How People Protect Their Privacy on Facebook: A Cost-Benefit View

Arun Vishwanath
Department of Communication and Management Science & Systems, University at Buffalo (UB), Buffalo, NY 14260 USA. E-mail: avishy@buffalo.edu

Weiai Xu
Department of Communication and Management Science & Systems, University at Buffalo (UB), Buffalo, NY 14260 USA

Zed Ngoh
Department of Communication and Management Science & Systems, University at Buffalo (UB), Buffalo, NY 14260 USA

Realizing the many benefits from Facebook require users to share information reciprocally, which has overtime created trillions of bytes of information online—a treasure trove for cybercriminals. The sole protection for any user are three sets of privacy protections afforded by Facebook: settings that control *information privacy* (i.e., security of social media accounts and identity information), *accessibility privacy* or anonymity (i.e., manage who can connect with a user), and those that control *expressive privacy* (i.e., control who can see a user's posts and tag you). Using these settings, however, involves a trade-off between making oneself accessible and thereby vulnerable to potential attacks, or enacting stringent protections that could potentially make someone inaccessible thereby reducing the benefits that are accruable through social media. Using two theoretical frameworks, Uses and Gratifications (U&G) and Protection Motivation Theory (PMT), the research examined how individuals congitvely juxtaposed the cost of maintaining privacy through the use of these settings against the benefits of openness. The application of the U&G framework revealed that social need fulfillment was the single most significant benefit driving privacy management. From the cost standpoint, the PMT framework pointed to perceived severity impacting expressive and information privacy, and perceived susceptability influencing accessibility privacy.

Received March 22, 2016; revised March 9, 2017; accepted March 31, 2017

 DOI: 10.1002/jasist.23894

Social networking platforms such as Facebook help people connect and communicate with others, form new relationships, and maintain existing ones (Shahnaz & Wok, 2011). Such relationships provide users benefits ranging from personal gratification to social support and social proof from being noticed and validated by one's friends and peers. Not surprisingly, billions of people world wide today use social media.

But the maintenance of relationships on platforms such as Facebook comes at a cost: People need to share information to receive feedback from others (Ellison, Steinfield, & Lampe, 2007). Much like in real-world relationships, virtually maintained relationships require individuals to not only post updates and share personal information but also to respond to other people's posts and updates to reciprocally receive feedback. However, unlike the real world, doing so on social media leaves trails of personally identifiable information (PII) that remain on the platform's servers. These trillions of bytes of PII, easily accessible on social media platforms, have become a treasure trove for cyber criminals.

Cyber criminals can use information posted on sites such as Facebook for impersonating someone or infiltrating their social networks and burglarizing them—as the infamous Hollywood "Bling Ring" demonstrated (Dvorak, 2001; Miller, 2012; Riley & Vance, 2012; Roche, 2011; Salkin, 2009). They can also use the information for crafting email and social media based spear phishing attacks that could be used to infect computer networks and steal PII from individual and corporate computer networks (Vishwanath, 2015). With social media sites moving into shopping, gaming, and serving as single sign-ons for other Internet services, just

access to a person's social media login and password could eventually translate to a loss of identity or a significant financial loss to a victim. Such attacks are common and some 10% of Facebook users have reported experiencing a loss of reputation, identity, or some form of monetary cost because of PII stolen from their social media accounts—a staggering statistic if we take into account the more than one billion worldwide user base on the platform. Not surprisingly, many Facebook users—86% in a 2013 Pew study—have made efforts to erase their digital footprint or taken steps to prevent individuals and organizations from observing their online behaviors (Rainie, Kiesler, Kang, & Madden, 2013).

Presently, the sole protection for any user is the privacy settings provided on Facebook. These settings can be broadly classified into three dimensions: settings that control *information privacy* (i.e., protect who can see a user's identity profile and access a user's digital account), settings that control *accessibility privacy* (i.e., manage who can connect with a user), and those that control the user's *expressive privacy* (i.e., control who can manage content related to a user's social image). Using these settings on Facebook, however, involves a trade-off between making oneself accessible and thereby vulnerable to potential attacks and unwanted attention, or enacting stringent protections that could reduce social, information, and entertainment benefits from social media use. Thus, as individuals utilize these Facebook settings, they need to cognitively juxtapose the cost of maintaining privacy against the benefits of openness. These cognitive processes reveal not only how people think about risk on social media but also how they react to various risk scenarios. Knowing this is key to developing usable security, where the focus of extant scholarship has been on designing easy-to-use security settings based on assessments of *how* people use security (Braz, Seffah, & M'raihi, 2007) rather than based on *why* people use security settings in certain ways. Explicating the underlying cognitive cost-benefit appraisal processes that lead individuals to enact different privacy protections is thus the central goal of the current article.

A theory that provides an assessment of cognitive cost appraisals is Protection Motivation Theory (PMT; Rogers, 1975). PMT proposes that people protect themselves from risks based on four factors: perceived severity (how adverse is the consequence of a risk), perceived susceptibility (the likelihood of the risk), response efficacy (how effective one believes the protective measures are to prevent the risk), and self-efficacy (how much confidence one has to adopt the protective measures on their own) (Rogers, 1975). These four factors have been positively linked to enactment of protective behaviors (Witte, 1992), thusly providing a means for relating the users' cognitive appraisal of the cost of a cyber breach to the enactment of various privacy protections on Facebook.

A framework that is well-suited to assessing the perceived benefits of using media is Uses and Gratifications (U&G). U&G posists that a finite number of gratifications sought drive the use of a medium (Sundar & Limperos, 2013; Vishwanath, 2008). These include social, information, entertainment, emotional, and escape needs (Sundar & Limperos, 2013)—all of which have been linked to the utilization of Facebook. Thus, U&G based gratifications sought from Facebook provide a means for relating the perceived benefits from using Facebook to the enactment of various privacy protections on Facebook.

