Understanding the Antecedents and Outcomes of Facebook Privacy Behaviors: An Integrated Model

Nancy K. Lankton, D. Harrison McKnight, and John F. Tripp

***Abstract*—Privacy in online social networking (OSN) is more complex than in traditional online environments, such as e-commerce. In addition to simply limiting self-disclosure, OSN users can also use privacy settings and manage their network size to ensure privacy. This complexity calls for an enhanced OSN privacy model that more completely explains privacy behaviors. Combining the privacy calculus model with part of the uses and gratifications approach, this paper proposes an OSN privacy model that depicts both antecedents (i.e., privacy concern, trusting beliefs, and personal interest) and outcomes (i.e., gratifications obtained) of perceived privacy and use behaviors. Using an Empanel survey sample collected from U.S. Facebook users, results show that privacy concern influences network size, trust influences privacy setting use and use frequency, and personal interest influences each privacy and use behavior. Findings also show that the privacy behaviors' influence on gratifications obtained is complex in nature. A three-way interaction influences enjoyment and habit gratifications, and a two-way interaction influences bonding social capital. This paper provides opportunities for future research regarding OSN privacy behaviors, and it discusses practical implications.**

***Index Terms*—Facebook, privacy, privacy behaviors, privacy calculus, uses and gratifications.**

I. Introduction

ONLINE social networking (OSN) has redefined the dynamics of privacy and information sharing. In the past, decisions regarding data sharing were generally based on whether a second party would keep one's information private [1]. For instance, one might share personal information like name and credit card number with an e-vendor in exchange for products or services with the understanding that the vendor would safeguard this personal information. Risks were real, but users had few options for controlling their privacy beyond choosing not to share the information.

By contrast, OSN privacy issues are more complex. Users may still control their personal information by choosing to limit what they disclose, but they also can take additional actions, such as using vendor-provided privacy control settings or managing who is in their friend network. Decisions about how to exercise control are critical given the vast amount of information users post on these sites. Risks exist when one exposes too much or the wrong types of information to the wrong people. These risks include potential abuses by online criminals, stalkers, bullies, and even friends [2]. While OSN research says users undergo a privacy calculus when deciding whether to disclose personal information [2], this literature has gaps in certain areas.

First, while users have multiple privacy behavior choices, most research models include only one OSN privacy behavior, usually self-disclosure (e.g., [3]). However, to protect their personal information, individuals can also use vendor-provided privacy settings, which are unique to OSN and can be used to limit access to certain audiences, such as friends of friends, all friends, or specific friends. Network size[1] is an important privacy behavior because of its effect on visibility. Even if individuals use privacy settings to restrict content access to friends only, they still must decide who and how many people to allow as OSN friends. Users may not explicitly manage their network's size. However, a small network is usually a homogeneous network (i.e., mostly friends) in which users find disclosure to be less privacy invasive. In contrast, a large network is typically a heterogeneous network (i.e., more types of people) in which users might struggle to determine the appropriateness of disclosure [5], [6]. Because users engage in various strategies to manage their privacy, research that examines only one privacy behavior may miss major aspects of OSN privacy complexity.

A second gap in information privacy research is the limited investigation of privacy behavior outcomes. Most studies do not examine privacy behaviors in a continued use setting to address how the behaviors affect beliefs, attitudes, and future OSN intentions. This could lead to inconclusive or erroneous conclusions about how effective the privacy behaviors are in keeping users gratified and involved in the site. Researchers show that privacy risks and concerns decrease usage continuance intentions [7], [8]. Yet how this happens is less clear. Users may react to privacy concerns by limiting disclosures (a privacy behavior—see Fig. 1), which may increase or decrease gratifying or favorable perceptions (e.g., usefulness, enjoyment) that in turn impact usage continuance intentions. Understanding the link between privacy risks and concerns, privacy behaviors, gratification perceptions, and usage continuance intentions can help clarify these

Manuscript received July 6, 2017; revised April 7, 2018 and August 25, 2018; accepted January 12, 2019. Date of publication February 11, 2019; date of current version July 16, 2020. Review of this manuscript was arranged by Department Editor T. Ravichandran. *(Corresponding author: Nancy K. Lankton.)*

N. K. Lankton is with the Division of Accountancy and Legal Environment, Marshall University, Huntington, WV 25755 USA (e-mail: lankton@marshall.edu).

D. H. McKnight is with the Department of Accounting and Information Systems, Michigan State University, East Lansing, MI 48824 USA (e-mail: mcknight@broad.msu.edu).

J. F. Tripp is with the Department of Management Information Systems, Baylor University, Waco, TX 76798 USA (e-mail: John_Tripp@baylor.edu).

Digital Object Identifier 10.1109/TEM.2019.2893541

[1]Ellison *et al.* [4] call this variable friending behavior, but measure it similar to how this paper measures it as the number of Facebook friends.

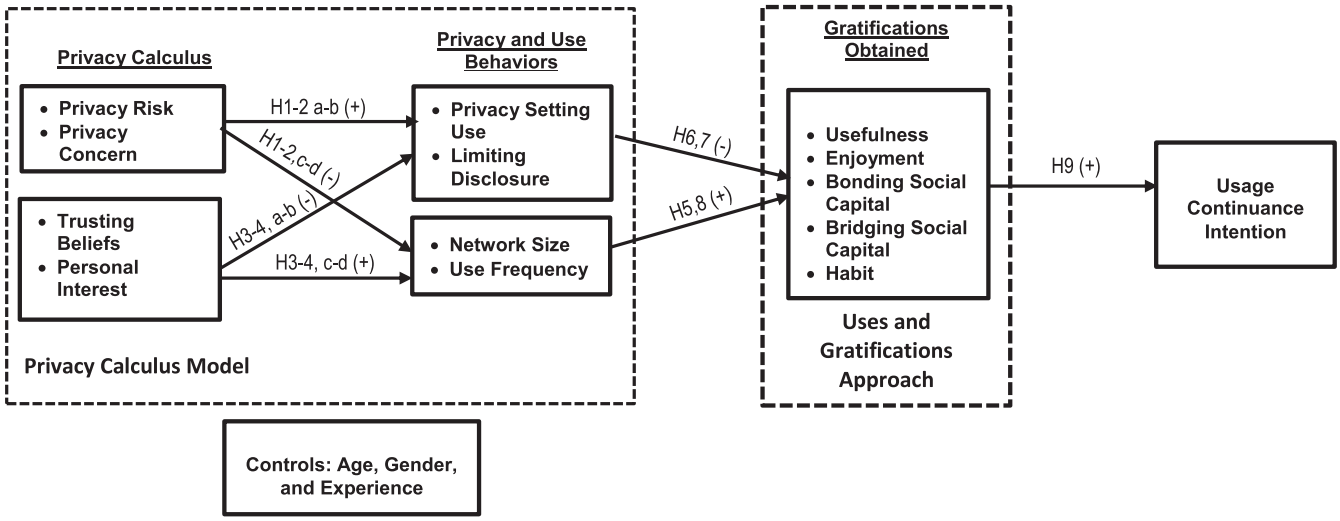


Fig. 1. Privacy behavior research model for a social network setting.

relationships, and can inform reports that users are posting less content on some social media sites[2] and that some site use has slowed or is even declining [9].

This paper's research objective is to examine the interplay of multiple privacy behaviors and their antecedents and outcomes in a theory-based and systematic manner. The research model (see Fig. 1) is developed by integrating the privacy calculus model with the uses and gratifications approach. Both have been used to understand OSN privacy and use, yet neither have provided a complete understanding of these behaviors. Combining privacy calculus with uses and gratifications helps predict both why users choose to behave in a more or less private way, and how these choices enhance their gratification perceptions and OSN usage continuance intention. The hypothesized model (see Fig. 1) is tested using survey data collected from a general U.S. population sample of Facebook users.

This paper contributes by serving as a baseline for future research. It sheds novel light on the complex issue of OSN privacy behaviors by using a more thorough set of concepts (all three privacy behaviors instead of one) and a new integrated theoretical framework (privacy calculus model and uses and gratifications approach). This research helps answer questions like "Does the OSN privacy calculus influence all privacy behaviors equally?" "Does keeping personal information more or less private lead to gratifications obtained?" and "Which privacy behaviors have which effects on gratifications obtained?" Such questions have either not yet been answered or have been examined in an *ad hoc* manner. Overall, the findings facilitate more informed research and practical decision making about OSN privacy.

II. Theory and Hypotheses Development

The theoretical model (see Fig. 1) uses both the privacy calculus model and part of the uses and gratifications approach. The privacy calculus model is based on expectancy theory, which broadly holds that individuals are motivated to maximize positive outcomes and minimize negative ones [7]. The uses and gratifications approach is a paradigm from the mass communication literature that examines the gratifications sought and the gratifications obtained from using media [10], [11]. Because this paper's focus is on explaining privacy behaviors, the model uses antecedents from the privacy calculus model, rather than gratifications sought, to explain user motivations for privacy and use behaviors. There is precedent for using expectancy theory models such as the privacy calculus model with the uses and gratifications approach. For example, in their uses and gratifications model, Rayburn and Palmgreen [12] contend that individual motivations are based on beliefs or expectancies that a media object possesses certain attributes and on an evaluation of those beliefs. The privacy calculus model is consistent with this notion because it captures the beliefs that are relevant to privacy and use behaviors (i.e., media use) and reflects the calculus or evaluation users undertake in determining whether to reveal their personal information.

A. Privacy Calculus Model

Dinev and Hart's privacy calculus model [7] contends that prior to disclosing information, individuals undergo a privacy calculus, weighing contrary beliefs that include risk, confidence, and enticement beliefs. Risk beliefs are perceived negative outcomes or the possibility of loss from disclosing, whereas confidence and enticement beliefs are beliefs that these risks can be mitigated [7]. Consistent with the privacy calculus model, the research model for this study includes both perceived privacy risks and privacy concerns to represent risk beliefs, trust to represent confidence beliefs, and personal interest to represent enticement beliefs [7] (see Fig. 1, left side).

