, M. Wetzels, Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models, Long Range Planning. 45 (2012) 359–394.

[81] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1981).

[82] J.C. Nunnally, Psychometric Theory, 3rd ed., McGraw-Hill New York, The University of Michigan, 1967.

[83] J. Henseler, C.M. Ringle, R.R. Sinkovics, The use of partial lease squares path modeling in international marketing, Advances in International Marketing. 20 (2009) 277–319.

[84] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, The Journal of Applied Psychology. 88 (2003) 879–903.

[85] H. Liang, N. Saraf, Q. Hu, Y. Xue, Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management, MIS Quarterly. 31 (2007) 59–87.

[86] I. Junglas, N. Johnson, C. Spitzmüller, Personality traits and concern for privacy: an empirical study in the context of location-based services, European Journal of Information Systems. 17 (2008) 387–402.

[87] H. Xu, H.-H. Teo, B.C.Y. Tan, R. Agarwal, The role of push-pull technology in privacy calculus: the case of location-based services, Journal of Management Information Systems. 26 (2009) 135–174.

[88] C. Martins, T. Oliveira, A. Popovic, Understanding the internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application, International Journal of Information Management. 34 (2014) 1–13.

[89] J. Lu, J.E. Yao, C.-S. Yu, Personal innovativeness, social influences and adoption of wireless internet services via mobile technology, The Journal of Strategic Information Systems. 14 (2005) 245–268.

Mehrdad Koohikamali is an Assistant Professor of Computer Information Systems in the College of Business Administration, California State Polytechnic University, Pomona. Mehrdad received his Ph.D. in Information Systems at the University of North Texas. He holds an M.S. in Applied GIS from the University of North Texas and an M.S. in GIS from the University of Tehran. His research and professional interests include location intelligence for business, big data analytics, social media analytics, text mining, and information privacy. He is a member of the Association for Information Systems and the Decision Sciences Institute. His work appears in journals such as *Decision Support Systems*, *Computers in Human Behavior*, *Informing Science*, and *Lecture Notes in Business Information Processing*. Mehrdad has several years of working experience in the field of GIS, ranging from GIS consultant, analyst, and a programmer to GIS manager. He is an expert in different areas of GIS data collection, such as satellite images, lidar, ultra-cam images, Photogrammetry, and land surveying. His hands-on experience with open-source and enterprise mapping platforms and deep understanding of modern businesses makes him an ideal location analytics strategist and leader. As a leader in location analytics area with emphasis for businesses, he has recently developed two novel courses on location analytics for decsion making and global analysis of spatial business. Mehrdad has kept his industry ties and has helped to transform many smalls businesses with the power of location intelligence.

Aaron M. French is an Assistant Professor of Management Information Systems in the College of Business at the University of New Mexico. He received his PhD in Business Information Systems at Mississippi State University. He has received outstanding teacher of the year awards at Mississippi State University and Kyungpook National University. His research has been published in the *Journal of Information Technology*, *Behaviour & Information Technology*, *Journal of Computer Information Systems*, *Communications of the Association for Information Systems*, *Information & Management*, and *Information Technology and People*. His research interests include social networking, eCommerce, cross-cultural studies and technology acceptance.

Dan J. Kim is a Professor of Information Technology and Decision Sciences (ITDS) at University of North Texas (UNT). His research interests are in multidisciplinary areas such as information security (InfoSec) and privacy, information assurance, and trust in electronic commerce. His research work has been published or in forthcoming > 150 papers in refereed journals, peer-reviewed book chapters, and conference proceedings including *Information Systems Research, Journal of Management Information Systems, Journal of AIS, Communications of ACM, Communications of AIS, EJIS, DSS, International Journal of Human-Computer Interaction, Journal of Organizational and End User Computing, IEEE Transactions on Professional Communication, Electronic Market, IEEE IT Professional, Journal of Global Information Management, and International Journal of Mobile Communications, and so on.* He has been received several federal grants and awards including the National Science Foundation CyberCorps multi-year grant: SFS, National Security Agency grant, 2012 Emerald management Review Citations of Excellence Awards, 2010 Best Published Paper Award in ISR, an Emerald Literati Network 2009 - Outstanding Paper Award, the ICIS 2003 Best Paper-First Runner-up Award, and the AMCIS 2005 Best Research Paper Award at AMCIS 2005. He was ranked at 22nd worldwide in terms of research productivity from year 2008 to 2010 based on top three leading IS journals: ISR, MISQ and JMIS.