Using these two theoretical frameworks, the current study examines the degree to which perceived costs enhance protection and perceived benefits foster a relaxation of the three available privacy settings on Facebook. The data for the study come from a cross-sectional survey of college students, an important demographic of social media users as well as frequent targets of cyber criminals. The article begins with an exposition of the two theoretical frameworks followed by the methods, measures, findings, and discussion of results in ensuing sections.

Theoretical Premise

Three Dimensions of Facebook Privacy

At its broadest level, privacy is a protection that people enact to selectively control others' access to themselves (Altman, 1975; Westin, 1967). In the real world privacy management involves the control of interpersonal boundaries to reduce discrepancies between one's desired and actual levels of privacy (Altman, 1975). To control this boundary, people take cognitive ownership of their private information and consider information to be private when individuals believe that the information belongs to them (Petronio, 2002). In the real world, private information is often implicitly protected by mutually understood, unwritten, and normative cognitive rules of sharing (e.g., anything personal you tell your friend is expected to be kept private) and through explicit legal guarantees (e.g., anything personal you reveal to your therapist is legally protected). In social media, however, these rules have to be actively managed by the individual through the use of the privacy management settings provided by platforms such as Facebook.

The privacy management settings Facebook affords can be broadly categorized using the classification proposed by DeCew (1997) into information privacy, accessibility privacy, and expressive privacy. These categories, although built prior to the advent Web 2.0, where the boundaries between private and public information is increasingly blurred, provide a convenient framework for dilenating the different privavy settings Facebook affords.

Information privacy focuses on the control of access to one's digital information. This includes user-disclosed information on Facebook, such as name, gender, residence, birth date, employment and education history, contact information and relationship status, which collectively constitute one's social identity. Social identity is further linked to one's private and economic life and a breach of this data could lead to serious issues such as identity theft and online harassment. As discused, a hacker with access to these pieces of digital information could easily steal an user's identity, open

DOI: 10.1002/asi

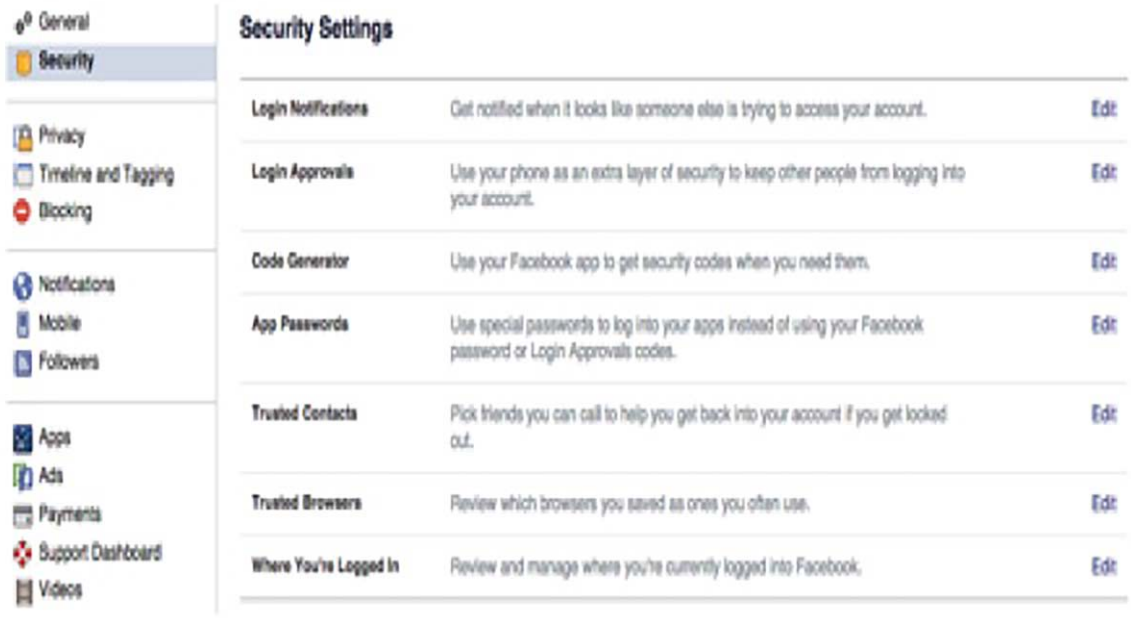

FIG. 1. Screen shot of Facebook's security settings. [Color figure can be viewed at wileyonlinelibrary.com]

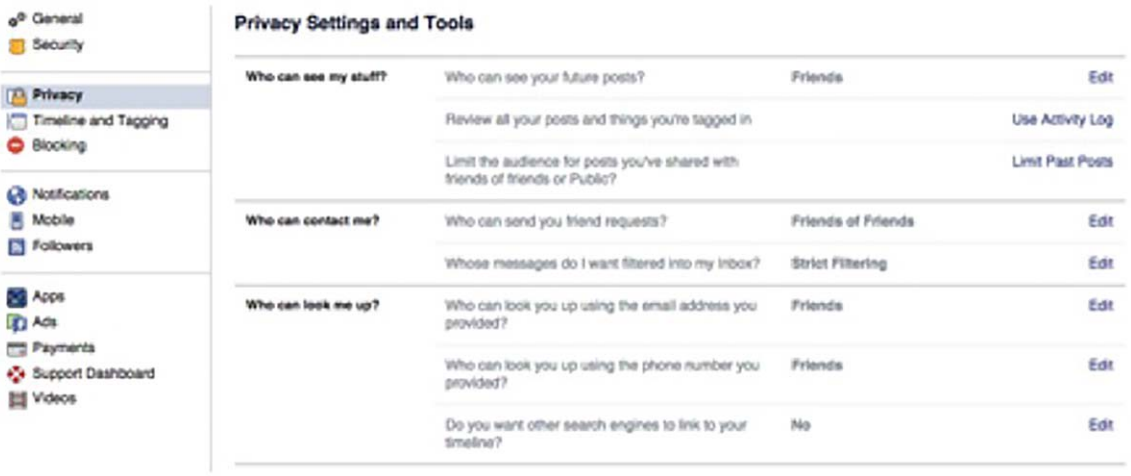

FIG. 2. Screen shot of Facebook's privacy settings and tools. [Color figure can be viewed at wileyonlinelibrary.com]

