Saving Face on Facebook: Privacy Concerns, Social Benefits, and Impression Management

Completed Research Paper

David W. Wilson
University of Arizona
Tucson, AZ, USA
davidwilsonphd@gmail.com

Jeffrey G. Proudfoot
Bentley University
Waltham, MA, USA
jproudfoot@bentley.edu

Joseph S. Valacich
University of Arizona
Tucson, AZ, USA
jsvalacich@cmi.arizona.edu

Abstract

Use of online social networks is nearly ubiquitous. Use of these services generally entails substantial personal disclosure and elicits significant privacy concerns. This research uses Social Exchange Theory and the impression management literature to examine how privacy concerns can be counterbalanced by the perceived social benefits afforded by a social network's ability to support impression management. We frame social network use as an attempt to engage in impression management, and we highlight the importance of a social network's impression management capabilities in predicting social benefits from, and use of, a social network. We test our model with a sample of 244 Facebook users, finding strong support for the proposed relationships. Our theory has important implications for researchers and practitioners interested in privacy issues within social networks.

Keywords: Impression management, privacy, social media, Social Exchange Theory

Introduction

Online social networks—online environments where users present themselves via individual profiles and communicate with other users (Gross and Acquisti 2005)—have exploded in popularity in the last decade, with an estimated 73 percent of adults in the US now using an online social network (Pew Research Center 2013a) and Facebook.com boasting over 1.2 billion active users (Kiss 2014). Most social network use constitutes unprecedented personal disclosure with broad implications; privacy activists and scholars have noted the clear privacy risks associated with extensive social network use (Giles 2010; Gross and Acquisti 2005; Krasnova et al. 2010). Social network users tend to be concerned about their privacy (Pew Research Center 2013b), and privacy concerns are cited as a key reason for abandoning social network accounts (Stieger et al. 2013). However, social network use, with its accompanying disclosure, permits deep customer segmentation, targeted advertising, and other business applications (Krasnova et al. 2010). It is thus of great value to practitioners and researchers to better understand the mechanisms by which individuals’ privacy concerns are overcome as they use social networks.

Online social networks are similar to other online settings (Dinev and Hart 2006) as they present users with two opposing goals: on one hand, users want to disclose information about themselves for several reasons, including cultivating friendships and feeling connected; on the other hand, users are concerned...
about their privacy, which should motivate them to disclose as little as possible about themselves. This research illuminates the tension between these two goals, and we frame the motivating benefits of disclosure as users’ attempts to establish and communicate an identity to their network peers. Individuals have an innate need to create and project an identity to people around them (Lecky and Taylor 1945; Secord and Backman 1965; Swann et al. 2004), and to manipulate that identity in strategic ways—an activity called impression management (Goffman 1959; Leary and Kowalski 1990). Social networking platforms provide users a wide, accessible audience to whom they can frequently communicate their personality, interests, and so forth. Though the growing popularity of social networks has instigated an explosion of new and interesting research (Bohnert and Ross 2010; Ganley and Lampe 2009; Khan and Jarvenpaa 2010; Krasnova et al. 2010; Posey et al. 2010), few of these studies (Krämer and Winter 2008) have explored use of these networks as fulfilling users’ need for identity communication and impression management. Since impression management is an important psychological need (Zhang 2008a; Zhang 2008b), it may be a key driver of extensive social network use, even in the face of numerous potential risks. The question guiding this research, then, is how does a social network’s ability to support impression management counterbalance the potential privacy concerns of social network use?

To investigate this question, we leverage two bases of theory—social exchange theory and impression management theory. This strong foundation is used to justify a theoretical model that places users’ concerns about privacy in opposition to their desire for impression management and other social benefits. We place particular emphasis on user perceptions regarding the extent to which the social network allows them to create and share their identity with others. We then test the model using a sample of 244 Facebook users, finding strong support for the importance of social networks’ impression management capabilities. We conclude by discussing the contributions of our findings to theory and practice.

**Related Literature**

Before we build and justify our theoretical model, we first briefly summarize the two literatures from which we draw our constructs and proposed relationships. We use social exchange theory, of which the popular privacy calculus framework is a subset, to understand how privacy-related risks or concerns can be outweighed by other perceived benefits. Lastly, we explore the motivational foundation for individuals’ need to create and manage impressions, and we survey the previous literature that has addressed these topics.

**Social Exchange Theory**

Use of an online social network is a primarily social activity, and we frame the benefits available to users as social benefits. Prior theorists have leveraged Social Exchange Theory (Blau 1964) to explain the cognitive process that individuals undergo when deciding whether to engage in a social relationship (Jarvenpaa and Staples 2001; Posey et al. 2010; Wasko and Faraj 2005). SET proposes that individuals weigh the costs and benefits of an interaction prior to engaging in a social interaction. Following the SET logic, individuals engage in activities that promote relationships when the perceived benefits associated with that behavior outweigh the costs expected from the action (Kankanhalli et al. 2005).

SET has been widely applied in the IS literature. Research based on SET has shown that employees are more willing to exchange information when they believe the organization will reciprocate with increased recognition (Jarvenpaa and Staples 2001). Users of online communities contribute more knowledge to other members if they perceive that their contributions will improve their reputation (Kankanhalli et al. 2005; Wasko and Faraj 2005). SET has been used in many other contexts, including CRM system approval (Gefen and Ridings 2002) and knowledge sharing in virtual teams (Staples and Webster 2008). We instantiate SET in our social network context to examine the cost-benefit decision process associated with social network use.