The privacy calculus model has been a theoretical basis for research studying online disclosure decisions in various contexts (see Table I). This paper expands on this research in three ways. First, as depicted in Fig. 1, the research model includes all factors from the privacy calculus model [7]. Few studies

[2][Online]. Available: https://www.forbes.com/sites/paularmstrongtech/2017/02/14/facebook-users-posted-a-third-less-content-in-2016-than-in-2015/#2e101282776d.

TABLE I
SAMPLE PRIVACY CALCULUS STUDIES

	Technology	Risk beliefs	Confidence beliefs	Enticement beliefs	Intention	Perceived behavior
Anderson & Agarwal [13]	Digital health exchange	X	X		X	
Chen & Chen [14]	Online social network sites	X				X
Cheung *et al.* [2]	Facebook	X	X	X		X
Dienlin and Metzger [15]	Facebook	X		X		X
Dinev *et al.* [16]	e-Commerce	X	X			X
Dinev and Hart [7]	e-Commerce	X	X	X	X	
Hallam and Zanella [17]	Wearable device	X		X	X	X
James *et al.* [18]	Facebook			X		X
Jiang *et al.* [19]	Online chat rooms	X		X		X
Kehr *et al.* [20]	Behavioral driving app	X	X	X	X	
Keith *et al.* [21]	Location based service app	X		X		X
Keith *et al.* [22]	Location based service app	X		X	X	X
Kordzadeh *et al.* [23]	Virtual health clinic	X		X		
Kordzadeh and Warren [24]	Virtual health clinic	X		X	X	
Krasnova *et al.* [25]	Facebook	X		X		X
Krasnova *et al.* [26]	Online social networks	X	X	X		X
Krasnova *et al.* [3]	Facebook	X	X	X		X
Li *et al.* 2010 [27]	Fax service web site	X		X	X	
Li *et al.* 2016 [28]	Healthcare wearable devices			X	X	
Morosan and DeFranco [29]	Hotel app	X	X	X	X	
Pentina *et al.* [30]	Mobile apps	X		X	X	X
Raschke *et al.* [31]	Fuel tax mobile app	X		X	X	
Sun *et al.* [32]	Location based services	X		X	X	
Wang *et al.* [33]	Mobile social apps	X		X	X	X
Wang *et al.* [34]	Mobile apps	X		X	X	
Xu *et al.* 2009-10 [35]	Location-based services	X		X	X	
Xu *et al.* 2011 [36]	Location-based services	X		X	X	
Xu *et al.* [37]	Location-based services	X		X	X	
Xu *et al.* [38]	Social network sites	X		X	X	
Zhao *et al.* [39]	Location-based services	X		X	X	

include all three belief types, with the confidence beliefs (trust) omitted most often (see Table I). Second, this paper's research model includes three privacy behaviors: limiting disclosure, privacy setting use, and network size within a full nomological network. Similar to other privacy calculus studies [16], it also examines use frequency behavior, which means the frequency of performing specific activities on the OSN website (e.g., tagging or posting photos, or accepting and declining friend requests). How often an individual performs these activities can depend on their privacy calculus and can serve to keep their information more or less private. Finally, none of the privacy calculus studies examine outcomes of the privacy and use behaviors. Based on these observations and gaps in the literature, the model shown in Fig. 1 includes all three calculus belief types, their relationships with perceived privacy and use behaviors, and the gratifications obtained from engaging in the privacy and use behaviors.

1) Privacy Risk Beliefs: Perceived Privacy Risks and Privacy Concerns: Perceived privacy risks and perceived privacy concerns are similar but distinct constructs. Both are considered risk beliefs, but perceived privacy risks assess what could happen to general OSN users' personal information, whereas perceived privacy concerns are an assessment of what could happen to one's own personal information [7]. Individuals may perceive risks related to the use, sharing, and misuse of information during online social activities [40]. For example, information posted on OSN websites can be collected and used by the provider, or by third parties such as advertising, human resources, or state agencies [3]. People may also perceive threats such as secret sharing, bullying, or profile viewing by third parties (e.g., employers) [26]. OSN risks may be exacerbated by increased media coverage of privacy abuse cases [3].[3]

The first set of hypotheses propose that perceived privacy risks and privacy concerns influence privacy and use behaviors (see Fig. 1). A recent review of the e-commerce literature shows that privacy concerns and risks have significant impacts on individuals' attitudes toward information practices, behavioral intention to provide information or protect privacy, and use behaviors [41]. Likewise, in an OSN context, individuals will engage in privacy behaviors because of perceived privacy risks and concerns. Privacy-concerned Facebook users tend to delete or edit something they previously posted, set their profile to private (friends only), and delete people from their network or friends' list [42]. Perceived privacy risks and concerns lead OSN

[3]Including about Facebook (e.g., [Online]. Available: https://www.cbsnews.com/news/facebook-cambridge-analytica-scandal-federal-investigation-data-scandal-mark-zuckerberg/).

users to limit their profile visibility, maintain smaller network size [14], and limit their self-disclosure [15], [25].

Perceived privacy risks and privacy concerns may also influence use frequency. Rather than controlling information disclosure, users may address risks by using the OSN site less. Supporting research finds that OSN users who are concerned about their information privacy use a site less [43] and are less likely to use it for participating in marketing activities [44].

H1: Perceived OSN privacy risks will positively influence (a) privacy setting use and (b) limiting disclosure, and they will negatively influence (c) network size and (d) use frequency.[4]

H2: Perceived OSN privacy concerns will positively influence (a) privacy setting use and (b) limiting disclosure, and they will negatively influence (c) network size and (d) use frequency.

2) Confidence Beliefs: Trusting Beliefs: Trusting beliefs in the OSN provider may also influence privacy and use behaviors. Trusting beliefs means a user's belief that the OSN provider has three desirable attributes: integrity, competence, and benevolence [45]. Trust is considered a confidence belief in the privacy calculus model. Knowing that the OSN provider has these positive traits gives users assurance that it will keep their personal information safe. Perceiving that the website has the positive attributes of integrity, competence, and benevolence is advantageous to the trustor in overcoming the risks of disclosing personal information.

Trusting beliefs in the provider should influence privacy and use behaviors because users who trust will not feel the need to control their information as much because they believe the provider will protect it. Prior research finds trusting beliefs facilitate online information sharing [45] and increase self-disclosure [3]. Similarly, users with higher trust are less protective, so they should disclose more, be less likely to use privacy settings to restrict access, and more likely to maintain larger friend networks.

Furthermore, because trusting beliefs often offset privacy risks, it can make one more apt to use the OSN site more often. Researchers find trust in the provider positively influences LinkedIn and Facebook usage intentions [41], and trust in Facebook positively influences user participation in OSN marketing activities [44].

H3(a)–(d): Trusting beliefs will negatively influence (a) privacy setting use and (b) limiting disclosure, and will positively influence (c) network size and (d) use frequency.

3) Enticement Beliefs: Personal Interest: Consistent with previous research on the privacy calculus model (e.g., [7], [36], [37]), personal interest can mitigate risks when undergoing a privacy calculus. Personal interest is defined as perceptions of cognitive attraction that entice one to relinquish some privacy to transact online [7], [46]. Dinev and Hart [7] claim that Internet personal interest is relevant to their study because "the Internet provides access to an incredibly wide range of information, goods, and services that might not otherwise be available or conveniently available to users. The Internet is an environment in which a wide range of subjects and products can be found to match a particular user's interest" (p. 68). Similarly, OSN websites like Facebook can provide many services making personal interest relevant to this paper. Personal interest means the overall attraction or desirability of making information more public overrides the perceived risks of using the OSN website [7].

Prior research supports personal interest as a privacy behavior antecedent. For example, personal Internet interest leads to increased willingness to provide personal information to interact on the Internet [7], to decreased security practices in a networked environment [46], and to increased self-disclosure in mobile coupon services [36], [37]. Personal interest can also increase OSN use frequency because it reflects a desire to meet personal needs using the OSN.

H4(a)–(d): Personal interest will negatively influence (a) privacy setting use and (b) limiting disclosure, and will positively influence (c) network size and (d) use frequency.

B. Gratifications Obtained From Privacy and Use Behaviors

The research model extends the privacy calculus model by depicting gratifications obtained from privacy and use behaviors. The gratifications are based on research using the uses and gratifications approach, which is a media use paradigm from mass communication research that dates back to the 1940s [10]. The main purpose of this approach is to explain why people choose one specific communication medium over another [47]. It contends that media users are goal directed in their usage, seeking out specific gratifications to fulfill their needs. Media choice depends on gratifying needs [48], [49]. In uses and gratifications research, a key distinction is made between gratifications sought and gratifications obtained [11]. Gratifications sought (also often referred to as "needs" or "motives") refer to those gratifications that audience members expect to obtain from a medium before they have actually come into contact with it [50]. In contrast, gratifications obtained refer to those gratifications that audience members actually experience through the use of a particular medium. OSN uses and gratifications research examines one or both of these gratifications (e.g., [2]—gratifications sought; [50]—both; [52]—gratifications obtained). While the Fig. 1 research model depicts gratifications obtained as the outcomes of these behaviors, it depicts privacy calculus as motivating privacy and use behaviors rather than gratifications sought because of this paper's focus is on privacy.

Much uses and gratifications research has investigated media use like radio, television, and the Internet [10]. Researchers have recently applied the approach to identify gratifications of online social media use, which fall into four main categories:

1) instrumental (task-oriented, extrinsic);
2) entertainment (having fun, being entertained);
3) social (maintaining and building relationships);
4) habitual (ritualized or routine) [48], [51], [53], [54].

[4]Although not hypothesized in this paper, the privacy behavior and use frequency variables could be related. Therefore, the Fig. 1 research model was tested with privacy setting use influencing limiting disclosure, network size, and frequency of use. Adding these relationships does not affect the significance of the relationships between the independent variables (perceived privacy risks, privacy concerns, trust, and personal interest) and the privacy and use behaviors. Nor does it affect the significance of the relationship between the privacy behavior and use frequency variables on their dependent variables (usefulness, enjoyment, bridging social capital, bonding social capital, and habit).

