

2018

How people protect their privacy on Facebook: A cost-benefit view

Arun Vishwanath
SUNY University at Buffalo

Weiai Xu
University of Massachusetts Amherst

Zed Ngoh
SUNY University at Buffalo

Follow this and additional works at: https://scholarworks.umass.edu/communication_faculty_pubs

 Part of the [Social Media Commons](#)

Recommended Citation

Vishwanath, Arun; Xu, Weiai; and Ngoh, Zed, "How people protect their privacy on Facebook: A cost-benefit view" (2018). *Journal of the Association for Information Science and Technology*. 58.
<https://doi.org/10.1002/asi.23894>

This Article is brought to you for free and open access by the Communication at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Communication Department Faculty Publication Series by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.

Running head: HOW PEOPLE PROTECT THEIR PRIVACY

How People Protect their Privacy on Social Networking Sites: A Cost-Benefit View

Arun Vishwanath, Ph.D., MBA

Weiai Xu, Ph.D.

Zed Ngoh, MA

February 2016

Author note

Arun Vishwanath, Ph.D., MBA, is an Associate Professor of Communication and Management Science & Systems, University at Buffalo (UB), Buffalo, NY 14260. Please address all correspondence to Arun Vishwanath, phone: 716-645-1163, fax: 716-645-2064; email: avishy@buffalo.edu.

HOW PEOPLE PROTECT THEIR PRIVACY

ABSTRACT

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 the users' 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 cognitively 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 susceptibility influencing accessibility privacy.

Keywords: social media privacy, protection motivation theory, uses and gratifications, cognitive process, cost-benefit evaluation

HOW PEOPLE PROTECT THEIR PRIVACY

How People Protect their Privacy on Social Networking Sites: A Cost-Benefit View

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 in order 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 in order 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.

Cybercrimes frequently occur where users are targeted by phishing messages crafted based on users' likes and dislikes disclosed on social media. There are also incidents of scammers using social media to impersonate other people and gain access to users' personal information. Leaking of such information has led to crimes ranging from petty theft to home invasion and organizational and national espionage (Dvorak, 2011; Miller, 2012; Riley & Vance, 2012; Roche, 2011). Already some 10% of users have reported experiencing a loss of reputation, identity, or some form of monetary cost due to PII stolen from their social media accounts. Many others—86% in a 2013 Pew study—have made efforts to erase their digital footprint or taken

HOW PEOPLE PROTECT THEIR PRIVACY

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 involve 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 paper.

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

HOW PEOPLE PROTECT THEIR PRIVACY

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 proposes that a finite number of gratifications sought drive the use of a medium (Sundar & Limperos, 2013). 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 paper 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

HOW PEOPLE PROTECT THEIR 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.

Information privacy focuses on the control of access to one's digital information. User-disclosed information on Facebook, such as name, gender, residence, birth date, employment and education history, contact information and relationship status, constitute one's social identity. This identity is 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. For instance, a hacker with access to these pieces of digital information could easily steal an user's identity, open credit cards, or procure access to other online accounts. The protection measure available to control digital data access is Facebook's "security settings" (see Figure 1 in appendices), which monitors login information and notifies users of suspicious activity.

HOW PEOPLE PROTECT THEIR PRIVACY

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 the one hand, a necessary step towards 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" (see Figure 2 in appendices) help users control who can find them using email or phone numbers, as well as who can send them private messages and friend-requests.

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

HOW PEOPLE PROTECT THEIR PRIVACY

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 (Rui & Stefanone, 2013), 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" (see Figure 3 in appendices), 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, while 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.

HOW PEOPLE PROTECT THEIR PRIVACY

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 anti-nuclear 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. While none of these work focuses on the enactment of privacy protections on social media, they altogether provide the impetus for hypothesizing that increased cost 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.

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

HOW PEOPLE PROTECT THEIR PRIVACY

H2: User's a) perceived severity, b) perceived susceptibility, c) response efficacy, and d) self-efficacy towards 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 towards the potential loss of social image will enhance the frequency and use of Facebook's privacy protections to control expressive privacy.

While 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.