credit cards, or procure access to other online accounts. The protection measure available to control access to this information on Facebook can be found it Security Settings" (Figure 1), which monitors login information and notifies users of suspicious activity.

Accessibility privacy involves control over the acquisition of information that could provide access to the individual (DeCew, 1997). Accessibility privacy focuses on the access to individuals rather than their private information (i.e., information privacy) and is premised on the idea that, at their core, individuals do not wish to be found or disturbed by others. This presumption corresponds to Westin's (1967) classical privacy theory that emphasizes solitude, intimacy, anonymity, and reserve. On Facebook, accessibility privacy involves managing how one is found on the platform. To be found by your friends and acquaintances is, on one hand, a necessary step toward realizing any of the rewards from social media, but on the other hand, being found makes users' easier targets of phishers and scammers who can utilize these accessible pieces of personal information to craft attacks. For instance, merely being searchable on social media makes it possible to target the user with a phony friend-request, a common type of social network-based phishing attack where the attacker impersonates another person and attempts to friend the user or sends a malware-laden message through the platform. To protect one's anonymity, Facebook's Privacy Settings and Tools (Figure 2) help users control who can find them using email or phone numbers, as well as who can send them private messages and friend-requests.

DOI: 10.1002/asi

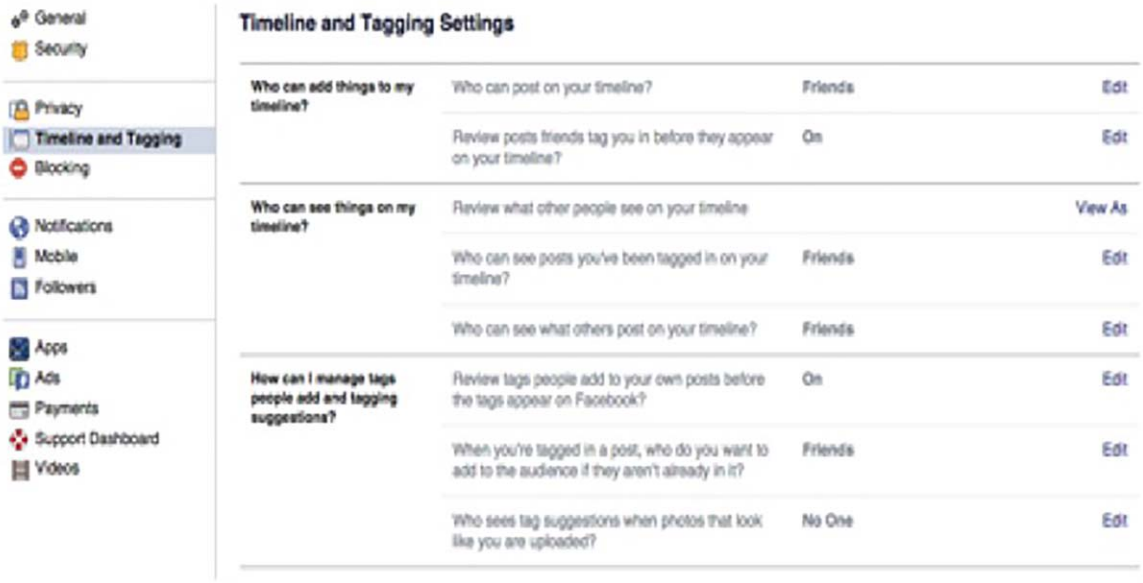

FIG. 3. Screen shot of Facebook's timeline and tagging settings. [Color figure can be viewed at wileyonlinelibrary.com]

Expressive privacy involves control over how one expresses one's self-identity or personhood through speech or activity (DeCew, 1997). Self-disclosure on social media is, in some ways, similar to public performances, as described by Goffman (1959), where individuals control or guide the formation of impressions by altering one's appearance or manner. Like these on-stage performances, Facebook users maintain desired impressions based on different times, audiences, or situations. However, the audiences on Facebook are large, diverse, and reflect overlapping social spheres (Joinson, Houghton, Vasalou, & Marder, 2011). Consequently, norms and expectations differ across these social spheres, necessitating a tailoring of online sharing to accommodate these disparate audiences. Users can manage their social image by selective self-presentation, or by controlling other-provided information that could affect one's social image (e.g., photo tags and comments from a user's friends). Undesired audiences and a loss of control over one's social image could result in damaged reputations (Debatin, Lovejoy, Horn, & Hughes, 2009). The control of one's social image on Facebook is enacted through the Timeline and Tagging Settings (Figure 3), which manages who can add to a user's timeline, see posts on a timeline, or add tags.

The enactment of these three sets of Facebook privacy settings are based on a cognitive assessment of the costs of ostensibly getting hacked, breached, or maligned against the many benefits that could accrue from being available, accessible, and reciprocally active on social media. The likely costs that drive the enactment of Facebook's privacy protections are examined next using PMT.