In this paper, these four gratifications obtained are represented by perceived usefulness (utility or effectiveness of OSN use [55]), enjoyment (pleasure from OSN use [55]), bonding and bridging social capital (resources accrued from relationships with individuals or groups resulting from OSN use [4]), and habit (OSN use is automatic [56]).

1) Use Frequency Effects: Based on the uses and gratifications approach, OSN use frequency should positively influence these gratifications obtained because they, by definition, fulfill OSN use. Researchers have verified through interviews and surveys that use frequency produces these gratifications. For example, Whiting and Williams [54] found this as they performed in-depth interviews with 25 people, asking them why they use social media and what they enjoy about it. Other researchers have empirically shown that the gratifications are associated with OSN use [48], [51].

H5(a)–(e): Use frequency will positively influence (a) usefulness, (b) enjoyment, (c) bonding social capital, (d) bridging social capital, and (e) habit.

The three privacy management behaviors should also influence gratifications obtained because they are congruous with the media use concept. Media use constitutes exposure or attentiveness to the media, and is a way that users can interact with, or use the OSN website. Both use and privacy behaviors expose one and make one attentive to the site. In prior research, OSN privacy behaviors have been associated with gratifications [57].

2) Limiting Disclosure Effects: The next set of hypotheses that predicts limiting disclosure will negatively influence OSN gratifications obtained. OSN use has gained popularity, attracting a great number of people who want to share personal information, such as names, photographs, personal interests, and contact information, as well as their current feelings and opinions [41]. Many join a social network website to disclose and share personal information to reap its benefits. Posting more personal information on one's profile will lead to more usefulness, enjoyment, social capital, and habit because disclosing can increase positive feedback and attention from others [58]. Interacting more can make the site seem more productive and efficient for social networking, and it can make it seem more fun and enjoyable. This makes site use more useful and enjoyable. Likewise, limiting disclosure would make the site seem less useful and enjoyable. Prior OSN research supports this finding [2], [3], [24].

Limiting disclosure will also negatively impact bonding and bridging social capital [58]. A key factor in building social capital is self-disclosure, especially as relationships begin [58]. Information gathered from a user's profile will establish common ground and facilitate communication and coordination processes [4]. Researchers find increased disclosure practices for people seeking new relationships [59], as well as those maintaining old ones [60]. Limiting disclosure would have a negative effect on these activities.

Limiting disclosure should also negatively affect habit because people who are not posting are not using the site. More frequent behavioral performance leads to habit [61]. Culnan and Armstrong [1] argue that past experiences allow users to become aware of the benefits and trust the process of sharing information, such that further disclosure becomes "compatible with their existing values and past experiences" (p. 109). This suggests that more disclosure leads to stronger habit and limiting disclosure leads to lower habit.

H6(a)–(d): Limiting disclosure will negatively influence (a) usefulness, (b) enjoyment, (c) bonding capital, (d) bridging capital, and (e) habit.

3) Privacy Setting Use Effects: The research model predicts that higher privacy setting use will negatively impact gratifications obtained. This makes sense because having restrictive privacy settings reduces the amount of personal information that others can see, and, as just discussed, can lead to lower gratifications obtained. Researchers find higher privacy setting use (i.e., more restrictive) is negatively associated with the perceived benefits of location-based services [18]. Also, because it requires attention and in some cases may be cognitively unmanageable [62], [63], privacy setting use may be seen as a burden leading to fewer gratifications obtained.

Previous research supports this prediction. For example, more restrictive privacy setting use works against one major reason Facebook is useful—to share personal information with as many friends as possible [56]. The higher the level of privacy setting use, the lower the usefulness of Facebook will be for social networking. By contrast, information management and social goals are associated with having less restrictive privacy settings for basic profile characteristics (e.g., ages, birthdays, schools, and images) [18]. Releasing this type of information attracts more friends with whom to interact [18], which could increase bonding and bridging social capital, and enjoyment and pleasure in using the site.

Having more restrictive privacy settings may also negatively affect habit. Habit negatively correlates with systematic privacy controls like using privacy settings, blocking unwanted contacts, and restricting the visibility of posts [57]. These actions take attention and intentionality, whereas a lack of attention, awareness, and intentionality are all dimensions of habit [65]. In this way, using restrictive privacy controls should decrease habit.

H7(a)–(e): Privacy setting use will negatively influence (a) usefulness, (b) enjoyment, (c) bonding capital, (d) bridging capital, and (e) habit.

4) Network Size Effects: Network size on the other hand should positively influence gratifications obtained. Researchers find the more friends that join an instant messaging network, the more users can develop their social circles, thereby increasing their utility [66]. Further, the more people including their peers who join an OSN site, the more users perceive usefulness and enjoyment [67]. Participants who reported the most Facebook friends also reported greater perceived bonding and bridging social capital than those reporting fewer [60]. All else equal, as individuals expand their network, they are better able to meet and stay in contact with friends. Finally, as network size increases, use of the OSN website will increase, making its use more routinized and habitual. A positive relationship between network

size and habit is suggested by findings in which habit correlates positively with more frequent site use by friends [56]. More friends should produce more habitual use.

H8(a)–(e): Network size will positively influence (a) usefulness, (b) enjoyment, (c) bonding social capital, (d) bridging social capital, and (e) habit.

The final set of hypotheses predict that these gratifications obtained will influence usage continuance intention. Usage continuance intention represents the decision to perform the use behavior, but is not the behavior itself. It focuses on users' projected future use of the OSN website in general, rather than on their current use level of specific features that is represented by the use frequency variable. This section does not argue separately for each gratification obtained (usefulness, enjoyment, bonding and bridging social capital, and habit) because they have been shown to influence continuance intentions in classic information system studies [61], [67], and in OSN studies [56], [66], [68].

H9a-e: (a) Usefulness, (b) enjoyment, (c) bonding social capital, (d) bridging social capital, and (e) habit will positively influence usage continuance intentions.

III. Methodology

This paper used online questionnaire data to test the research model. Facebook is the focal OSN website for the study due to its prominence. The dataset was collected in spring 2014, using Empanel, a data collection company that specializes in Internet-based survey panel recruitment. The company provided 595 potential respondents who were general, U.S. population, Internet users.[5] Initial screening identified 544 Facebook users who were at least aged 18. About 239 responses had data quality issues (170 responses for not passing quality assurance questions,[6] and 69 responses for not spending at least 12 min on the survey or for responding with all the same answers) and were eliminated. This resulted in 305 usable responses for a usable response rate of 56%. The average age of the sample was 44 years, with more females than males (64% versus 36%). This is generally representative of Facebook users because in 2014, the age group 30–49 was the second largest age group, and more women than men used Facebook.[7]

The questionnaire is shown in the Appendix. Most scales were adapted from previous research: privacy risk, privacy concern, and personal interest [7], habit [56], [61], continuance intention [56], usefulness and enjoyment [55], [69], trusting beliefs [45], and bonding and bridging social capital [70]. All items were adapted to relate to the OSN setting.

The authors created the items for the privacy behaviors and use frequency. Privacy setting use consisted of a list of information and asked respondents who they allow to see those types of information, from everyone on Facebook to no one [63]. These items were created based on the Facebook settings at the time of the study. Because of this construct's formative nature (an individual might use privacy settings to control who can see their contact information, but not their work information), yet the high correlations among some items, items were averaged for the analysis. This makes theoretical sense because a higher (lower) average indicates using privacy settings to obtain more (less) privacy. The limiting disclosure items from Krasnova *et al*. [24] served as a guide. For example, Krasnova's items refer to having a detailed and comprehensive profile. This is like this paper's items about limiting content and personal or sensitive information. For network size, respondents reported approximately how many total Facebook friends they had (1 = 1–50; 7 = greater than 1000). Finally, the formative usage frequency items represented actual tasks users could perform in Facebook (e.g., tag or post photos, play games, accept or decline friend requests). Other measures were age, gender (1 = male, 2 = female), and experience (use duration) as control variables. Table II presents variable means and standard deviations.

Most items (excluding limiting disclosure) were pilot tested in an undergraduate information systems course ($n = 391$). The items loaded well on their intended constructs, and the constructs demonstrated good reliability. To reflect Facebook functionality added after the pilot, items 8 and 9 were added to the privacy setting use construct.

Trusting beliefs were treated as a reflective second-order factor with integrity, competence, and benevolence as first-order factors. This analysis followed the guidelines set forth by Hardin *et al*. [71], which says to use reflective factors if:

1) the first-order factors are expected to correlate;
2) they reflect the psychological and theoretical construct;
3) the researchers' interest is in knowing how the second-order factor affects other variables, not in explaining its variance. This practice is consistent with prior trust research [56].

IV. Data Analysis

The data analysis used SmartPLS 3 [72]. First, the measurement model was analyzed for convergent validity. Results showed that the PLS factor loadings for each variable were above 0.70 except for bonding social capital items 3 and 9 that loaded at 0.54 and 0.41, respectively, and bridging social capital item 4 that loaded at 0.66. The two bonding social capital items that were less than 0.60 were deleted and the bridging social capital item was retained as it was closer to the 0.70 cutoff and the construct otherwise demonstrated good convergent validity. The Cronbach alpha's (CA), D. G. rho's (DG), composite reliabilities (CR), and average variances extracted (AVE) were all greater than the minimum standard amounts (CA—0.70 [73]; DG—0.70 [74]; CR—0.80; and AVE—0.50 [75]) (see Table II). These findings all support convergent validity.

Next discriminant validity was analyzed by comparing the variable intercorrelations with the square roots of the AVEs

[5]Empanel provided users who live in the United States. All Empanel subjects must be Internet users.

[6]These questions were interspersed throughout the survey, and they asked the respondents to answer a particular question (unrelated to the survey) in a particular way.