A popular framework within the privacy literature—the privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006)—can arguably be framed as a special case of SET. The privacy calculus frames privacy-threatening behavior as the outcome of a cost-benefit decision process, following the assumption that private information can be treated as a tradable good. This calculus involves weighing the perceived concerns or risks against the perceived benefits of the interaction, with disclosure or other behavior occurring when benefits outweigh risks.
IS researchers have extended the work of Culnan and Armstrong (1999) to the context of the Internet (Dinev and Hart 2006), where the potential methods with which to collect and analyze private information have been expanded to nearly all forms of electronic interactions. The privacy issues associated with electronic interactions have motivated a rich stream of research. This research has investigated such mitigating factors as privacy policy statements (Li et al. 2011), industry and government regulation (Xu et al. 2009), familiarity with the vendor (van Slyke et al. 2006), and personally relevant benefits (Dinev and Hart 2006) as possible factors that persuade users to transact in online settings by increasing perceived benefits or reducing perceived risks associated with disclosure.

While the privacy calculus framework has been rather extensively tested in the e-commerce literature, it has not been frequently applied to the privacy issues present in online social networks. The rich privacy theories being advanced in e-commerce research may not adapt well to the social network context, given the differences between the two contexts in terms of the goal of the interaction (completing an online transaction vs. social connectedness and/or identity formulation). Further, some concerns associated with privacy in an e-commerce transaction (e.g., risk of financial loss) may be very different from those in an online social network (e.g., risk of social embarrassment). The social psychology perspective developed in this research provides unique insight into the concerns and motivations inherent to the social network context.

In summary, SET, of which the privacy calculus framework is a special case, frames behaviors as a result of a cost-benefit evaluation. We use SET as a guiding framework to better understand the tension between the risks of social network use and the perceived social benefits available online. We use SET further to understand the role of trust in augmenting the cost-benefit evaluations within the model. Before building the model, we will first explore identity, impression management behaviors, and the implications of social network use on those behaviors.

Impression Management

Theories regarding identity are numerous and well established. Identity is defined as “the individual’s self-appraisal of a variety of attributes along the dimensions of physical and cognitive abilities, personal traits and motives, and the multiplicity of social roles including worker, family member, and community citizen” (Whitbourne and Connolly 1999, p. 28). This definition implies that identity consists of both personal and social aspects, or the self and the “social self” (Brewer 1991). Thus, an identity is one’s mental model of himself, both in terms of who he is (i.e., characteristics that make him unique or identifiable) and to which groups he belongs (e.g., cultural, religious or familial affiliations).

Once an identity is formed, an individual desires to communicate or present that identity to others in order to provide an impression consistent with the individual’s goals. Goffman’s (1959) impression management theory underscores this point, arguing that in any social setting, individuals are in a constant state of impression management, desiring to convey and manage an “act” for others. Goffman (1967) also argues that this impression management takes place in both direct interactions and, important for our purposes, mediated interactions.

Self-presentation in online social networks has several unique nuances that bear mentioning. First, consistent with Social Presence Theory (Short et al. 1976), technology-mediated communication lacks many cues present in non-mediated communication, restricting the communicator in his social influence. When the “actor” is not physically present with his audience, it is more difficult (or often impossible) to perceive and respond to nonverbal cues to ensure the desired impression. Thus, impression management via a social network may be less effective than in person. On the other hand, following the logic of Media Synchronicity Theory (MST; Dennis et al. 2008), some aspects of technology might be beneficial to impression management. Two key antecedents in MST, rehearsability and reprocessability, both relate to asynchronous communication (which describes most technology-mediated self-presentation), wherein sender and receiver are able to think carefully about, and fully process, messages being communicated. Such features have been cited as a reason that individuals can manage self-presentations more strategically in online settings than in face-to-face settings (Ellison et al. 2006). Thus, it is important for users to be able to control the presentation of their identity information to others—i.e., to feel that they are able to engage in impression management.
Another issue associated with impression management via social networks is the relative permanence of communicated identity information. Ma and Agarwal (2007, p. 51) refer to “deep profiling” in online communities, highlighting their recording capabilities, where past interaction activity, personal information, and other data are recorded long-term and accessible to other members of the community. As found by Ma and Agarwal, this stored information can be useful in building cohesion in an online community. But such capabilities (also present in most online social networks) are also problematic in terms of self-presentation. For example, users of Facebook can upload pictures and “tag” their friends, after which that picture is associated with the tagged user’s profile and available for future viewers to see and interpret. Depending on the content of the picture, the user may or may not feel that it represents her desired identity. User profiles on online social networks have been found to directly influence others’ perceptions of them (Bohnert and Ross 2010). This is less of an issue in face-to-face impression management, in which an individual’s identity information is less permanent (restricted to memory of past direct interactions or hear-say from others who have had direct interaction with the individual). Control of identity-related information, current or past, is thus crucial for impression management in online social networking environments.

Finally, identity information often has broader reach in social networking environments. In face-to-face impression management, an individual is generally perfectly aware of whom she is communicating with regarding her identity (i.e., the people in the immediate vicinity). In an online social network communication, the individual is unaware of who will see and interpret identity information. This presents specific problems, for example, when online social networks are used to screen candidates for professional job openings. Recruiters may interpret college students’ social networking profiles in ways unintended by the students (Bohnert and Ross 2010). Again, allowing users control over identity communication (i.e., the ability to engage in impression management) should be an important precursor to users’ motivation and willingness to engage with a social network, particularly in the face of the privacy risks associated with such use.