HOW PEOPLE PROTECT THEIR PRIVACY

The present research focused on the first-order gratifications people derive from Facebook rather than 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:

HOW PEOPLE PROTECT THEIR PRIVACY

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

Facebook users' degree of privacy protection management was measured using the settings available on Facebook under the following categories: security settings, privacy settings and tools, and timeline and tagging settings. For each function within these categories, participants were asked the extent to which they were aware of the setting (i.e., who could access the setting) followed by the frequency with which they changed the setting using a 1 (*Not at all*

HOW PEOPLE PROTECT THEIR PRIVACY

frequently) to 5 (*Very frequently*) response scale. To accurately ascertain the intensity with which each setting was enacted, the individual awareness/visibility responses were weighted by the frequency with which the setting was changed.

Privacy protection towards social image. Six items measured participants' level of openness towards allowing other users to see their timeline or to add to it. A Likert-type scale of 1 (*I am not aware of this setting*)–5 (*No one*), where 1 signified an open profile while 5 signified a private profile, was used. 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 Exploratory Factor Analysis (EFA) was conducted on the items ($mean=3.38$, $s.d.=.78$, $\alpha=.92$). Those items were then weighted by the respective frequency of change response and averaged to create an index for final analysis ($mean=6.42$, $s.d.=3.37$).

Privacy protection towards anonymity. Four items measured participants' level of openness towards allowing other users to contact them. Again, a Likert-type scale of 1–5, was used. Sample items 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 ($mean=2.73$, $s.d.=.75$, $\alpha=.71$). The items were weighted by the respective frequency of change response and averaged to create an index for final analysis ($mean=5.42$, $s.d.=3.48$).

Privacy protection towards digital data. Six items measured participants' level of awareness of the protective measures that Facebook offers to prevent the loss of digital data. Sample items include “I am aware of the Secure Browsing setting” and “I am aware of the Login Notifications setting.” Each item was scored using a Likert-type scale of 1 (*Strongly disagree*) to 5 (*Strongly agree*). EFA was conducted on the items ($mean=3.13$, $s.d.=.90$, $\alpha=.88$). The items

HOW PEOPLE PROTECT THEIR PRIVACY

were weighted by the respective frequency of change response and averaged to create an index for final modeling ($mean=6.17$, $s.d.=3.90$).

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 ($mean=3.61$, $s.d.=.87$, $\alpha=.85$), 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 ($mean=3.14$, $s.d.=.78$, $\alpha=.82$), 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

HOW PEOPLE PROTECT THEIR PRIVACY

inspection of items suggested that one dimension was related to unauthorized access of digital data ($mean=3.21, s.d.=.68, \alpha=.83$). 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 ($mean=2.91, s.d.=.88, \alpha=.87$) and the responses in this dimension were averaged to create an index for H2, H3, H5 and H6.

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 ($mean=3.20, s.d.=.75, \alpha=.89$).

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 ($mean=3.56, s.d.=.73, \alpha=.91$).

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

HOW PEOPLE PROTECT THEIR PRIVACY

dimensions explicated by prior research: social needs ($mean=2.83, s.d.=.79, \alpha=.87$), information needs ($mean=3.35, s.d.=.77, \alpha=.81$) and entertainment needs ($mean=3.43, s.d.=.80, \alpha=.80$). The responses in each dimension were averaged to create an index.

Findings

H1 and H4, H 2 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, perceived severity and perceived susceptibility towards 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, $F(7, 505) = 15.06, p<.001$, 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 towards digital data. Additionally, social needs positively predicted protection enactment ($\beta=.43, t=8.53, p<.001$), while information needs ($\beta=-.14, t=-2.55, p=.011$) negatively predicted protection enactment towards unauthorized access of digital data. Therefore, H1 and H4 were partially supported.

Table 1.

Testing H1 and H4 on protection enactment towards unauthorized access of digital data
(information privacy)

HOW PEOPLE PROTECT THEIR PRIVACY

	First block (PMT)		Second block (U&G)	
	β	S.E.	β	S.E.
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
<i>F</i> , Adj. <i>R</i> ²	<i>F</i> (7, 505) = 15.06**, .16			
* <i>p</i> < .05 (two-tailed), ** <i>p</i> < .01 (two-tailed)				

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.