Protection Motivation Theory on Facebook Privacy

PMT was first introduced by Rogers (1975) to explore the effects of fear appeal messages on persuasion. This framework describes four factors that are cognitively processed when a threat is presented: perceived severity, perceived susceptibility, response efficacy, and self-efficacy (Rogers, 1975). Perceived severity and perceived susceptibility represent threat appraisal, whereas response efficacy and self-efficacy represent coping appraisal (Rogers, 1983). These appraisals involve personal considerations of the breadth and scope of the threat and the individuals capability of being able to deal with it. Thus, together, they signify the costs associated with a perceived risk or threat.

PMT predicts that people are most likely to adopt recommended protective behaviors when they believe that the associated costs from it is likely to be high, that is, the threat is serious, that they are susceptible to it, and that they can execute these behaviors on their own and these enacted behaviors can prevent the risk (Rogers, 1983). The theory has been successfully applied to explain the enactment of a wide range of personal health-related behaviors (Floyd, Prentice-Dunn, & Rogers, 2000), including the prevention of adolescent drug trafficking (Wu, Stanton, Li, Galbraith, & Cole, 2005), improving security policy compliance in organizations (Herath & Rao, 2009), and even antinuclear war behaviors (Wolf, Gregory, & Stephan, 1986). More recent research has extended it to the technology-related risk domain to study online privacy intrusion (Meso, Yi Ding, & Shuting Xu, 2013; Milne, Labrecque, & Cromer, 2009; Sangmi, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009), identity theft (Lai, Li, & Hsieh, 2012), online spying and hacking (Chenoweth, Minch, & Gattiker, 2009) and other, broad I.T. threats (Liang & Xue, 2009; Moser, Bruppacher, & Mosler, 2011).

Almost all these studies suggest an enhancement of protections in the face of increased cognitive cost and coping appraisals. Although none of this work focuses on the enactment of privacy protections on social media, they altogether provide the impetus for hypothesizing that increased cost

DOI: 10.1002/asi

and coping appraisals of risks from social media use would lead to an enhancement of the protections afforded on Facebook to control information, accessibility, and expressive privacy. This leads to the following hypotheses about the relationship between PMT based threats and the privacy protections afforded by Facebook:

H1: *User's (a) perceived severity, (b) perceived susceptibility, (c) response efficacy, and (d) self-efficacy toward unauthorized access of digital data will enhance the frequency and use of Facebook's privacy protections to control* information *privacy*.

H2: *User's (a) perceived severity, (b) perceived susceptibility, (c) response efficacy, and (d) self-efficacy toward loss of anonymity will enhance the frequency and use of Facebook's privacy protections to control* accessibility privacy.

H3: *User's (a) perceived severity, (b) perceived susceptibility, (c) response efficacy, and (d) self-efficacy toward the potential loss of social image will enhance the frequency and use of Facebook's privacy protections to control* expressive privacy.

Although PMT-based appraisals are expected to enhance protections, considerations of the perceived benefits from social media are expected to stymie the enactment of protections. The perceived benefits of Facebook are examined next using the lens provided by the Uses and Gratifications paradigm.

Uses and Gratifications (U&G) of Facebook

The U&G paradigm is an audience-centric approach that presumes people have innate needs or benefits that they seek to satisfy through the selection and use of media.

Recent applications of this paradigm have led to the discovery of a variety of gratifications driving Facebook use depending on whether the research focused on top-level gratifications or specific Facebook functionalities. For instance, Ray (2007) found three first-order drivers of Facebook use, primarily information, surveillance, and entertainment use. With a focus on specific functionalities, Raacke and Bonds-Raacke (2008) found that people use Facebook for keeping in touch with old and new friends, locating old friends and making new friends, as well as posting and looking at photos. In line with the latter approach, Joinson (2008) found seven unique U&G of Facebook including social connection, shared identities, content, social investigation, social network surfing, and status updating.

The present research focused on the first-order gratifications people derive from Facebook rather then the gratifications they derive from its individual functions. This is because Facebook's offerings are constantly evolving with technology, limiting the implications of functionality-focused research findings to the short-term. A guide to the top-level gratifications from Facebook comes from a recent exhaustive review of U&G studies from 1940 to 2011 that found media use to be driven chiefly by considerations of social, identity, information, and entertainment needs (Sundar & Limperos, 2013). These broadly map on to the three top-level gratifications made possible through Facebook use. Specially, the gratifications are: information (e.g., users can follow current events and various organizations' updates), social (e.g., make friends and keep in touch with old friends), and entertainment (e.g., play games).

Fulfilling information needs require seeking knowledge about events and people; social needs involve being abreast with the happenings around us in the social world; and entertainment needs require mood alleviating activities. Satisfying these through Facebook require a degree of openness, availability, and accessibility by other users on the platform. For instance, Facebook users' information needs can be fulfilled by subscribing to public Facebook pages' timelines, which makes a user's profile visible to the page admin and all others who follow the same page. Social needs can be fulfilled by sharing personal thoughts and activities through status updates. Finally, fulfilling entertainment needs on Facebook can be done by playing social games or shopping, which requires interaction through the site, often with strangers, that cannot be accomplished without revealing profile information. Thus, realizing the benefits of Facebook require the relaxation of the afforded privacy controls, which lead to the following hypotheses:

H4: *The perceived (a) social needs, (b) information needs, and (c) entertainment needs fulfilled by Facebook will reduce the frequency and use of Facebook's privacy protections to control* information privacy.

H5: *The perceived (a) social needs, (b) information needs, and (c) entertainment needs fulfilled by Facebook will reduce the frequency and use of Facebook's privacy protections to control* accessibility privacy.

H6: *The perceived (a) social needs, (b) information needs, and (c) entertainment needs fulfilled by Facebook will reduce the frequency and use of Facebook's privacy protections to control* expressive privacy.