[7][Online]. Available: http://www.pewinternet.org/2015/01/09/demographics-of-key-social-networking-platforms-2/

TABLE II
CONSTRUCT MEAN, STANDARD DEVIATION (SD), CRONBACH ALPHA (CA), D. G. RHO (DG), COMPOSITE RELIABILITY (CR), AND AVERAGE VARIANCE EXTRACTED (AVE)

Construct	Mean	SD	CA	DG	CR	AVE
Privacy Risk	5.12	1.36	.89	.93	.93	.76
Privacy Concern	5.08	1.50	.93	.98	.95	.83
Trusting Beliefs: Integrity	4.48	1.63	.97	.97	.98	.94
Trusting Beliefs: Competence	5.68	1.30	.94	.94	.96	.90
Trusting Beliefs: Benevolence	4.10	1.71	.92	.92	.95	.86
Personal Interest	3.41	1.62	.87	.88	.92	.79
Limiting Disclosure	6.03	1.09	.81	.84	.88	.71
Privacy Setting Use	2.68	0.99	na	na	na	na
Network Size	3.60	2.13	na	na	na	na
Use Frequency	4.04	1.32	na	na	na	na
Usefulness	4.72	1.50	.95	.95	.96	.87
Enjoyment	5.36	1.39	.97	.97	.98	.94
Bonding Capital	4.14	1.43	.91	.92	.93	.63
Bridging Capital	4.59	1.37	.95	.95	.96	.68
Habit	4.95	1.71	.94	.94	.96	.81
Continuance Intention	5.89	1.27	.99	.99	.99	.97
Age	43.86	12.84	na	na	na	na
Gender	64% F, 36% M	na	na	na	na	na
Experience	5.73	1.55	na	na	na	na

TABLE III
CONSTRUCT CORRELATIONS (SQUARE ROOT OF AVERAGE VARIANCE EXTRACTED ON DIAGONAL)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1. Privacy Risk	.87																		
2. Privacy Concern	.65	.91																	
3. Trusting Belief: Integrity	-.37	-.28	.97																
4. Trusting Belief: Competence	-.17	-.15	.59	.95															
5. Trusting Belief: Benevolence	-.35	-.19	.81	.57	.92														
6. Personal Interest	-.19	-.11	.39	.25	.41	.89													
7. Use Frequency	-.14	-.03	.36	.30	.44	.50	1.00												
8. Limiting Disclosure	.21	.20	-.22	-.04	-.21	-.30	-.17	.85											
9. Privacy Setting Use	.20	.22	-.28	-.22	-.27	-.37	-.28	.20	1.00										
10. Network Size	-.08	-.18	.06	.07	.02	.21	.35	-.17	-.25	1.00									
11. Perceived Usefulness	-.16	-.11	.45	.49	.51	.50	.56	-.15	-.25	.24	.93								
12. Enjoyment	-.25	-.21	.48	.52	.52	.41	.53	-.11	-.29	.20	.66	.97							
13. Bonding Social Capital	-.06	-.04	.27	.32	.28	.33	.50	-.14	-.32	.24	.44	.44	.79						
14. Bridging Social Capital	-.09	-.07	.32	.38	.37	.50	.61	-.13	-.35	.31	.64	.59	.59	.83					
15. Habit	-.24	-.22	.41	.41	.46	.48	.62	-.14	-.27	.25	.63	.74	.43	.60	.90				
16. Continuance Intention	-.30	-.29	.43	.47	.40	.31	.42	-.06	-.23	.18	.54	.72	.36	.44	.63	.99			
17. Age	.01	.03	.00	.09	.03	.10	.25	-.13	-.12	.33	.16	.01	.18	.13	.10	-.02	1.00		
18. Gender	-.07	.03	-.01	-.04	-.01	.05	.11	.07	-.01	.10	.02	.06	-.03	.09	.17	.06	.16	1.00	
19. Experience	-.03	-.14	.00	.10	-.05	.09	.15	-.03	-.25	.37	.10	.12	.17	.08	.18	.15	.26	.01	1.00

(see Table III). Each correlation is lower than the square root of the AVEs of the two correlated variables, which supports discriminant validity [75]. Also, all PLS cross loadings are lower than each item loading. Multicollinearity is also not a problem as the highest variance inflation factor is 2.68, which is well below the suggested cutoff of 5.00 [76].

Common method variance was assessed by using Harman's single-factor test [77], which found that the first factor did not explain a majority of the variance explained (only 34% of the 85% explained). Based on this, common method variance was not a major problem. Also, several steps may have prevented common method bias. First, several open-ended questions (e.g., one about risk of using Facebook) were mixed among the quantitative questions to give respondents an occasional mental break. Second, different questions had different scale headers such as Strongly Disagree–Strongly Agree, Not at all Concerned–Very Concerned, and Not True at All–Absolutely True (see Appendix). Third, items were grouped by construct so as not to disrupt the instrument's logical flow [77].

The appropriateness of the reflective second-order trusting belief factor was also assessed. First, the first-order factors were significantly intercorrelated ($p < 0.05$), with moderate to high values 0.57 to 0.81 (see Table III). Second, each first-order factor loaded significantly on the second-order factor (0.80–0.92, $p < 0.001$). Third, the second-order construct indicators—CA (0.85), DG (0.86), CR (0.91), and AVE (0.77)—are all within suggested guidelines. This shows using reflective second-order trusting belief factors is appropriate.

Table IV presents the structural model results. *H1(a)–(d)* are not supported because privacy risk did not significantly affect any of the privacy behaviors or use frequency. Privacy concerns only significantly influences network size. This supports *H2(c)*, but not *H2(a)*, *(b)*, and *(d)*. In support of *H3(a)* and *(d)*, trusting beliefs influences both privacy setting use (negatively) and use frequency (positively). Trusting beliefs do not significantly influence limiting disclosure or network size, so *H3(b)* and *(c)* are not supported. Personal interest significantly influences all its predicted outcomes, supporting *H4(a)–(d)*. Use frequency influences all five gratifications obtained as hypothesized, supporting *H5(a)–(e)*. However, there was no support for *H6(a)–(e)* as limiting disclosure does not significantly affect any gratification. Privacy setting use significantly influences enjoyment [see *H7(b)*], bonding social capital [see *H7(c)*], and bridging social capital [see *H7(d)*]. It does not influence usefulness or habit [see *H7(a)* and *(e)*]. Network size only significantly influences bridging capital, supporting *H8(d)*, and not supporting *H8(a)–(c)*, and *(e)*. Finally, there was support for *H9(b)* and *(e)* because enjoyment and habit significantly influence contin-

TABLE IV
PLS STRUCTURAL MODEL RESULTS

Hypothesis	Path coefficient	Hypothesis	Path coefficient
H1 Privacy Risk →		H7: Privacy Setting Use →	
(a) Limiting Disclosure	.09ns	(a) Usefulness	-.09ns
(b) Privacy Setting Use	.00ns	(b) Enjoyment	-.15**
(c) Network Size	.07ns	(c) Bonding Social Capital	-.17***
(d) Use Frequency	-.03ns	(d) Bridging Social Capital	-.18***
H2 Privacy Concern →		(e) Habit	-.08ns
(a) Limiting Disclosure	.12ns	H8: Network Size →	
(b) Privacy Setting Use	.14ns	(a) Usefulness	.03ns
(c) Network Size	-.19**	(b) Enjoyment	-.01ns
(d) Use Frequency	.10ns	(c) Bonding Social Capital	.02ns
H3 Trusting Beliefs →		(d) Bridging Social Capital	.12*
(a) Limiting Disclosure	-.01ns	(e) Habit	.04ns
(b) Privacy Setting Use	-.14*	H9: → Continuance Intention	
(c) Network Size	-.04ns	(a) Usefulness	.11ns
(d) Use Frequency	.28***	(b) Enjoyment	.52***
H4: Personal Interest →		(c) Bonding Social Capital	.04ns
(a) Limiting Disclosure	-.27***	(d) Bridging Social Capital	-.07ns
(b) Privacy Setting Use	-.28***	(e) Habit	.20**
(c) Network Size	.16**		
(d) Use Frequency	.37***	CONTROL VARIABLE EFFECTS[1]	
H5: Use Frequency →		Age → Limiting Disclosure	-.14*
Usefulness	.51***	Age → Network Size	24***
Enjoyment	.49***	Age → Use Frequency	.17***
Bonding Social Capital	.43***	Age → Habit	-.12**
Bridging Social Capital	.54***	Gender → Habit	.13**
Habit	.58***	Length Experience → Privacy Setting Use	-.12*
H6: Limiting Disclosure →		Length Experience → Network Size	.27***
Usefulness	-.04ns		
Enjoyment	.00ns		
Bonding Social Capital	-.01ns		
Bridging Social Capital	.00ns		
Habit	-.04ns		
VARIANCE EXPLAINED			
Limiting Disclosure	13%	Enjoyment	29%
Privacy Setting Use	19%	Bonding Social Capital	28%
Network Size	22%	Bridging Social Capital	41%
Use Frequency	31%	Habit	41%
Usefulness	31%	Continuance Intention	54%

*p<.05, **p<.01, ***p<.001; [1] Only significant control variable effects are shown.

uance intention, but usefulness, bonding, and bridging capital do not.

To supplement these findings, five supplemental analyses were performed. First, because some researchers examine both trust in the OSN provider and trust in other members [2], trust in Facebook friends and trust in Facebook strangers were added to the left side of the model. These variables were measured as second-order factors similar to the trust in Facebook beliefs factor and passed all validity tests. Findings show that trust in Facebook friends has a significant positive effect on limiting disclosure ($\beta = 0.14$, $p < 0.05$), and usage frequency ($\beta = 0.14$, $p < 0.05$). This means that the more users trust Facebook friends, the more they limit disclosure and the more frequently they use Facebook. Also, trust in Facebook strangers has a significant positive effect on privacy setting use ($\beta = 0.13$, $p < 0.05$), meaning the more users trust strangers the more they use privacy settings to limit access. No other previously reported results changed.

Second, because there is a chance that trust could moderate the effects of privacy concern and privacy risks on the privacy and use behaviors, the trust × privacy concern and trust × privacy risks interactions were added to the model. Findings show a significant positive interaction effect for the relationship from trust × privacy concern to use frequency ($\beta = 0.23$, $p < 0.01$). All previously reported significance levels remain the same. This result shows that trust becomes even more important as privacy concerns increase. Trust allows users to feel more comfortable about using the OSN website despite their concerns.