**Prior Research Investigating Impression Management**

While impression management features are clearly a relevant topic in the context of online social networks, relatively little work in the IS literature has informed this important topic; however, there are numerous related topics that have received attention. Several researchers have acknowledged the personal home page as an effective form of self-presentation (Döring 2002; Schau and Gilly 2003; Wynn and Katz 1997). Avatars are an obvious self-presentation method in technology-mediated environments, and there has been some limited research on avatars in the context of identity communication (e.g., Messinger et al. 2008; Nowak and Rauh 2005). Lee et al. (2013) also examined self-presentation as one of several potential benefits of social network use, though their analysis combined this with other benefits and did not consider the concept separately.

Given the relevance of impression management to psychological well-being and motivation (Zhang 2008a; Zhang 2008b), several scholars have investigated these topics in other domains. Ellison et al. (2006) used qualitative interview data to investigate self-presentation strategies in an online dating site, finding that users were heavily involved in both creating and interpreting impressions being given. Krämer and Winter (2008) specifically investigated impression management behaviors in online social networks. They studied the relationship between (offline) personality traits and patterns of online self-presentation, finding that self-reported efficacy with impression management predicted number of online connections and the nature of, and level of detail in, online profiles. These prior studies clearly establish online social networks as an effective means of impression management. They do not address, however, the network’s ability to support impression management as a key counterbalance against privacy concerns in determining usage behavior.

One area that has received several references to identity communication is the online communities literature. Blanchard and Markus (2004) highlight identity communication features (e.g., signatures) as important in explaining online community participation. Shin and Kim (2010) found self-presentation in several online communities to significantly predict knowledge contribution. Most notably, Ma and Agarwal (2007) introduced the concept of identity verification to the online communities literature. They term this construct perceived identity verification, and define it as “perceived confirmation from other community members of a focal person’s belief about his identities” (p. 46). Their final model includes...
three specific artifacts of the online community that support identity verification—virtual copresence, self-presentation, and deep profiling. The online community’s ability to facilitate these activities is therefore related to users’ feelings that their identities are known and understood by others in the online community. This verification was shown to significantly impact both satisfaction and knowledge contribution.

The research investigating identity communication in online communities is particularly relevant to our present topic. These previous researchers have shown some of the positive outcomes that result from users being enabled to communicate their “self” to other users in technology-mediated environments. We build on these findings to explore the importance of impression management capabilities within online social networks.

In summary, individuals desire to communicate their identities to others. Online social networks provide an important channel through which individuals can manage impressions, but there exists a need to better understand the importance of impression management capabilities in determining whether users are willing and motivated to use social networks, even in the face of significant privacy risks. We thus develop a research model and propose specific hypotheses in the next section to explain users’ social network use, exploring the tension between user desires for impression management and their concerns regarding privacy.

**Theory Development and Research Model**

Our research model, shown in Figure 1, merges concepts from two streams of research. We first leverage social exchange theory to model the tension between privacy concerns and social benefits in determining social network usage patterns. We use SET further to argue that trust in the social network provider will augment the cost-benefit evaluation between privacy concerns and perceived social benefits. Finally, we propose the perceived impression management capabilities construct and theorize regarding its effects within our model. The result is a concise model that allows us to examine the unique tension between users’ desire to present themselves to others and their concerns about the privacy of the information being presented.

**Privacy Concerns Regarding Social Network Use**

*General information privacy concerns* are not specific to a particular website or company, but are instead defined as the “individual’s general tendency to worry about information privacy” (Li et al. 2011, p. 434). In most prior work, users’ privacy concerns are measured in general terms (Chellappa and Sin 2005; Dinev and Hart 2006; Li 2014; van Slyke et al. 2006). This allows for situational factors to override stated privacy concerns and influence behavior (Li et al. 2011; van Slyke et al. 2006; Wilson and Valacich 2012). Situational factors can either add to or counteract the effects of users’ general privacy concerns. A given website may evoke privacy concerns—sometimes referred to as privacy risks (Smith et al. 2011)—because of a reputation of prior privacy invasions, because the user is unfamiliar with the site (Li 2014), or, conceivably, because of poor perceived website quality. These *site-specific privacy concerns* are defined as the user’s privacy concerns about a specific website, and are significantly, positively influenced by general information privacy concerns (Li 2014). Site-specific privacy concerns, therefore, are the primary negative cost evaluated in the social exchange, and are negatively related to intentions to use the website. If an online service is successful in mitigating concerns by convincing users of the benefits of privacy disclosure, they will be more successful in encouraging use of the service (Chellappa and Sin 2005; Lu et al. 2004; Xu et al. 2009). These relationships are neither surprising nor novel, having been evaluated many times in the privacy literature (Eastlick et al. 2006; Smith et al. 2011). We replicate these relationships within our model, and hypothesize:

*H1:* Users’ general information privacy concerns will positively influence their site-specific privacy concerns.