Method

Participants

Data for the study were gathered using a cross sectional survey of undergraduate students enrolled in communication classes at a large Northeastern university. A total of 513 participants (57% male) responded to an IRB approved online survey over a two-week period in the fall of the 2014.

Measures

Facebook privacy protections. DeCew's (1997) dimensions of privacy can be operationalized using the three different types of setting Facebook affords for privay management: *Information privacy* can be measured based on how users manage their Facebook Security Settings; *Accessiblity privacy* can be measured based on how users manager their Facebook Privacy Settings and Tools; and

DOI: 10.1002/asi

Expressive privacy can be measured based on how users manage their Facebook Timeline and Tagging Settings. The Facebook interface affords users the ability to individually manage subsetting within each of these settings (as shown in Figures 1–3).

To measure these, individual items were developed that measured the extent to which participants were aware of the setting or their level of openeness of the setting (using a 1–5 scale, not at all aware–very aware or open to none–open to everyone) followed by the frequency with which they changed that setting (not at all frequent/infrequent–very frequently). Using these two evaluation dimensions netted a two-dimensional semantic differential measure that captured potency and intensity, which were then multipled (i.e., Potency × Intensity) to derive a weighted score. This resulted in four broad groups of users: those who were minimally aware of a setting and used it infrequently; the minimally aware frequent users; the maximally aware infrequent users; and the maximally aware frequent users. The overall scores ranged from 1–25, with scores being tied for individuals who had low awareness and high frequency (score of 5) and those who have high awareness and low frequency (score of 5) because the net effect of the two behaviours are thought to be more or less the same. That is people who don't know what they are doing and do it often might mistakenly use the wrong settings, which is the same as someone knowingly not changing their settings.[1]

Information privacy managed using Facebook's security settings. Six items measured participants' level of awareness of the protective measures that Facebook offers to prevent the loss of digital data within the Security Settings category on the interface. Sample items include "I am aware of the Secure Browsing setting" and "I am aware of the Login Notifications setting." Exploratory Factor Analysis (EFA) was conducted on the items, mean = 3.13, $SD = 0.90$, $\alpha = 0.88$. The items were weighted by the respective frequency of change response and averaged to create an index for final modeling, mean = 6.17, $SD = 3.90$.

Accessibility privacy managed using Facebook's privacy settings. Four items measured participants' level of openness toward allowing other users to contact them. Sample items drawn from Facebook's Privacy Settings read: "Who can look you up through Facebook using your email address or phone number" and "Who can send you private messages." Similarly, an EFA was conducted on the items, mean = 2.73, $SD = 0.75$, $\alpha = 0.71$. The items were weighted by the respective frequency of change response and averaged to create an index for final analysis, mean = 5.42, $SD = 3.48$.

Expressive privacy managed using Facebook's timeline and tagging settings. Six items measured participants' level of openness toward allowing other users to see their timeline or to add to it. Sample items read: "Who can see the status updates or photos you post" and "Who do you accept status updates or photo tagging requests from." An EFA was conducted on the items, mean = 3.38, $SD = 0.78$, $\alpha = 0.92$. Those items were then weighted by the respective frequency of change response and averaged to create an index for final analysis, mean = 6.42, $SD = 3.37$.

PMT Based Measures of Perceived Cost

The independent variable of PMT was measured using a Likert-type scale of 1 (*Strongly disagree*) to 5 (*Strongly agree*).

Perceived severity. Nine items measured participants' perceived level of severity toward losses from each dimension of online privacy. Sample items read: "Having my personal information or photos stolen through Facebook would be a serious problem for me" (unauthorized access of digital data), "Having people I do not know send me messages or friend requests through Facebook would be a serious problem for me" (loss of anonymity), and "Having people I do not know see my status updates or photos in Facebook would be a serious problem for me" (loss of social image). EFA was conducted on the items and two dimensions were revealed. The first dimension was related to unauthorized access of digital data, mean = 3.61, $SD = 0.87$, $\alpha = 0.85$, and items in this dimension were averaged to create an index for testing H1 and H4. The second dimension was related to loss of anonymity and social image, mean = 3.14, $SD = 0.78$, $\alpha = 0.82$, and the responses in this dimension were averaged to create an index for testing H2, H3, H5, and H6.

Perceived susceptibility. Nine items measured participants' level of susceptibility from attacks targeted at each dimension of online privacy. Sample items read: "I feel that I could be subjected to identity theft or hacking through Facebook" (unauthorized access of digital data), "I feel that people I do not know can easily send me messages or friend requests through Facebook" (loss of anonymity), and "I feel that people I do not know can easily see my status updates or photos in Facebook" (loss of social image). Again, an EFA netted two dimensions and a closer inspection of items suggested that one dimension was related to unauthorized access of digital data, mean = 3.21, $SD = 0.68$, $\alpha = 0.83$. Responses on this dimension were averaged into an index for testing H1 and H4. The other dimension was related to loss of anonymity and social image, mean = 2.91, $SD = 0.88$, $\alpha = 0.87$, and the responses in this dimension were averaged to create an index for H2, H3, H5, and H6.

[1]This premised on the idea that keeping settings unchanged leaves the user vulnerable because technology is constantly evalolving as are cyber attacks. This is precisely why settings on platforms change frequently and users are often instructed to review settings and change things like their passwords frequently. Hence, leaving things set in any one way—the proverbial "build a single big wall around a house"—does not assure protection and does not reflect how privacy settings are managed by users.