Third, the model was revised to include two-way and three-way interactions among the three privacy behaviors to account for a possible interrelationship among the privacy behaviors in which users may employ more than one behavior to achieve

TABLE V
MEDIATION TEST

	Indirect effects	Direct effects	Total effects
Use frequency	.41***	-.01ns	.40***
Limiting Disclosure	-.01ns	.03ns	.01ns
Privacy setting use	-.10*	-.01ns	-.11*
Network Size	.01ns	.01ns	.02ns

their privacy goals [62]. Results show that the two-way interaction between privacy setting use and network size significantly influences bonding social capital ($\beta = 0.10$, $p < 0.05$). Also, the three-way interaction between limiting disclosure, privacy setting use, and network size significantly influences enjoyment ($\beta = 0.12$, $p < 0.05$) and habit ($\beta = 0.10$, $p < 0.05$). All other previously reported results are unchanged.

Fourth, a mediation analysis was run to test whether the gratifications obtained fully or partially mediate the relationship between the privacy and use frequency behaviors and usage continuance intentions. Instead of the traditional Baron and Kenny [77] method, a more statistically advanced approach can be used for testing mediation in more complex models with multiple mediators as in this paper [79]. Using this approach, the authors tested a model that includes the total indirect effects of the privacy behavior and use frequency constructs on usage continuance intentions via all the gratifications obtained, controlling for the direct effect of the privacy and use behavior constructs on continuance intention. Mediation exists if the total indirect effects are significant via a bootstrapping analysis. Furthermore, if the direct effects are significant, then partial mediation exists, and if they are not significant, full mediation exists. Findings show that use frequency and privacy setting use have significant indirect effects on continuance intention (see Table V). However, neither of their direct effects on usage continuance intentions are significant, meaning the gratifications obtained fully mediate the relationships.

Finally, two revised models were analyzed. One that includes usefulness and enjoyment as antecedents of the privacy and use behaviors, and another that includes all the gratifications obtained as predicting the privacy and use behaviors (i.e., treating them as gratifications sought). To be consistent with the privacy calculus model by Dinev and Hart [7] and only include the constructs they did, these models were not hypothesized. Also, in this paper, usefulness and enjoyment are measured as gratifications obtained by being worded to represent beliefs after the use of the media/technology (e.g., [12]). This wording is consistent with the meaning of gratifications obtained, which refers to gratifications that users actually experience through the use of a particular medium, rather than gratifications sought [10]. The revised models result in a lower variance explained for continuance intention (41% and 20% versus 54%), and an almost equal higher variance explained for use frequency (45% and 54% versus 31%). However, in both revised models, the gratifications obtained have lower effects on use frequency than use frequency had on the gratifications obtained in the hypothesized model. This suggests that the hypothesized model is better fitting. In the revised model with all the gratifications predicting the privacy and use behaviors, privacy setting use has a negative effect on continuance intention ($\beta = -0.11, p < 0.05$). This negative relationship is better explained by the hypothesized model because it details how privacy setting use negatively influences continuance intention (by decreasing enjoyment, bonding social capital, and bridging social capital). In summary, these revised models do not follow theory as well as the original hypothesized model, nor do they coincide with the operationalization of the variables (usefulness and enjoyment in particular). Finally, the revised models are not good overall at predicting the variables and explaining variance.

V. DISCUSSION, IMPLICATIONS, AND LIMITATIONS

OSN users can protect their personal information by limiting disclosure, using more restrictive privacy settings and managing their network size. Yet no work to the authors' knowledge has examined all three behaviors simultaneously in a continued use context. This paper investigates a full model of OSN privacy behavior antecedents and consequents. It integrates the privacy calculus model with the uses and gratifications approach to develop hypotheses about OSN privacy behaviors and use frequency. In this way, the research model provides a more comprehensive view of privacy behaviors than can be developed with either theory alone. Overall, the model explains 54% in usage continuance intentions, which is more than other OSN continued use studies [56]. The model contributes to the information privacy and OSN literature in several ways.

A. Contribution 1: A Clear Focus on All Three OSN Privacy Behaviors

This paper puts privacy behaviors on center stage instead of privacy concern. It contributes by examining three OSN privacy behaviors and their nomological network. Decomposing a model's core constructs into context-specific factors contributes to theory development [80]. In this paper, this was done by decomposing the privacy behavior concept into the three privacy behaviors most dominant in OSN privacy behavior research: privacy setting use, limiting disclosure, and network size. This adds to the current OSN literature because many papers examine only one privacy behavior such as limiting disclosure [25] or privacy setting use [56], [63]. Revealing personal information in an OSN context involves not only posting information to one's profile, but also using less restrictive privacy settings and accepting more users as friends. Findings show that users' privacy calculus varies by behavior, and that each behavior has different consequents. These differences could not be understood if only one behavior was examined or if a more general concept representing self-disclosure/information revelation was used. Examining the three behaviors individually provides a

more nuanced, yet comprehensive picture of OSN information revelation in general.

Focusing on the individual privacy behaviors is also important because users differ in how much they use each behavior. In this paper, respondents tend to limit disclosure (mean of 6.03/7.00), use privacy settings to be more restrictive (i.e., the average is close to the friends only setting), and have a network size of approximately 151–250 users. As one's friend list increases, the less well one knows them, making one's personal information increasingly less private. It is unlikely that respondents know all their friends well and because of this they are using a strategy of keeping their information private through less disclosure. This is called the lowest common denominator strategy, in which individuals, to deal with large friend lists, assess how their identity can be portrayed as acceptable to the lowest common denominator of content viewers [62]. They post only benign information that will not harm their reputation and/or be offensive to this group [62]. However, unlike the lowest common denominator strategy, the average user in this paper has an even more private strategy because they also use privacy settings. This constitutes a different approach to privacy management.

B. Contribution 2: Testing the Combined Antecedents to Three OSN Privacy Behaviors

This paper also contributes by being the first OSN study to examine the combined effect of risk beliefs (perceived privacy risk and privacy concerns), confidence beliefs (trust), and enticement beliefs (personal interest) on the three privacy behaviors and use frequency. Personal interest was by far the most influential. Personal interest had a significantly negative influence on limiting disclosure and privacy setting use and a positive influence on network size and use frequency. This means that individuals who believe their personal interests in using Facebook outweigh their concerns have a more public approach to information sharing. This helps explain the privacy paradox that individuals concerned about privacy risks still disclose information. This supports the premise behind the privacy calculus model. It also adds to the literature because while others study enticement beliefs' impact on using OSNs, few researchers have examined enticement beliefs' impact on all three privacy behaviors. Further, the enticement items measure the calculus people undergo. Very little privacy calculus research studies enticement beliefs in this manner (for an exception, see Xu *et al*.'s [35], [36] perceived value construct). This adds a key finding to the literature.

Findings also show that trust in Facebook leads to lower privacy setting use. Those who trust have confidence that Facebook will keep their information safe. While trust does not influence limiting disclosure as in other privacy calculus studies (e.g., [7]), this could be because these studies did not include all competing antecedents as this paper does. The results suggest that while trust does not influence a user to post more/less information, or to have more/fewer friends, it does engender less need to control access to the information. Trust and control are generally believed to be opposite forces because trust allows people to feel psychologically that they can control a situation [81]. Trust also has a significant impact on use frequency, meaning that individuals will use an honest, caring, and competent OSN website more often.

Finally, privacy risk and privacy concern have very little influence on the privacy behaviors or use frequency, with the only hypothesis supported being the negative influence of privacy concerns on network size. These findings are similar to [14] who found privacy concerns predicted friending but not disclosure. But they also find privacy concerns predict privacy setting use, which this paper does not. This could be because they did not include contrary beliefs in their privacy calculus model. It could also be due to using student respondents, who are more adept at using privacy settings.

C. Contribution 3: Testing Differential Effects of Use Behaviors on OSN Gratifications Obtained

This paper contributes in a major way by showing the differential effects of privacy behaviors on OSN gratifications obtained. This is key because investigating the outcomes of specific privacy behaviors has been largely neglected in the information systems privacy literature. This paper finds that the effects depend on the privacy behavior and the gratification. This paper also shows that use frequency has positive effects on all gratifications obtained, which provides empirical support for these factors being important OSN gratifications. While privacy behaviors have weaker influences on the gratifications obtained, this paper's results are a first step in understanding their implications for continued use.

And importantly, findings show that the privacy behaviors affect the OSN gratifications in an interactive way. The supplemental analysis finds a three-way interaction among the privacy behaviors on predicting enjoyment and habit. Because the three-way interaction is significant, the significant negative effect of privacy behavior on enjoyment in the main analysis cannot be interpreted. The three-way interaction means that as one's friend list gets larger, users will enjoy using Facebook and feel its use has become habitual if they also set more restrictive privacy settings and limit disclosure. While having a larger friends list may contribute to more pleasurable and routine social networking, this is only true if users protect the "visibility" of their information by engaging in more restrictive privacy behaviors. Control over privacy in this case is not seen as a burden as predicted, but rather gives them more pleasure and increased feelings of automaticity. Further, the lowest common denominator approach assumes individuals deal with large friend lists by not posting as much information. They would not use privacy settings because this would be too confusing with so many friends. Current findings suggest that individuals may combine the lowest common denominator strategy with privacy setting use to obtain pleasure and feel like Facebook use has become routine. This is consistent with the earlier discussion of the mean privacy behaviors.

The two-way interaction between privacy setting use and network size on bonding social capital is also significant, meaning that as network size increases, using more restrictive privacy settings increases bonding capital. This is supported by research

that claims bonding capital may decrease the more friends one has because individuals cannot feel comfortable or close to everyone. However, by putting people into groups, individuals can better control who sees what, and they can share more private information with their closer friends to increase bonding capital [82]. While Ellison *et al*. [82] also find that higher privacy setting use increases bonding capital, by examining its interaction effect with network size, the findings in this research contribute by explaining an important nuance of this relationship.