*H2:* Users’ site-specific privacy concerns will negatively influence their intentions to use the online social network.
Perceived Social Benefits as Motivation to Use Social Networks

Goffman (1967) suggests that impression management takes place any time a person is in the presence of others. We follow this logic and extend it to the social presence afforded by social networks, thus assuming that as users communicate information about themselves within social networks, they are implicitly engaging in impression management. Framed in this way, intentions to use a social network can be at least partially explained by the traditional predictors of impression management behavior. Leary and Kowalski (1990) suggest that people are motivated to engage in impression management in order to derive social benefits. Social benefits derived from self-presentation of identities, then, are the key motivator within our SET-based model. Social benefits for projecting one’s identity can include approval, friendship, assistance, power, and so forth (Leary and Kowalski 1990).

In the context of social networks use, one can easily see how perceived social benefits constitute a primary motivation for use of these networks. For example, a Facebook user might carefully post a steady stream of humorous statements for his friends to view, intending to project the impression that he is funny, likable, and so on. Likewise, a user may limit her social networking posts to only those that imply she is a model student who constantly studies and achieves high grades in all her classes. It is quite possible that much, if not most, of individuals’ use of a social network is derived from the perceived social benefits available to users through social network use.

In summary, SET (Blau 1964) proposes that individuals engage in relationship-promoting activities in anticipation of expected intangible benefits (Gefen and Ridings 2002). These perceived benefits are weighed against potential costs, and the individual will engage in the activity if he or she perceives a net benefit. Assuming that social network use is a primarily social activity, we can thus hypothesize that:

\[ H_3: \text{A user’s perceived social benefits from using a social network will positively affect the user’s intentions to use the social network.} \]

Trust in the Social Network Provider

Research has shown that trust provides a foundation for effective online marketplace exchanges (Ba and Pavlou 2002; Pavlou and Dimoka 2006; Pavlou and Gefen 2004) and is an important precursor to the formation of behavioral intentions to engage in online shopping (Gefen et al. 2003) and social network
use (Shin 2010). Specifically in the context of social networks, trust has been identified as an important antecedent to social network usage (Krasnova et al. 2010; Posey et al. 2010). Following prior research (Dinev and Hart 2006; Krasnova et al. 2010), we define trust in terms of a belief that another party possesses characteristics that inhibit it from engaging in opportunistic behavior (Harrison McKnight et al. 2002; McKnight et al. 2002). Applied within our context, trust in the social network provider refers to the user’s belief that the social network provider is honest, trustworthy, and will act in the user’s best interest.

We position trust as a key predictor of site-specific privacy concerns. Prior research indicates that consumers who trust a firm are less concerned about their privacy in dealing with that firm (Belanger et al. 2002; Schoenbachler and Gordon 2002). SET (Blau 1964) argues that trust serves to reduce the costs of social interactions (Metzger 2004), and building trust is thus an effective strategy for mitigating privacy concerns (Milne and Boza 1999; Smith et al. 2011). Users who trust that the social network provider will not act opportunistically with the information they provide will be less concerned about their privacy when interacting with the social network. We thus hypothesize:

\[ H_{4a}: \text{Users' trust in the social network provider will negatively influence their site-specific privacy concerns}. \]

Trust in the social network provider should also impact users’ expectations for social benefits from using the service. We again find support for this claim in SET (Blau 1964), wherein trust is found to fortify exchange relationships, reduce uncertainty, and increase the benefits of a given exchange. As noted, the role of trust in reducing uncertainty has been shown in other contexts (Ba and Pavlou 2002; Pavlou and Gefen 2004), and SET clearly argues that when uncertainty or ambiguity in a social exchange is reduced, the benefits from that exchange are perceived as more likely (Blau 1964). In our social network context, when users can trust the social network provider to act in the users’ best interest, their expectations of connecting with friends, feeling companionship, receiving recognition, etc. are more certain. Accordingly, we hypothesize:

\[ H_{4b}: \text{Users' trust in the social network provider will positively influence their perceived social benefits}. \]

**Impression Management Capabilities**

Individuals perceive themselves as embodying certain traits, values, abilities, and interests—in short, an identity. This identity is constructed from experiences and from reflections on those experiences (Reeve 2005). People also have a need for uniqueness (Fromkin 1970). Thus, representing the unique attributes that make up oneself is a primary goal in self-presentation (Goffman 1959). Self-verification theory (Swann 1983) suggests that people want to be known and understood by others. People are motivated to maintain their identities, project those identities to others (e.g., Lecky and Taylor 1945; Secord and Backman 1965), and actively solicit friends and acquaintances to confirm their identities (Swann et al. 2004).

The presentation of self via technology has been seen in a number of contexts. Personal Web pages have been labeled as an effective medium for self-expression (Döring 2002). Likewise, customizable signatures (Blanchard and Markus 2004) and self-selected avatars (Nowak and Rauh 2005) in online communities are another form of communication of the user’s identity. Impression management has been shown to be a relevant activity in both online dating sites (Ellison et al. 2006) and online social networks (Krämer and Winter 2008; Lee et al.). In our social network context, an example of identity communication is the ability of a user to create and manage his profile on an online social network (e.g., select a profile picture, decide what to post and how often, remove unwanted comments or photo tags, etc.).