DOI: 10.1002/asi

TABLE 1. Testing H1 and H4 about protection enactment toward unauthorized access of digital data (information privacy)

	First block (PMT)		Second block (U&G)	
	β	*SE*	*β*	*SE*
Perceived severity	−.14*	.23	−.09	.22
Perceived susceptibility	.20**	.26	.13*	.25
Response efficacy	.11*	.26	.05	.25
Self-efficacy	.003	.29	.05	.27
Social needs			.43**	.25
Information needs			−.14*	.28
Entertainment needs			−.10	.25
F, Adj. R^2	*F* (7, 505) = 15.06**, .16			

* $p < .05$ (two-tailed), ** $p < .01$ (two-tailed).

TABLE 2. Testing H2 and H5 about protection enactment for loss of anonymity (accessibility privacy)

	First block (PMT)		Second block (U&G)	
	β	*SE*	*β*	*SE*
Perceived severity	.24**	.20	.19**	.19
Perceived susceptibility	.15*	.17	.08	.17
Response efficacy	.03	.23	.001	.22
Self-efficacy	−.18**	.24	−.11*	.23
Social needs			.38**	.22
Information needs			−.14*	.25
Entertainment needs			−.12*	.22
F, Adj. R^2	*F* (7, 505) = 16.70**, .18			

* $p < .05$ (two-tailed), ** $p < .01$ (two-tailed).

Response efficacy. Five items measure participants' beliefs about the extent to which Facebook's privacy settings were effective in protecting their account. Sample items read: "By changing my privacy settings, I believe that Facebook will protect my personal information or photos" and "If someone is trying to access my personal info, Facebook privacy settings are effective to prevent it." An EFA was conducted on the items before the responses were averaged to create an index, mean = 3.20, $SD = 0.75$, $\alpha = 0.89$.

Self-efficacy. Seven items measured participants' beliefs that they could manage their Facebook privacy settings on their own. Sample items read: "I believe that I have the ability to protect my personal information on Facebook" and "I feel confident that I can change my Facebook privacy settings without help from anyone." An EFA was conducted on the items before the responses were averaged to create an index, mean = 3.56, $SD = 0.73$, $\alpha = 0.91$.

U&G Based Measures of Perceived Benefits From Facebook

The independent variables of U&G were measured using a Likert-type scale of 1 (*Strongly disagree*) to 5 (*Strongly agree*). Based on prior research (Joinson, 2008; Raacke & Bonds-Raacke, 2008; Ray, 2007; Sundar & Limperos, 2013), 17 items measured participants' likely benefits from Facebook. Example items read: "I use Facebook because I can make new friends" and "I use Facebook because it diverts my attention when I am bored or stressed." An EFA conducted on the items revealed three dimensions mapping on to the three gratification dimensions explicated by prior research: social needs, mean = 2.83, $SD = 0.79$, $\alpha = 0.87$, information needs, mean = 3.35, $SD = 0.77$, $\alpha = 0.81$, and entertainment needs, mean = 3.43, $SD = 0.80$, $\alpha = 0.80$. The responses in each dimension were averaged to create an index.

Results

H1 and H4, H2 and H5, and H3 and H6, examined the relative influence of PMT based costs versus U&G based benefits, on the enactment of information privacy, accessibility privacy, and expressive privacy protections afforded by Facebook, respectively. Each set of hypotheses was tested using a hierarchical regression with PMT-based perceived costs and U&G-based benefits as independent measures, and the weighted variable measuring enactment of the respective Facebook's privacy setting as the dependent variable.

In each model, the PMT factors indicating perceived costs were entered first followed by the U&G based benfits. The rationale for this stems from a large body of cognitive research in contexts ranging from advertising to message framing that shows the salience of fear appeals and perceived losses over benefits during decision-making (Vishwanath, 2009). Thus, perceived severity and perceived susceptibility toward unauthorized access of digital data, the user's response efficacy, and self-efficacy were entered in the first block, followed by the U&G variables (i.e., social needs, information needs, and entertainment needs) in the second block.

The first model testing H1 and H4 was significant, $F(7, 505) = 15.06$, $p < 0.001$, explaining 16% of the variance in the enactment of Facebook's information privacy settings. Table 1 presents the tests. Perceived susceptibility, $\beta = .13$, $t = 3.07$, $p = .002$, positively predicted protection enactment toward digital data. In addition, social needs positively predicted protection enactment, $\beta = .43$, $t = 8.53$, $p < .001$, whereas information needs, $\beta = -.14$, $t = -2.55$, $p = .011$, negatively predicted protection enactment toward unauthorized access of digital data. Therefore, H1 and H4 were partially supported.

Next, The analysis was repeated to examine the enactment of accessibility privacy settings afforded by Facebook. Table 2 presents the results from testing H2 and H5.

The regression model was also significant, $F(7, 505) = 16.70$, $p < .001$, and explained 18% of the variance in the protection enactment. In the model, perceived severity, $\beta = .19$, $t = 4.51$, $p < .001$, positively predicted protection enactment, while self-efficacy negatively predicted protection enactment, $\beta = -.11$, $t = -2.20$, $p = .029$. Thus, H2 was partially supported. Among the U&G predictors,

DOI: 10.1002/asi

TABLE 3. Testing H3 and H6 about protection enactment for loss of social image (expressive privacy)

	First block (PMT)		Second block (U&G)	
	β	*SE*	β	*SE*
Perceived severity	.29**	.19	.24**	.19
Perceived susceptibility	.12**	.16	.06	.16
Response efficacy	.01	.22	−.03	.22
Self-efficacy	.10	.23	−.05	.23
Social needs			.31**	.22
Information needs			−.06	.24
Entertainment needs			−.07	.21
F, Adj. R^2	F (7, 505) = 13.84**, .15			

* $p < .05$ (two-tailed), ** $p < .01$ (two-tailed).

social needs positively predicted protection enactment, $\beta = .38$, $t = 7.47$, $p < .001$; protection enactment was negatively predicted by information needs, $\beta = -.14$, $t = -2.52$, $p = .012$, and entertainment needs, $\beta = -.12$, $t = -2.33$, $p = .02$). Based on the findings, H5 was partially supported.