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

	First block (PMT)		Second block (U&G)	
	β	S.E.	β	S.E.
Perceived severity	.24**	.20	.19**	.19
Perceived susceptibility	.15*	.17	.08	.17

HOW PEOPLE PROTECT THEIR PRIVACY

Response efficacy	.03	.23	.001	.22
Self-efficacy	-.18**	.24	-.11*	.23
Social needs			.38**	.22
Information needs			-.14*	.25
Entertainment needs			-.12*	.22
<i>F</i> , Adj. <i>R</i> ²	<i>F</i> (7, 505) = 16.70**, .18			
* <i>p</i> < .05 (two-tailed), ** <i>p</i> < .01 (two-tailed)				

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 ($\beta = -.11, t = -2.20, p = .029$). Among the U&G predictors, 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.

Table 3.

Testing H3 and H6 on protection enactment for loss of social image (expressive privacy)

HOW PEOPLE PROTECT THEIR PRIVACY

	First block (PMT)		Second block (U&G)	
	β	S.E.	β	S.E.
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
$F, \text{Adj. } R^2$	$F(7, 505) = 13.84^{**}, .15$			
* $p < .05$ (two-tailed), ** $p < .01$ (two-tailed)				

Discussion

The research examined the cognitive cost-benefit appraisal processes that underlie users' enactment of privacy protections on Facebook. 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.

The application of U&G framework pointed to social need fulfillment as the single most significant Facebook benefit that enhances the protection of information privacy, accessibility

HOW PEOPLE PROTECT THEIR PRIVACY

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. In contrast, information needs and entertainment needs appear to relax the intensity of enactment, ostensibly because on Facebook, individuals can seek information by lurking or by divulging limited profile information to information and content providers.

Relative to the benefits, the perceived costs of social media use 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 anonymity). 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 towards 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 ignoring the fact that not all settings are underutilized

HOW PEOPLE PROTECT THEIR PRIVACY

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. Additionally, given the influence of individual level differences in coping efficacy, security designers 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. While college students are an important demographic of social media users and are often targets of cyber criminals, they are also atypical of the broader U.S. or global population of Internet users. This 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 as participant biases from 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. 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 all 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 breach. Such research could be done

HOW PEOPLE PROTECT THEIR PRIVACY

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.

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

- Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies* (Vol. 4258, pp. 36-58): Springer Berlin Heidelberg.
- Alexa. (2014). Alexa top 500 global sites. Retrieved October 30, 2014, from <http://www.alexa.com/topsites>
- Altman, I. (1973). *Social penetration: The development of interpersonal relationships*. Holt Rinehart and Winston: New York.
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co.: Monterey, Calif.
- Barnes, S. B. (2006). *A privacy paradox: Social networking in the United States*.
- Binder, J., Howes, A., & Sutcliffe, A. (2009). *The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, USA.
- 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). Springer Berlin Heidelberg.
- Chenoweth, T., Minch, R., & Gattiker, T. (2009, 5-8 January). *Application of Protection Motivation Theory to Adoption of Protective Technologies*. Paper presented at the 42nd Hawaii International Conference on System Sciences.

HOW PEOPLE PROTECT THEIR PRIVACY

- 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*(1), 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*. Cornell University Press: Ithaca, N.Y.
- Duggan, M., & Smith, A. (2013). Demographics of key social networking platforms. Retrieved October 13, 2014, from <http://www.pewinternet.org/2013/12/30/demographics-of-key-social-networking-platforms/>
- Dvorak, J. C. (2001). LinkedIn Account Hacked, *PC Magazine*.
- 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*(4), 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*(2), 407-429.
- Goffman, E. (1959). *The presentation of self in everyday life*. Doubleday: Garden City, N.Y.
- Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. *Unpublished paper presented at the “Privacy Poster Fair” at the Carnegie Mellon University School of Library and Information Science, 9*.
- Ibrahim, Y. (2008). The new risk communities: Social networking sites and risk. *International Journal of Media & Cultural Politics, 4*(2), 245-253. doi: 10.1386/macp.4.2.245_3
- 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.