These features support the user in communicating his identity to other users, as well as in managing that identity (i.e., engaging in impression management). Such capabilities—which we label as perceived impression management capabilities—should have two positive impacts within our model. First, when an individual’s identity is successfully communicated to others, the individual feels known, connected, and identifies with the other individuals (Swann 1990; Swann and Ely 1984; Thatcher and Greer 2008). As noted above, prior research has presented social benefits as a key motivation for impression management behavior, and individuals self-present in order to obtain approval, friendship, assistance, power, and so forth (Leary and Kowalski 1990). This suggests that if users perceive greater impression management
capabilities in an online social network service, they will have higher expectations for the social benefits associated with using the social network service. Accordingly, we hypothesize:

\[ H_{5a}: \text{Perceived impression management capabilities of an online social network will positively influence users' perceived social benefits.} \]

Second, since individuals generally have a desire to communicate their identities and manage the impressions they are providing (Swann et al. 2004), perceived impression management capabilities should also directly impact users’ intentions to use the social network. As users feel that they are more able to engage in impression management using a given social network service, we predict that their usage patterns will increase. This claim suggests our final hypothesis:

\[ H_{5b}: \text{Perceived impression management capabilities of an online social network will positively influence users’ intentions to use the social network.} \]

**Methodology**

The model was tested with Facebook users recruited from undergraduate courses at a large university in the United States. Student subjects are appropriate for this context, since they are heavy users of the Internet and social media (Jones 2009).

**Measurement**

Wherever possible, measures were adapted from prior research. Measures for motivation to use a social network were operationalized as one’s intentions towards continued use, and were adapted from Kim et al. (2008). Measures for perceived social benefits were adapted from (Jin et al. 2010) and those for site-specific privacy concerns from (Li 2014). General information privacy concerns were measured using items from (Smith et al. 1996), and trust in social network provider using items from (Krasnova et al. 2010). Measures for perceived impression management capabilities were developed for this study. The development procedure followed prior literature on scale development procedures (MacKenzie et al. 2011), including conceptual definition, measure development, and refinement through pilot-testing. The measurement items are included in Table A1 in Appendix A. In addition to the constructs found within our theoretical model, we also included measures of various demographic variables, such as age, sex, and ethnicity, to be included as control variables.

**Analysis and Results**

In this section, we detail the pre-analysis and data validation procedures undergone to establish construct validity and reliability of the measurement items used. After establishing these necessary pre-conditions, we proceed to evaluate the proposed model using structural equation modeling (SEM). All data validation and model testing was completed in R (R Core Team 2014) using the lavaan SEM package (Rosseel 2012).

**Sample Characteristics**

The sample consisted of 244 usable responses (after filtering out incomplete responses and several participants who either missed attention-checking questions or were not Facebook users). This sample was 62% male, 77% Caucasian, and nearly all (96%) reported English as their primary language. They were young adults \((M_{\text{age}} = 21.4, \ SD = 2.0)\) in their first few years of college \((M_{\text{Yrs\ College}} = 3.16, \ SD = 1.47)\). The participants were heavy users of Facebook; over 69% reported having more than 400 Facebook friends, and 69% reported that they spend at least 30 minutes a day using Facebook.

**Establishing Construct Validity**

A first step in establishing factorial validity is to determine which constructs are formative and which are reflective (Diamantopoulos and Winklhofer 2001). Previous methodologists have suggested examining how constructs were formed and validated in other literature and modeling constructs accordingly (Cenfetelli and Bassellier 2009; Diamantopoulos and Winklhofer 2001; Petter et al. 2007). Following these guidelines, we note that all measures adapted for this study have been previously modeled and...
measured as reflective, first-order constructs (Jin et al. 2010; Kim et al. 2008; Krasnova et al. 2010; Li 2014; Smith et al. 1996). Measures developed for this study were likewise theorized and intended as reflective measures. We thus follow prior literature and validate the measures using guidelines established for reflective construct measurement.

The next step in the pre-analysis was to establish factorial validity and the reliability of the measures used. Since most constructs and many relationships hypothesized in the model are derived from prior literature, we chose to use confirmatory factor analysis (CFA) to validate the measurement model. CFA is appropriate in situations where strong theory suggests known relationships among the indicators and their intended factors (Brown 2006), as in our case. Upon fitting the proposed measurement structure of the model, measurement items that loaded poorly onto their respective factors and reduced reliability were dropped. The refined model exhibited acceptable fit to the data (Chi-sq = 207.42, df = 153, p = 0.002, Chi-sq/df = 1.36, CFI = 0.98, TLI = 0.97, RMSEA = 0.038, SRMR = 0.043). Satisfied that the model was a good fit to the data, we could then calculate correlations, reliabilities, and AVEs to further aid in establishing factorial validity. These metrics are summarized in Table 1.

<table>
<thead>
<tr>
<th>Construct Name</th>
<th>CR</th>
<th>AVE</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General privacy concerns</td>
<td>.735</td>
<td>.581</td>
<td>.763</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Perceived IM capabilities</td>
<td>.859</td>
<td>.551</td>
<td>.170</td>
<td>.742</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Trust in social network provider</td>
<td>.875</td>
<td>.609</td>
<td>.024</td>
<td>.316</td>
<td>.780</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Perceived social benefits</td>
<td>.771</td>
<td>.531</td>
<td>.072</td>
<td>.485</td>
<td>.301</td>
<td>.729</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Site-specific privacy concerns</td>
<td>.727</td>
<td>.585</td>
<td>.469</td>
<td>-110</td>
<td>-221</td>
<td>-029</td>
<td>.765</td>
<td></td>
</tr>
<tr>
<td>6. Intentions to use Facebook</td>
<td>.827</td>
<td>.720</td>
<td>-035</td>
<td>.553</td>
<td>.396</td>
<td>.584</td>
<td>-192</td>
<td>.849</td>
</tr>
</tbody>
</table>

In order to demonstrate factorial validity, the average variance extracted (AVE) for a construct should be > 0.5 (convergent validity) (Hair et al. 2010). In addition, discriminant validity is demonstrated when the square root of a construct’s AVE is higher than the correlation between that construct and all other constructs in the model (Hair et al. 2010). As shown in Table 1, the constructs in the model meet all of these criteria. To establish reliability, the composite reliability value should be 0.7 (Fornell and Larcker 1981; Kock 2010; Nunnally and Bernstein 1994). The computed reliability values shown in Table 1 indicate sufficient reliabilities.