Lastly, the model testing H3 and H6 concerning the enactment of expressive privacy protections afforded by Facebook was also significant, $F(7, 505) = 13.84$, $p < .001$, and explained 15% of the variance in privacy enactment. The results of these tests are presented in Table 3. In this model, perceived severity, $\beta = .24$, $t = 5.49$, $p < .001$, positively predicted protection enactment. From the U&G constructs, social needs, $\beta = .31$, $t = 6.002$, $p < .001$, positively predicted protection.

Discussion

The research examined the cognitive cost-benefit appraisal processes that underlie users' management of various privacy protections on Facebook. DeCew's (1997) dimensions of privacy provided a mechanism for categorizing the afforded protections. PMT provided the framework to assess users' cognitive cost appraisals while U&G provided the lens to understand the perceived benefits that drive their privacy enactments.

Based on the relative beta weights across the regressions tested, it appears that users' privacy management on Facebook is premised on the juxtaposition of benefits against cost, rather than costs versus benefits. That is, when it comes to how users manage their Facebook privacy, they focus on benefits rather than the costs.

Among the benefits, social need fulfillment was the single most significant Facebook benefit that influenced how the user managed their Facebook settings that protected their *information privacy*, *accessibility privacy*, and *expressive privacy*. Social needs, such as finding new friends, maintaining existing relationships, and getting social support, likely leads to a more active consideration of who gets access to the users digital data, who has access to the individual, and who can influence their self-presentation. Social needs also likely foster impression management and tailored self-presentation. The other benefits the drive Facebook use, information needs and entertainment needs, appear to relax the intensity of enactment of such privacy protections. This is perhaps because such benefits can be acquired by simply lurking on Facebook and looking at other people's profiles or by passively receiving feeds from others. None of these activities require the user to divulge personal information, meaning they do not require active privacy management.

Relative to the benefits, the perceived costs of social media use—the first block in our regressions— stem from the losses one could potentially incur and the effort it would take to mitigate the loss. The testing of the PMT framework pointed to perceived severity and perceived susceptibility of privacy incursions having significant impacts on privacy management. From these, perceived severity had a relatively stronger influence on the enactment of *expressive privacy* (i.e., loss of social image) and *accessibility privacy* (i.e., loss of annoymity). This is likely again a reflection of the social nature of Facebook use, where most people use the platform for self-presentation, making the fear of social losses stemming from inaccurate self-presentation or public embarrassment a bigger, more significant threat. In contrast, digital or *information privacy* losses, although important, are viewed as less impactful, perhaps because of the private way in which these costs can be incurred. For instance, the social embarrassment from a photograph that shows a user in a negative light being posted is harder to deal with privately than the loss of a password or some digital information.

These findings have several practical implications toward privacy protection behaviors on SNSs and for the design of usable security, where research tends to focus on designing easy to use and useful security settings, often ignorning the fact that not all settings are underutilized merely because of design. Most settings, it appears, are ignored because users care less about them and instead focus solely on settings that protect social information leaks. Knowing this allows for better security design and more effective communication about the benefits of various settings. Such communication could emphasize the relatedness of all security settings, connect the social implications of the loss of any of them, and explain how coping with one requires monitoring all the others. In addition, given the influence of individual level differences in coping efficacy, security desingers should develop mechanisms to communicate in a simple way the value of each setting as well as how individuals could deal with breaches that stem from the misappropriation of any setting.

However, in-line with any sample-based, social science research, the study has a few limitations, beginning with the use of a student sample. College students are an important demographic of social media users and are often targets of cyber criminals. In addition, using a homogenous sample of students gave us a fair degree of control over potential confounds stemming from differences in social media use frequency, knowledge and experience with social media, and general technological efficacy. That said, college students are also a-typical of the broader U.S. or global population of

DOI: 10.1002/asi

Internet users, which somewhat restricts the generalizability of the findings to just college age adults. Another limitation is the use of self-reports, which are subject to errors in memory as well participant biases from social disirablity to being primed by other survey items. For instance, subjects could have reported their desired privacy setting or the setting they felt the researcher was attempting to gauge. In addition, students could ostensibly be more aware of privacy, perhaps because of being warned about it in class, leading to their use of more restricted settings.

Yet another limitation is the treatment of the three different privacy settings afforded by the Facebook interface as independent dimensions. In theory, these could be thought of as related, perhaps as nested or dependent factors, but in practice they are treated on Facebook as independent, mutually exclusive settings. Our treatment is practically and ecologically consistent but a theory driven treatment could perhaps net different results. Further, the three dimensions of privacy proposed by DeCew's (1997) were developed prior to the advent of social media. Hence, although it offers a convenient framework for categorizing the privacy management settings afforded by Facebook, its appropriateness, coverage, and validity in explaining digital privacy in the Web 2.0 world, where the boundaries between public and private information are increasingly blurred, remains to be ascertained. This is a limitation of the current application of the dimensions and a topic ripe for future research. Finally, the study used a cross-sectional design, where the dependent and independent measures were collected at the same time and where relational tests were supported by theory rather than established by natural time.

These are limitations of social science research that utilizes this approach (many of which do) and requires future research to address. Research could use an adult, national or global sample, behavioral measures of Facebook settings procured from Facebook, and experiments to assess what settings users changed in response to a privacy beach. Such research could be done in other countries and also focus on other social networking platforms such as Twitter and LinkedIn, to examine the cross-cultural and multi-platform generalizability of these results. Finally, how users chose their privacy settings on social media is to a large extent dictated by the afforances of each platform. Knowing whether the afforded settings are adequate or whether users expect different settings or perhaps more control over individual settings is another future research question, the answer to which could enhance how people manage their privacy better.