More privacy setting use has a negative impact, and network size has a positive impact, on bridging social capital. Both of these relationships support predictions [see H7(d) and H8(d)] that having a more public profile and having a large number of friends can help one make new connections. There are no significant effects of the privacy behaviors on usefulness, which while surprising, means that users expect Facebook to enhance their social networking effectiveness regardless of privacy behaviors. The finding that privacy behaviors do not directly affect usage continuance intentions, rather they are fully mediated by the gratifications obtained shows *how* privacy behaviors affect use intention (i.e., via gratifications obtained), which has not previously been examined.

In sum, this paper adds to the literature by suggesting that users may juggle the three behaviors that represent controls—privacy setting use, friending fewer people, and disclosing less personal information. Showing the effects of all three privacy behaviors on outcomes helps show the full picture of how OSN privacy behaviors work. While model parsimony is usually desirable, Hirschman [83, p. 89] in being "against parsimony" supports less parsimony when the complexity of the situation calls for a larger more explanatory model.

D. Research Implications

This research implies that it is crucial to include multiple privacy behaviors and gratifications obtained in other privacy models. The privacy calculus model typically only addresses one privacy behavior, information disclosure [7]; but this paper shows that all three privacy behaviors play a role—and sometimes an interactive role—in an OSN privacy calculus model. Also, neither the privacy calculus model nor the antecedents-privacy concerns-outcomes macromodel [84] depicts privacy behavior outcomes. These models should be extended to include both other privacy behaviors and OSN gratifications obtained. Likewise, this paper's findings could extend research using communications privacy management theory, which depicts how people create and manage the boundaries around personal information [85]. To better understand the unsupported relationships, future research could investigate the relationships among privacy behaviors and gratifications obtained with different samples and in different time periods.

Another research implication involves the effects of personal interest, trust, and privacy concern on the privacy and use behaviors. Findings show that when personal interests override privacy concerns, individuals maintain more public privacy behaviors. This is a core part of the privacy calculus model and helps explain the privacy paradox. While some others include this personal interest variable [35], [36], more privacy calculus researchers should include this variable in their models to better understand why users choose certain privacy behaviors.

Another important implication is that individuals may use different combinations of privacy behaviors to affect certain outcomes. This seems similar to Kirsch's [86] finding that systems development stakeholders implement different portfolios of control (formal and informal) that use overlapping and complementary mechanisms. Examining only one control or one type of control is inadequate for understanding multiple controls in a complex environment [86]. Identifying and studying the *portfolios* of control people use provides a richer understanding of how they achieve project objectives [85]. While findings show that a strategy of using more restrictive privacy settings, limiting disclosure, and having a larger network size positively influences enjoyment and habit, other control strategies influence bonding and bridging social capital. Future research can further investigate these and other privacy behavior strategies. One way to do this would be to determine privacy behavior clusters and run the Fig. 1 research model by cluster.

Future research can also continue to study the OSN privacy behaviors explored in this paper and other privacy behaviors like wall management, asking a friend to untag a photo [57] or posting fake information. These behaviors probably have additional effects.

E. Practical Implications

This research also has practical implications. First, studying the various privacy behaviors used on Facebook can increase awareness of their use and importance to providers, developers, marketers, and employers. For example, findings show that users do not limit their friend list much, but instead compensate by limiting the content posted and others' access to this content. This accentuates the need for providers and developers to continue to make privacy settings easier to use. For example, around the time of this survey, Facebook changed its default privacy setting from everyone or public to friends.[8] However, some actions have been inconsistent with privacy management. Since the survey was performed for this paper, Facebook reportedly made it impossible to hide user profiles from strangers.[9] If individuals are relying on privacy settings (and limiting disclosure) to deal with increased friend lists, and this leads to enjoyment and continued use, OSN providers should ensure access can be controlled through privacy settings.

This research can also inform marketers because findings show how and why consumers protect their personal information on OSN websites. Companies that encourage more involvement with social media can influence continued use. However, more importantly, this paper's findings show that if users feel their personal interests override their concerns, they will be more likely to engage in more public behaviors. Companies should continue to find ways to entice personal interest and involve users through feedback systems, advertisements, personalization, new features, and coupon offers.

[8][Online]. Available: https://www.forbes.com/sites/larrymagid/2014/05/22/facebook-changes-default-privacy-setting-for-new-users/#29905dcf59ac

[9][Online]. Available: https://www.theguardian.com/technology/2016/jun/29/facebook-privacy-secret-profile-exposed

F. Limitations

This paper also has several limitations. First, because the study is not longitudinal in nature, the model relationships are correlational not causal. There is a chance, for example, that enjoyment influences privacy behaviors or that privacy behaviors influence trust. However, theory and prior empirical research guided the development of this paper's research model and the direction of relationships between variables. Further, supplemental models do not explain as well as the original model. Second, there might be many ways to measure certain privacy behaviors. For example, while limiting disclosure items asked subjects how much they limit content, it could also be measured by asking what specific content they limit. Finally, because this paper used perceptual measures of privacy behaviors, results are not proven to be applicable to actual behaviors. However, these perceptual measures may correlate well with the actual behaviors based on other research works. For one example of many, Pavlou and Gefen [87] find that in an online marketplace, transaction intentions and actual transaction behavior correlated at 0.68. This shows that models using perceived measures may provide a reasonable set of proxy evidence for behaviors.

VI. Conclusion

This paper contributed to information systems research by using an integrated model to examine OSN privacy behaviors. It developed and tested a nomological network focusing on three OSN privacy behaviors and use frequency. Findings showed that users' privacy concerns, trust, and personal interest in using Facebook affected their privacy behaviors and use frequency. More concerns resulted in users being more private by limiting their friend list, while more trust and personal interest influenced users to be more public. Further, the privacy and use behaviors led to key OSN gratifications obtained, some of which led to usage continuance intention. The clear linkage from privacy behaviors to these outcomes took privacy research in a new direction. Overall, a model focusing on both the antecedents and outcomes of privacy behaviors provided significant insights. This research not only examined privacy behaviors and how they influence intentions to continue using OSN, but it also created opportunities for future research to understand OSN privacy and its complex nature.

Appendix

Measurement Items

Privacy Risk (7-point Likert from (1) Very Low Risk to (7) Very High Risk)

What do you believe is the risk for MySNW.com users due to the possibility that:

1) MySNW.com entries and posts could be sold to third parties?
2) Personal information submitted could be misused?
3) Personal information could be made available to unknown individuals or companies without your knowledge?
4) Personal information could be made available to government agencies?

Privacy Concern (7-point Likert from (1) Not at all Concerned to (7) Very Concerned)

1) I am concerned that the information I submit on MySNW.com could be misused.
2) I am concerned that a person could find private information about me on MySNW.com.
3) I am concerned about submitting information on MySNW.com because of what others might do with it.
4) I am concerned about submitting information on Mysnw.com because it could be used in a way I did not foresee.

Trusting Beliefs

Integrity (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) MySNW.com is truthful in its dealings with me.
2) MySNW.com is honest.
3) MySNW.com keeps its commitments.

Competence (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) MYSNW.com is competent and effective in providing OSN.
2) MySNW.com performs the role of facilitating OSN very well.
3) MySNW.com is a capable and proficient OSN provider.

Benevolence (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) MySNW.com acts in my best interest.
2) MySNW.com does its best to help me if I need help.
3) MySNW.com is interested in my well-being, not just its own.

Personal Interest (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) I find that personal interests in using MySNW.com override my concerns of possible risk or vulnerability that I may have regarding my privacy.
2) The greater my interest in using MySNW.com, the more I tend to suppress my privacy concerns.
3) In general, my need to use MySNW.com is greater than my concern about privacy.

Limiting Disclosure (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) I limit the content I place on MySNW.com.
2) I do not place things on MySNW.com that I do not want others to see.
3) I do not have very personal information on my MySNW.com account.

Privacy Setting Use (5-point Likert (1) Everyone on SNW.com, (2) Friends of Friends, (3) Only Friends, (4) Customize (specific people), (5) No One) Who do you allow to see the following types of information?

1) Basic information (sex, birthday, hometown, political and religious views).
2) Contact information (emails, IM screen name, home/school addresses and phone numbers, website URL).
3) Relationship information (status, interested in, looking for).

4) Personal information (activities, interests, about me, favorite movies, TV shows, books, and quotes).
5) Educational information (university, concentration, class, year, high school).
6) Work information (employer, position, description, city/town, time period).
7) Tagged photos.
8) Your status, photos, and posts.
9) Places you check into.

Network Size (8-point scale (1) 1–50, (2) 51–100, (3) 101–150, (4) 151–250, (5) 251–350, (6) 351–500, (7) 501–1000, (8) Greater than 1000)

1) Approximately how many total MySNW.com friends do you have?

Usage Frequency (7-point scale from (1) Not at all to (7) Extremely frequently. I use MySNW.com . . .

1) To improve how my profile and my other postings look.
2) To accept of decline friend requests.
3) To read posts on my wall.
4) To tag or post photos.
5) To search for new friends.
6) To search for and locate old friends.
7) To read the wall/news feed about others.
8) To browse through others' photos.
9) To play games.
10) To use nongame apps.
11) To look for social events/parties to attend.
12) To create or join a group.
13) To send messages to friends.

Usefulness (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) Using MySNW.com improves my performance in OSN.
2) Using MySNW.com increases my productivity in OSN.
3) Using MySNW.com enhances my effectiveness in OSN.
4) I find MySNW.com to be useful for OSN.

Enjoyment (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) I find using MySNW.com to be enjoyable.
2) The actual process of using MySNW.com is pleasant.
3) I have fun using MySNW.com.