### Evaluating Common-Methods Bias

Because all survey items were measured using the same method (an online survey), the possibility exists that some of the shared variance among the constructs is due to the common method rather than the underlying relationships among the constructs. Though precautions were implemented to reduce this likelihood (e.g., randomizing the order of survey items) (Straub et al. 2004), it is necessary to test for common-methods bias in the measurement model. We first note that no correlations shown in Tables 2 and 3 are above 0.90. Correlations above this threshold may indicate a common-methods bias (Pavlou et al. 2007). A more stringent approach to testing common-methods bias is the common latent factor method (Podsakoff et al. 2003), wherein the influence of a common latent “method” factor on each individual indicator is modeled, noting any large changes to the loading of each indicator on its corresponding construct. If “large” changes (i.e., > 0.2) are observed, the method factor is retained in the structural model in order to remove the method’s influence from the estimated parameters in the structural model (Podsakoff et al. 2003). Upon adding the common method factor to the measurement model, no changes in standardized item loadings larger than 0.05 in magnitude were observed. We thus conclude that the common method used for measurement did not significantly impact our results.

Having established the validity and reliability of the constructs measured, we now proceed to describe the SEM analysis of the full model.
Model Testing Results

We tested the theoretical model shown in Figure 1 using SEM. Fitting the structural model to the data produced generally acceptable indications of fit (Chi-sq = 247.31, dfModel = 196, p = 0.008, Chi-sq/df = 1.26, CFI = 0.98, TLI = 0.97, RMSEA = 0.033, SRMR = 0.051) (Hair et al. 2010). We also included sex (female = 1) and age as control variables predicting both site-specific privacy concerns and intentions to use the social network. Only significant paths from the control variables were retained in the final model, which is shown in Figure 2 with model testing results. Hypothesized relationships shown in the theoretical model in Figure 1 were tested in conjunction with the SEM analysis. The tested hypotheses, along with their corresponding path estimates and significance levels, are summarized in Table 2.

Table 2. Hypothesis Testing Results

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Path Est.</th>
<th>Support?</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1. General privacy concerns (\rightarrow) Site-specific privacy concerns</td>
<td>.437***</td>
<td>Yes</td>
</tr>
<tr>
<td>H2. Site-specific privacy concerns (\rightarrow) (-) Intentions to use social network</td>
<td>-.144*</td>
<td>Yes</td>
</tr>
<tr>
<td>H3. Perceived social benefits (\rightarrow) Intentions to use social network</td>
<td>.324***</td>
<td>Yes</td>
</tr>
<tr>
<td>H4a. Trust in social network provider (\rightarrow) (-) Site-specific privacy concerns</td>
<td>-.274***</td>
<td>Yes</td>
</tr>
<tr>
<td>H4b. Trust in social network provider (\rightarrow) Perceived social benefits</td>
<td>.219**</td>
<td>Yes</td>
</tr>
<tr>
<td>H5a. Perceived IM capabilities (\rightarrow) Perceived social benefits</td>
<td>.409***</td>
<td>Yes</td>
</tr>
<tr>
<td>H5b. Perceived IM capabilities (\rightarrow) Intentions to use social network</td>
<td>.234**</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Notes: *** = significance at \(p < .001\); ** = significance at \(p < .01\); * = significance at \(p < .05\).

Discussion

This research addressed the following question: how does a social network’s ability to support impression management counterbalance the potential privacy concerns of social network use? Our
model summarizes relationships among privacy, trust, perceived social benefits, and perceived impression management capabilities. As several of these constructs have been tested previously, the key contribution of this research is our positioning of perceived impression management capabilities as a primary driver of both perceived social benefits and usage intentions. As such, a network’s ability to fulfill users’ needs regarding creating and presenting their identities has been positioned as a key counterweight in the tension between privacy concerns and benefits available from use of the online social network. This section includes an overview of the model testing results, implications for research and practice, as well as limitations and future research.

User privacy concerns and trust in the social network provider were found to play an important role in the model. As predicted, general privacy concerns significantly influenced site-specific privacy concerns (H1), and these, in turn, negatively influenced users’ intentions to use the social network (H2). A user’s trust in the social network provider exhibited a negative effect on site-specific privacy concerns (H4a) and a positive effect on the perceived social benefits of using the social networking site (H4b).

In addition, the model hypothesized several facilitators of social network use. First, a key positive predictor of users’ intentions to use the social network was the perceived social benefits from using that social network (H3). Our newly introduced construct, perceived impression management capabilities, also played an important part in explaining usage intentions. This construct had significant, positive influences on both perceived social benefits (H5a) and intentions to use the social network (H5b). Figure 2 and Table 2 provide the tested research model and a summary of the hypothesis testing results, respectively.