All said, however, the findings of the study are noteworthy. Decision science has long accepted the idea that people go through a cost-benefit evaluation prior to making important decisions. None have, however, addressed the theoretical constituents of costs and benefits or its implications on the enactment of the privacy protections afforded by social media. By extending the theoretical lens provided by PMT and U&G, the present study not only explains the cognitive processes but also allow us pinpoint the specific costs and specific benefits that drive the enactment of various privacy protections on Facebook.

References

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Monterey, CA: Brooks/Cole Pub. Co.

Braz, C., Seffah, A., & M'raihi, D. (2007). Designing a trade-off between usability and security: A metrics based-model. In Human-computer interaction–INTERACT 2007 (pp. 114–126). Berlin: Springer.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. Paper presented at the 42nd Hawaii International Conference on System Sciences.

Debatin, B., Lovejoy, J.P., Horn, A.-K., & Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15, 83–108. doi: 10.1111/j.1083-6101.2009.01494.x

DeCew, J.W. (1997). In pursuit of privacy: Law, ethics, and the rise of technology. Ithaca, NY: Cornell University Press.

Dvorak, J.C. (2001). LinkedIn Account Hacked. PC Magzine.

Ellison, N.B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12, 1143–1168.

Floyd, D.L., Prentice-Dunn, S., & Rogers, R.W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30, 407–429.

Goffman, E. (1959). The presentation of self in everyday life. Garden City, NY: Doubleday.

Herath, T., & Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18, 106–125.

Joinson, A.N. (2008). Looking at, looking up or keeping up with people? Motives and use of Facebook. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Joinson, A.N., Houghton, D.J., Vasalou, A., & Marder, B.L. (2011). Digital crowding: Privacy, self-disclosure, and technology. In Privacy online (pp. 33–45). Berlin: Springer.

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. Decision Support Systems, 52, 353–363. https://doi.org/10.1016/j.dss.2011.09.002

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33, 71–90.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. Journal of Information Privacy & Security, 9, 47–67.

Milne, G.R., Labrecque, L.I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. Journal of Consumer Affairs, 43, 449–473. doi: 10.1111/j.1745-6606.2009.01148.x

Miller, S. (2012). Sen. Grassley's Twitter Account Hacked by SOPA Protesters. ABC News. http://abcnews.go.com/blogs/politics/2012/01/sen-grassleys-twitter-account-hacked-by-sopa-protesters/.

Moser, S., Bruppacher, S.E., & Mosler, H.-J. (2011). How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies. Risk Analysis, 31, 832–846. doi: 10.1111/j.1539-6924.2010.01544.x

Nielsen, (2010). Facebook users average 7 hours a month in January as Digital universe expands. Retrieved from http://www.nielsen.com/us/en/newswire/2010/facebook-users-average-7-hrs-a-month-in-january-as-digital-universe-expands.html

Petronio, S.S. (2002). Boundaries of privacy: Dialectics of disclosure. Albany: State University of New York Press.

Raacke, J., & Bonds-Raacke, J. (2008). MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking

sites. Cyberpsychology & Behavior, 11, 169–174. doi: 10.1089/cpb.2007.0056
Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. Retrieved from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/
Ray, M.B. (2007). Needs, motives, and behaviors in computer-mediated communication: An inductive exploration of social networking websites. Paper presented at the 57th Annual Conference of the International Communication Association, San Francisco, CA.
Riley, M.A., & Vance, A. (2012). China corporate espionage boom knocks wind out of U.S. Companies, Bloomberg Business Week.
Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91, 93.
Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153–176). New York: Guilford.
Roche, J.L. (2011). Bank of America just had the ultimate social media fail. Business Insider.
Salkin, A. (2009). Going for bling: Hollywood Burglars, New York Times. Retrieved from http://www.nytimes.com/2009/11/15/fashion/15bling.html
Sangmi, C., Bagchi-Sen, S., Morrell, C., Rao, H.R., & Upadhyaya, S.J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. IEEE Transactions on Professional Communication, 52, 167–182. doi: 10.1109/TPC.2009.2017985
Shahnaz, L., & Wok, S. (2011). Religious motives for using Facebook among university Muslim students. Paper presented at the Seminar Kebangsaan Media dan Dakwah, Universiti Sains Islam Malaysia.
Sundar, S.S., & Limperos, A.M. (2013). Uses and grats 2.0: New gratifications for new media. Journal of Broadcasting & Electronic Media, 57, 504–525. doi: 10.1080/08838151.2013.845827
Vishwanath, A. (2008). The 360 news experience: Audience connections with the ubiquitous news organization. Journalism & Mass Communication Quarterly, 85, 7–22.
Vishwanath, A. (2009). From belief-importance to intention: The impact of framing on technology adoption. Communication Monographs, 76, 177–206.
Vishwanath, A. (2015). Diffusion of deception in social media: Social contagion effects and its antecedents. Information Systems Frontiers, 17, 1353–1367.
Westin, A.F. (1967). Privacy and freedom (1st ed.). New York: Atheneum.
Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs, 59, 329.
Wolf, S., Gregory, W.L., & Stephan, W.G. (1986). Protection motivation theory: Prediction of intentions to engage in anti-nuclear war behaviors 1. Journal of Applied Social Psychology, 16, 310–321.
Wu, Y., Stanton, B.F., Li, X., Galbraith, J., & Cole, M.L. (2005). Protection motivation theory and adolescent drug trafficking: Relationship between health motivation and longitudinal risk involvement. Journal of Pediatric Psychology, 30, 127–137.