Bonding Social Capital (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) There are several people on Facebook.com I trust to help solve my problems.
2) There is someone on Facebook.com I can turn to for advice about making very important decisions.
3) There is no one on Facebook.com that I feel comfortable talking to about intimate personal problems (*dropped*).
4) When I feel lonely, there are several people on Facebook.com I can talk to.
5) If I needed an emergency loan of $500, I know someone on Facebook.com I can turn to.
6) The people I interact with on Facebook.com would put their reputation on the line for me.
7) The people I interact with on Facebook.com would be good job references for me.
8) The people I interact with on Facebook.com would share their last dollar with me.
9) I do not know people on Facebook.com well enough to get them to do anything important (*dropped*).
10) The people I interact with on Facebook.com would help me fight an injustice.

Bridging Social Capital (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) Interacting with people on Facebook.com makes me interested in things that happen outside of my town.
2) Interacting with people on Facebook.com makes me want to try new things.
3) Interacting with people on Facebook.com makes me interested in what people like me are thinking.
4) Talking with people on Facebook.com makes me curious about other places in the world.
5) Interacting with people on Facebook.com makes me feel like part of a larger community.
6) Interacting with people on Facebook.com makes me feel connected to the bigger picture.
7) Interacting with people on Facebook.com reminds me that everyone in the world is connected.
8) I am willing to spend time to support general Facebook.com community activities.
9) Interacting with people on Facebook.com gives me new people to talk to.
10) On Facebook.com, I come in contact with new people all the time.

Habit (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1) The use of MySNW.com has become a habit for me.
2) Using MySNW.com is natural for me.
3) I do not even think twice before using MySNW.com.
4) Using MySNW.com has become automatic to me.
5) When faced with a particular t ask, using MySNW.com is an obvious choice for me.

Continuance Intention (7-point Likert from (1) Not True at All to (7) Absolutely True)

1) In the near future, I intend to continue using MySNW.com
2) I intend to continue using MySNW.com
3) I predict that I would continue using MySNW.com.

Prior Experience (7-point scale from (1) Have not used at all to (7) More than 5 years)

1) How long have you been using MySNW.com?

REFERENCES

[1] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation," *Org. Sci.*, vol. 10, pp. 104–115, 1999.
[2] C. Cheung, Z. W. Y. Lee, and T. K. H. Chan, "Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence," *Internet Res.*, vol. 25, no. 2, pp. 279–299, 2015.
[3] H. Krasnova, N. F. Veltri, and O. Gűnther, "Self-disclosure and privacy calculus on social networking sites: The role of culture," *Bus. Inf. Syst. Eng.*, vol. 4, no. 3, pp. 127–135, 2012.
[4] N. B. Ellison, J. Vitak, C. Steinfield, R. Gray, and C. Lampe, "Negotiating privacy concerns and social capital needs in a social media environment," in *Privacy Online*, S. Trepte and L. Reinecke, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 19–32.

[5] P. Block and T. Grund, "Multidimensional homophily in friendship networks," *Netw. Sci.*, vol. 2, no. 2, pp. 189–212, 2014.

[6] S. L. Feld, "Social structural determinants of similarity among associates," *Amer. Sociol. Rev.*, vol. 47, no. 6, pp. 797–801, 1982.

[7] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, 2006.

[8] E. S.-T. Wang and R.-L. Lin, "Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention," *Behav. Inf. Technol.*, vol. 36, no. 1, pp. 2–10, 2017.

[9] R. Chen, S. K. Sharma, and H. R. Rao, "Members' site use continuance on Facebook: Examining the role of relational capital," *Decis. Support Syst.*, vol. 90, pp. 86–98, 2016.

[10] T. E. Ruggiero, "Uses and gratifications theory in the 21st century," *Mass Commun. Soc.*, vol. 3, pp. 3–37, 2000.

[11] P. Palmgreen, L. A. Wenner, and J. D. Rayburn, "Relations between gratifications sought and obtained: A study of television news," *Commun. Res.*, vol. 7, no. 2, pp. 161–192, 1980.

[12] J. D. Rayburn and P. Palmgreen, "Merging uses and gratifications and expectancy-value theory," *Commun. Res.*, vol. 11, pp. 537–562, 1984.

[13] C. L. Anderson and R. Agarwal, "The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Inf. Syst. Res.*, vol. 22, no. 3, pp. 469–490, Sep. 2011.

[14] H.-T. Chen and W. Chen, "Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection," *Cyberpsychol., Behav., Social Netw.*, vol. 18, no. 1, pp. 13–19, 2015.

[15] T. Dienlin and M. J. Metzger, "An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample," *J. Comput.-Mediated Commun.*, vol. 21, pp. 368–383, 2016.

[16] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, and C. Colautti, "Privacy calculus model in e-commerce: A study of Italy and the United States," *Eur. J. Inf. Syst.*, vol. 15, no. 4, pp. 389–402, 2006.

[17] C. Hallam and G. Zanella, "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards," *Comput. Hum. Behav.*, vol. 68, pp. 217–227, 2017.

[18] T. L. James, M. Warkentin, and S. E. Collignon, "A dual privacy decision model for online social networks," *Inf. Manage.*, vol. 52, pp. 893–908, 2015.

[19] Z. Jiang, C. S. Heng, and B. C. F. Choi, "Research note: Privacy concerns and privacy-protective behavior in synchronous online social interactions," *Inf. Syst. Res.*, vol. 24, no. 3, pp. 579–595, 2013.

[20] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch, "Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Inf. Syst. J.*, vol. 25, pp. 607–635, 2015.

[21] M. J. Keith, J. S. Babb, P. B. Lowry, C. P. Furner, and A. Abdullat, "The role of mobile-computing self-efficacy in consumer information disclosure," *Inf. Syst. J.*, vol. 25, pp. 637–667, 2015.

[22] M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry, and C. Greer, "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior," *Int. J. Hum.-Comput. Studies*, vol. 71, pp. 1163–1173, 2013.

[23] N. Kordzadeh, J. Warren, and A. Seifi, "Antecedents of privacy calculus components in virtual health communities," *Int. J. Inf. Manage.*, vol. 36, pp. 724–734, 2016.

[24] N. Kordzadeh and J. Warren, "Communicating personal health information in virtual health communities: an integration of privacy calculus model and affective commitment," *J. Assoc. Inf. Syst.*, vol. 18, no. 1, pp. 45–81, 2017.

[25] H. Krasnova, E. Kolesnikova, and O. Gűnther, "It won't happen to me!: Self-disclosure in online social networks," in *Proc. 15th Amer. Conf. Inf. Syst.*, San Francisco, CA, USA, Aug. 6–9, 2009, pp. 1–9.

[26] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: Why we disclose?" *J. Inf. Technol.*, vol. 25, pp. 109–125, 2010.

[27] H. Li, R. Sarathy, and H. Xu, "Understanding situational online information disclosure as a privacy calculus," *J. Comput. Inf. Syst.*, vol. 51, no. 1, pp. 62–71, 2010.

[28] H. Li, J. Wu, Y. Gaob, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," *Int. J. Med. Inform.*, vol. 88, pp. 8–17, 2016.

[29] C. Morosan and A. DeFranco, "Disclosing personal information via hotel apps: A privacy calculus perspective," *Int. J. Hospitality Manage.*, vol. 47, pp. 120–130, 2015.

[30] I. Pentina, L. Zhang, H. Bata, and Y. Chen, "Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison," *Comput. Hum. Behav.*, vol. 65, pp. 409–419, 2016.

[31] R. L. Raschke, A. S. Krishen, and P. Kachroo, "Understanding the components of information privacy threats for location-based services," *J. Inf. Syst.*, vol. 28, pp. 227–242, 2014.

[32] Y. Sun, N. Wang, X.-L. Shen, and J. X. Zhang, "Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences," *Comput. Hum. Behav.*, vol. 52, pp. 278–292, 2015.

[33] L. Wang, J. Yan, J. Lin, and W. Cui, "Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking," *Int. J. Inf. Manage.*, vol. 37, pp. 1428–1440, 2017.

[34] T. Wang, T. D. Duong, and C. C. Chen, "Intention to disclose personal information via mobile applications: A privacy calculus perspective," *Int. J. Inf. Manage.*, vol. 36, pp. 531–542, 2016.

[35] H. Xu, H.-H. Teo, B. C. Y. Tan, and R. Agarwal, "The role of push–pull technology in privacy calculus: The case of location-based services," *J. Manage. Inf. Syst.*, vol. 26, no. 3, pp. 135–173, 2009.

[36] H. Xu, X. Luo, J. M. Carroll, and M. B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decis. Support Syst.*, vol. 51, pp. 42–52, 2011.

[37] H. Xu, C. Zhang, P. Shi, and P. Song, "Exploring the role of overt vs. covert personalization strategy in privacy calculus," in *Proc. Acad. Manage. Annu. Meeting*, 2009, pp. 1–6.

[38] F. Xu, K. Michael, and Z. Chen, "Factors affecting privacy disclosure on social network sites: an integrated model," *Electron. Commerce Res.*, vol. 13, pp. 151–168, 2013.

[39] L. Zhao, Y. Lu, and S. Gupta, "Disclosure intention of location-related information in location-based social network services," *Int. J. Electron. Commerce*, vol. 16, no. 4, pp. 53–89, 2012.

[40] S. E. Chang, A. Y. Liu, and W. C. Shen, "User trust in social networking services: A comparison of Facebook and LinkedIn," *Comput. Hum. Behav.*, vol. 69, pp. 207–217, 2017.

[41] Y. Li, "Empirical studies on online information privacy concerns: Literature review and an integrative framework," *Commun. Assoc. Inf. Syst.*, vol. 28, 2011.

[42] Y. Feng and W. Xie, "Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," *Comput. Hum. Behav.*, vol. 33, pp. 153–162, 2014.

[43] Y. Jordaan and G. Van Heerden, "Online privacy-related predictors of Facebook usage intensity," *Comput. Hum. Behav.*, vol. 70, pp. 90–96, 2017.

[44] M. Ng, "Factors influencing the consumer adoption of Facebook: A two-country study of youth markets," *Comput. Hum. Behav.*, vol. 54, pp. 491–500, 2016.

[45] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Inf. Syst. Res.*, vol. 13, no. 3, pp. 334–359, 2002.