Implications for Research

This paper contributes to the privacy literature by providing theoretical justification for the effects of trust in online interactions. Using SET, we proposed that trust would both decrease site-specific privacy concerns and increase perceived social benefits. The outcome that trust is negatively correlated with privacy concerns is not surprising, and indeed supports prior findings (Belanger et al. 2002). The nomological position of trust within prior privacy research is debated in the literature with conflicting opinions (Smith et al. 2011); some authors model trust as antecedent to privacy concerns and others model trust as an outcome of privacy. Our model uses established theory (SET) to position trust as an antecedent to privacy concerns and perceived benefits. The model testing results provide important empirical evidence that informs this ongoing debate.

We also provide compelling evidence that perceived social benefits—especially those derived from the social network’s ability to support impression management—play an important role in counterbalancing potential privacy concerns in determining social network use. Theory surrounding perceived social benefits in the context of privacy is relatively scarce. This may be partially due to the IS discipline’s heavy focus on the e-commerce context, where social benefits are not as relevant as other benefits such as convenience or cost savings (Smith et al. 2011). Our model indicates the importance of social benefits in the social network context. We further provide two important ways in which perceived social benefits are generated. Trust in the social network provider serves to increase the perceived benefits of socially engaging via the social network. Impression management capabilities provided by the social network also predict higher perceived social benefits. Our results thus constitute a significant contribution to our limited understanding of perceived social benefits and trust in the context of privacy.

The key contribution of this paper is the evaluation of a novel construct, perceived impression management capabilities, on users’ intentions to participate in online social networks. Leveraging strong social psychology theory, this work builds on recent theoretical work (Wilson et al. 2014) to empirically test the concept of impression management capabilities and theorize regarding their role in online social networks. Though several recent studies have examined the motivations driving the use of online social networks (Ganley and Lampe 2009; Khan and Jarvenpaa 2010; Krasnova et al. 2010; Lu and Hsiao 2010; Posey et al. 2010) and others have examined impression management behavior in online social networks (Krämer and Winter 2008), relatively little prior research has explored the use of these networks as fulfilling users’ need for expressing themselves and engaging in impression management, particularly in the context of privacy concerns. Our model testing results indicate that impression management is a key function of online social network use, and an important counterbalance against users’ concerns about the
privacy of their personal information. These networks clearly constitute an important channel for communicating about one’s identity, and there remains much to learn about what motivates users to use these networks to engage in impression management. Future work can build on these unique concepts for further insights into the mechanisms surrounding personal use of social networks.

**Implications for Practice**

This research also has practical implications for online businesses and social network providers. First, privacy concerns and trust play an important role in how users perceive and interact with social networks. It is critical that developers of social networks recognize these key factors and identify ways of fostering trust and mitigating user concerns. For example, Facebook has often been criticized for implementing privacy controls that are difficult to access and cumbersome to use. Leveraging human-computer interaction best practices in an effort to optimize the design of social network interfaces may yield increased site adoption rates by Internet users who place a high priority on privacy controls. Additionally, this research suggests that a user’s age influences privacy concerns within the context of social network use. Developers of social networks may choose to include additional information on how user privacy is ensured for specific demographic groups.

Second, many online businesses use social media as a primary marketing tool, relying on social network users to share and discuss products and services. The theory developed here highlights the importance of users’ impression management goals inherent in their use of social networks. Businesses could leverage this notion, building positive impressions, for example, into their sharing prompts (e.g., “Your clothing purchase shows that you are both sophisticated and up-to-date. Click here to share this with your friends!”). Identifying ways of converging the corporate goals of increasing revenue and the user goals of having control over the image that they are projecting to followers should serve to facilitate both a robust commercial presence and an active user base in social networking sites.

Third, given the social motives embedded within social network usage behavior, impression management capabilities could be a key function that social network providers should seek to develop. As an example, a social network could provide its users more granular feedback regarding who is viewing their profile and to what extent (e.g., “Who knew that people were so frequently viewing that picture of me in my bath robe?”). Allowing users more control over the impressions they are making within their network could be an important facilitator of more extensive social network use.

**Limitations and Future Research**

This research was conducted as an exploratory, theory-building exercise; it employed a single method to collect data with a student sample. The subjects in our sample are clearly in the population of interest as all participants reported using Facebook; however, students are in many ways a homogenous group, which may limit the generalizability of the findings. A study investigating the reasons why Americans participate in social networks reports that out of 2,277 adults, roughly two-thirds have a presence on a social networking site (Smith 2011). Clearly, students are not the only participants operating in the social-networking space, and statements about the causal relationships presented in this model should be interpreted with caution. Exploring the totality of impression management behavior occurring within the demographically diverse population of social network users should be an objective of future research.

Our research is also limited to behavior occurring within a single online social network (Facebook.com). While Facebook is the most popular social network (Pew Research Center 2013a), and therefore deserving of our focus, these findings may not generalize to other social networks. LinkedIn, for example, is a popular social network designed primarily for professional networking, and privacy concerns and especially impression management behaviors may be very different in that context. Future research should investigate these relationships in other social networks to develop further insights.

Lastly, the nomological net tested in this analysis likely excludes relevant constructs that account for portions of the unexplained variance in the research model. For example, the perceived impression management capabilities construct was operationalized to explore users’ perception of how effective a social network is as a platform for impression management. However, impression management
capabilities could also be measured by investigating myriad human-computer interaction factors, including the design, aesthetics, and ease of use of the interface for a given social network. Expanding the scope of this work to account for additional factors that may influence impression management capabilities and intentions to use social networking sites is an opportunity for future research.