[46] T. James, Q. Nottingham, and B. C. Kim, "Determining the antecedents of digital security practices in the general public dimension," *Inf. Technol. Manage.*, vol. 4, pp. 69–89, 2013.

[47] C. M. K. Cheung, P.-Y. Chiu, and M. K. O. Lee, "Online social networks: Why do students use Facebook?" *Comput. Hum. Behav.*, vol. 27, pp. 1337–1343, 2011.

[48] L. J. Orchard, C. Fullwood, N. Galbraith, and N. Morris, "Individual differences as predictors of social networking," *J. Comput.-Mediated Commun.*, vol. 19, pp. 388–402, 2014.

[49] A. M. Rubin, "The uses-and-gratifications perspective of media effects," in *Media Effects*, J. Bryant and D. Zillmann, Eds. Mahwah, NJ, USA: Lawrence Erlbaum Associates, 2002, pp. 525–548.

[50] A. Quan-Haase and A. L. Young, "Uses and gratifications of social media: A comparison of Facebook and instant messaging," *Bull. Sci., Technol. Soc.*, vol. 30, no. 5, pp. 350–361, 2010.

[51] Z. Wang, J. M. Tchernev, and T. Solloway, "A longitudinal examination of social media use, needs, and gratifications among college students," *Comput. Hum. Behav.*, vol. 28, pp. 1829–1839, 2012.

[52] A. N. Joinson, "'Looking at', 'Looking up' or 'Keeping up with' people? Motives and uses of Facebook," in *Proc. CHI, Online Soc. Netw.*, Florence, Italy, Apr. 5–10, 2008, pp. 1027–1036.

[53] E. Katz, H. Haas, and M. Gurevitch, "On the use of the mass media for important things," *Amer. Sociol. Rev.*, vol. 38, no. 2, pp. 164–181, 1973.

[54] A. Whiting and D. Williams, "Why people use social media: A uses and gratifications approach," *Qual. Market Res.*, vol. 16, no. 4 pp. 362–369, 2013.

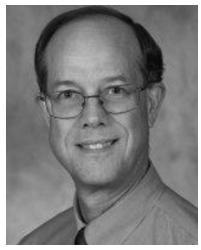
[55] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "Extrinsic and intrinsic motivation to use computers in the workplace," *J. Appl. Soc. Psychol.*, vol. 22, no. 14, pp. 1111–1132, 1992.

[56] N. Lankton, H. McKnight, and J. Thatcher, "The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website," *IEEE Trans. Eng. Manage.*, vol. 59, no. 4, pp. 654–665, Nov. 2012.
[57] K. Quinn, "Why we share: A uses and gratifications approach to privacy regulation in social media use," *J. Broadcast. Electron. Media*, vol. 60, no. 1, pp. 61–86, 2016.
[58] D. Liu and B. Brown, "Self-disclosure on social networking sites, positive feedback, and social capital among Chinese college students," *Comput. Hum. Behav*, vol. 38, pp. 213–219, 2014.
[59] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of FACEBOOK," *Comput. Hum. Behav.*, vol. 26, pp. 406–418, 2010.
[60] G. Seidman, "Expressing the 'True Self' on Facebook," *Comput. Hum. Behav.*, vol. 31, pp. 367–372, 2014.
[61] M. Limayem, S. G. Hirt, and C. M. K. Cheung, "How habit limits the predictive power of intention: The case of information systems continuance," *MIS Quart.*, vol. 31, no. 4, pp. 705–737, 2007.
[62] B. Hogan, "The presentation of self in the age of social media: Distinguishing performances and exhibitions online," *Bull. Sci., Technol. Soc.*, vol. 30, no. 6, pp. 377–386, 2010.
[63] M. Bartsch and T. Dienlin, "Control your Facebook: An analysis of online privacy literacy," *Comput. Hum. Behav.*, vol. 56, 147–154, 2016.
[64] J. A. Bargh and T. L. Chartrand, "The unbearable automaticity of being," *Amer. Psychol.*, vol. 54, pp. 462–479, 1999.
[65] C. P. Lin and A. Bhattacherjee, "Understanding online social support and its antecedents: A socio-cognitive model," *Soc. Sci. J.*, vol. 46, pp. 724–737, 2009.
[66] K. Y. Lin and H.-P. Lu, "Why people use social networking sites: An empirical study integrating network externalities and motivation theory," *Comput. Hum. Behav.*, vol. 27, pp. 1152–1161, 2011.
[67] V. Venkatesh, M. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: toward a unified view," *MIS Quart.*, vol. 27, no. 3, pp. 425–478, 2003.
[68] Y. P. Chang and D. H. Zhu, "The role of perceived social capital and flow experience in building users' continuance intention to social networking sites in China," *Comput. Hum. Behav.*, vol. 26, pp. 995–1001, 2012.
[69] A. Bhattacherjee and G. Premkumar, "Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test," *MIS Quart.*, vol. 28, no. 2, pp. 229–254, 2004.
[70] D. Williams, "On and off the 'net: Scales for social capital in an online era," *J. Comput.-Mediated Commun.*, vol. 11, no. 2, 2006, Art. no. 11.
[71] A. Hardin, J. Chang, and M. A. Fuller, "Formative versus reflective measurement: Comment on Marakas, Johnson, and Clay 2007," *J. Assoc. Inf. Syst.*, vol. 9, no. 9, pp. 519–534, 2008.
[72] C. M. Ringle, S. Wende, and J.-M. Becker, "SmartPLS 3. Boenningstedt: SmartPLS GmbH," 2015. [Online]. Available: http://www.smartpls.com
[73] J. C. Nunnally and I. H. Bernstein, *Psychometric Theory*, 3rd ed. New York, NY, USA: McGraw-Hill, 1994.
[74] V. E. Vinzi, L. Trinchera, and S. Amato, "PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement," in *Handbook of Partial Least Squares: Concepts, Methods, and Applications*, V. E. Vinzi, W. W. Chin, J. Henseler, and H. Wang, Eds. Heidelberg, Germany: Springer, 2010, pp. 47–82.
[75] C. Fornell and D. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Market. Res.*, vol. 18, no. 3, pp. 39–50, 1981.
[76] S. Menard, *Applied Logistic Regression Analysis: Sage University Series on Quantitative Applications in the Social Science*. Thousand Oaks, CA, USA: Sage, 1995.
[77] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003.
[78] R. M. Baron and D. A. Kenny, "The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations," *J. Pers. Soc. Psychol.*, vol. 51, no. 6, pp. 1173–1182, 1986.
[79] A. Vance, P. B. Lowry, and D. Eggett, "Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations," *MIS Quart.*, vol. 39, no. 2, pp. 345–366, 2015.
[80] W. F. Hong, K. Y. Chan, J. K. L. Thong, L C. Chasalow, and G. Dhillon, "A framework and guidelines for context-specific theorizing in information systems research," *Inform. Syst. Res*, vol. 25, no. 1, pp. 111–136, 2014.
[81] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Acad. Manage. Rev.*, vol. 23, no. 3, pp. 393–404, 1998.
[82] N. B. Ellison, C. Steinfield, and C. Lampe, "Connection strategies: Social capital implications of Facebook-enabled communication practices," *New Media Soc.*, vol. 13, no. 6, pp. 873–892, 2011.
[83] A. O. Hirschman, "Against parsimony: Three easy ways of complicating some categories of economic discourse." *Amer. Econ. Rev.*, vol. 74, no. 1, pp. 89–96, 1984.
[84] S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY, USA: State Univ. New York Press, 2002.
[85] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, no. 4, pp. 989–1015, 2011.
[86] L. S. Kirsch, "Portfolios of control modes and IS project management," *Inf. Syst. Res.*, vol. 8, no. 3, pp. 215–239, 1997.
[87] P. Pavlou and D. Gefen, "Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role," *Inf. Syst. Res.*, vol. 16, no. 4, pp. 372–399. 2005.

Nancy K. Lankton received the Ph.D. degree in business administration from Arizona State University, Tempe, AZ, USA, in 2000.

She started her career in public accounting, and has worked in accounting and finance industry positions. She is currently the Chair of the Division of Accountancy and Legal Environment, Brad D. Smith Schools of Business, Marshall University, Huntington, WV, USA. She has authored or coauthored papers published in highly recognized, leading peer-reviewed journals including *Contemporary Accounting Research, Information Systems Research*, the *Journal of Strategic Information Systems*, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, the *Journal of Management Information Systems*, the *Journal of Information Systems*, and the *Journal of the Association for Information Systems*. Her current research interests include technology trust and corporate/IT governance.

Dr. Lankton is on the review board for the Journal of the Association for Information Systems.



Harrison McKnight received the Ph.D. degree in management information systems (MIS) from the University of Minnesota, Minneapolis, MN, USA, in 1997.

After a four year stint at Florida State University, he joined Michigan State University in 2001. He primarily conducts behavioral field research, focusing on trust in technology, sharing economy trust, initial trust, trust building, trust change over time, trust repair, expectation disconfirmation theory, and technical employee retention. He has served as an Associate Editor for *MIS Quarterly*, *Information and Management*, and the *Journal of Trust Research*. Some of his work has been published in *MIS Quarterly*, the *Academy of Management Review*, *Information Systems Research*, the *Journal of the Association for Information Systems*, *Journal of Management Information Systems*, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, and the *Journal of Strategic Information Systems*.

John F. Tripp received the Ph.D. degree in information technology management from Michigan State University, East Lansing, MI, USA, in 2012.

He is an Assistant Professor of Information Systems with Baylor University, Waco, TX, USA. Before beginning his Ph.D. degree, he worked for more than 17 years in industry as a Software Developer, Project Manager, and the IT Director. His research has appeared or is forthcoming in the *Journal of the Association for Information Systems*, *Computers and Human Behavior, Journal of Computer Information Systems, Information Systems and e-Business Management,* and the *Journal of Management Systems*. His research has appeared in the proceedings of multiple conferences including the International Conference on Information Systems, the Hawaii International Conference on Systems Sciences, the European Conference of Information Systems, and the Americas Conference on Information Systems.