Another potential area for expansion of the research model relates to our operationalization for several other concepts. First, this study used a high-level operationalization of perceived social benefits, and future work could more specifically investigate social benefits that are especially relevant in social networks in the context of impression management (Lee et al. 2013). We have also limited our measurement of trust to trust in the social network provider, and future work could also investigate perceived trust in one’s network peers as a possible predictor of privacy concerns and perceived social benefits. Lastly, we included a limited subset of potential control variables (limited to demographic characteristics of the users). Other relevant control variables include personality traits (e.g., social anxiety or public self-consciousness), and these may be a topic of interest for future research in this area.

Conclusion

This research uses Social Exchange Theory (Blau 1964) and the impression management literature (Goffman 1959; Leary and Kowalski 1990) to examine how privacy concerns can be counterbalanced by the perceived social benefits afforded by a social network’s ability to support impression management. We frame social network use as an attempt to engage in impression management, and we highlight the importance of a social network’s impression management capabilities in predicting social benefits from, and use of, a social network. We test our model with a sample of 244 Facebook users, finding strong support for the proposed relationships. Our theory has important implications for researchers interested in privacy issues within social networks. Social network providers can also benefit from this research, as our findings indicate the importance of enabling impression management within a social network.
## Appendix A: Measurement Items

<table>
<thead>
<tr>
<th>Construct</th>
<th>Code</th>
<th>Items</th>
<th>Composite Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>General information privacy concerns</td>
<td>GIPC1</td>
<td>All things considered, the Internet would cause serious privacy problems.</td>
<td>.735</td>
</tr>
<tr>
<td>(Smith et al. 1996)</td>
<td>GIPC2</td>
<td>Compared to others, I am more sensitive about the way online companies handle my personal information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GIPC3</td>
<td>To me, it is the most important thing to keep my privacy intact from online companies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GIPC4R</td>
<td>I believe other people are too concerned with online privacy issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GIPC5</td>
<td>Compared with other subjects on my mind, personal privacy is very important.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GIPC6</td>
<td>I am concerned about threats to my personal privacy today.</td>
<td></td>
</tr>
<tr>
<td>Intentions to use social network</td>
<td>INT1</td>
<td>I intend to use Facebook in the future.</td>
<td>.827</td>
</tr>
<tr>
<td>(Kim et al. 2008)</td>
<td>INT2</td>
<td>I intend to recommend my friends to use Facebook in the future.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>INT3</td>
<td>The next website I visit will probably be Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>INT4</td>
<td>I’d like to use Facebook soon.</td>
<td></td>
</tr>
<tr>
<td>Perceived impression management</td>
<td>PIMC1</td>
<td>Using Facebook, I can accurately express my identity.</td>
<td>.859</td>
</tr>
<tr>
<td>capabilities (Developed for this study)</td>
<td>PIMC2</td>
<td>Using Facebook, I can portray the image I want.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIMC3</td>
<td>Using Facebook, I am able to present myself in the way that I want.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIMC4</td>
<td>Using Facebook, I can adequately convey information about who I am.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIMC5</td>
<td>Using Facebook, I am able to project my desired identity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIMC6</td>
<td>Using Facebook, others will view me in the way that I want.</td>
<td></td>
</tr>
<tr>
<td>Perceived social benefits</td>
<td>PSB1</td>
<td>The friendship aspect of my relationship with the other members of Facebook is important to me.</td>
<td>.771</td>
</tr>
<tr>
<td>(Jin et al. 2010)</td>
<td>PSB2</td>
<td>I enjoy spending time with the members of Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSB3</td>
<td>I value the close, personal relationship that I have with the members of Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSB4</td>
<td>I feel that I connect socially with my friends through Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSB5</td>
<td>Facebook allows me to feel socially included.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSB6</td>
<td>I would feel disconnected from my friends if I lost access to Facebook.</td>
<td></td>
</tr>
<tr>
<td>Site-specific privacy concerns</td>
<td>SSPC1</td>
<td>I am concerned that Facebook is collecting too much information about me.</td>
<td>.723</td>
</tr>
<tr>
<td>(Li 2014)</td>
<td>SSPC2R</td>
<td>It does not bother me when Facebook asks me for personal information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSPC3</td>
<td>I am concerned about my privacy when Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSPC4R</td>
<td>I have no doubts about how well my privacy is protected on Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSPC5</td>
<td>My personal information could be misused when transacting with Facebook.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSPC6</td>
<td>My personal information could be accessed by unknown parties when transacting with Facebook.</td>
<td></td>
</tr>
<tr>
<td>Trust in social network provider</td>
<td>TSP1</td>
<td>Facebook is open and receptive to the needs of its members.</td>
<td>.875</td>
</tr>
<tr>
<td>(Krasnova et al. 2010)</td>
<td>TSP2</td>
<td>It makes good-faith efforts to address most member concerns.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TSP3</td>
<td>It is also interested in the well-being of its members, not just its own.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TSP4</td>
<td>It is honest in its dealings with me.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TSP5</td>
<td>It keeps its commitments to its members.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TSP6</td>
<td>It is trustworthy.</td>
<td></td>
</tr>
</tbody>
</table>
References


Facebook: Privacy Concerns, Social Benefits, and Impression Management


Social Media and Digital Collaborations