HOW PEOPLE PROTECT THEIR PRIVACY

- Joinson, A. N., Houghton, D. J., Vasalou, A., & Marder, B. L. (2011). Digital crowding: Privacy, self-disclosure, and technology *Privacy Online* (pp. 33-45): Springer.
- Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. *Project MAC: MIT Project on Mathematics and Computing, 1*.
- Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353-363. doi: <http://dx.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*(1), 71-90.
- Meso, P. p. g. e., Yi Ding, y. g. e., & Shuting Xu, s. g. e. (2013). Applying Protection Motivation Theory to Information Security Training for College Students. *Journal of Information Privacy & Security, 9*(1), 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*(3), 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*(5), 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 February 15, 2014, from

HOW PEOPLE PROTECT THEIR PRIVACY

<http://www.nielsen.com/us/en/newswire/2010/facebook-users-average-7-hrs-a-month-in-january-as-digital-universe-expands.html>

Pagliery, J. (2013). 2 million Facebook, Gmail and Twitter passwords stolen in massive hack.

Retrieved October 31, 2014, from

<http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/>

Park, N., Jin, B., & Annie Jin, S.-A. (2011). Effects of self-disclosure on relational intimacy in

Facebook. *Computers in Human Behavior*, 27(5), 1974-1983. doi:

<http://dx.doi.org/10.1016/j.chb.2011.05.004>

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

Raacke, J., & Bonds-Raacke, J. (2008). MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. *Cyberpsychology & Behavior: The Impact Of The Internet, Multimedia And Virtual Reality On Behavior And Society*, 11(2), 169-174. doi: 10.1089/cpb.2007.0056

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. Retrieved October 30, 2014, 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.

Reuters. (2013). Facebook reveals daily users for U.S. and UK, data aimed at advertisers.

Retrieved February 15, 2014, from <http://in.reuters.com/article/2013/08/13/facebook-users-idINDEE97C0DC20130813>

HOW PEOPLE PROTECT THEIR PRIVACY

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*(1), 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 Publications, Incorporated.

Roche, J. L. (2011). Bank Of America Just Had The Ultimate Social Media Fail, *Business Insider*.

Rui, J., & Stefanone, M. A. (2013). Strategic self-presentation online: A cross-cultural study. *Computers in Human Behavior, 29*(1), 110-118. doi:
<http://dx.doi.org/10.1016/j.chb.2012.07.022>

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*(2), 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.

Sullivan, B. (2014). 13.1 Million Americans Hit By Identity Theft in 2013. Retrieved February 15, 2014, from <http://blog.credit.com/2014/02/13-1-million-hit-by-identity-theft-in-2013-75414/>

HOW PEOPLE PROTECT THEIR PRIVACY

Sundar, S. S., & Limperos, A. M. (2013). Uses and grats 2.0: New gratifications for new media.

Journal of Broadcasting & Electronic Media, 57(4), 504-525. doi:

10.1080/08838151.2013.845827

Taddicken, M., & Jers, C. (2011). The uses of privacy online: Trading a loss of privacy for social web gratifications? *Privacy online* (pp. 143-156): Springer.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36. doi:

10.1177/0270467607311484

Tyma, A. (2007). Rules of Interchange: Privacy in Online Social Communities--A Rhetorical Critique of MySpace.Com. *Journal of the Communication, Speech & Theatre Association of North Dakota*, 20, 31-39.

Uwe, W., & Jörg, D. (2001). Motives of adolescents to use the internet as a function of personality traits, personal and social factors. *Journal of Educational Computing Research*, 24(1), 13-27. doi: 10.2190/ANPM-LN97-AUT2-D2EJ

Westin, A. F. (1967). *Privacy and freedom* ([1st ed.] ed.). Atheneum: New York.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, 59(4), 329.

HOW PEOPLE PROTECT THEIR PRIVACY

Figure 1. Screen shot of Facebook's security settings, captured on October 30, 2014.

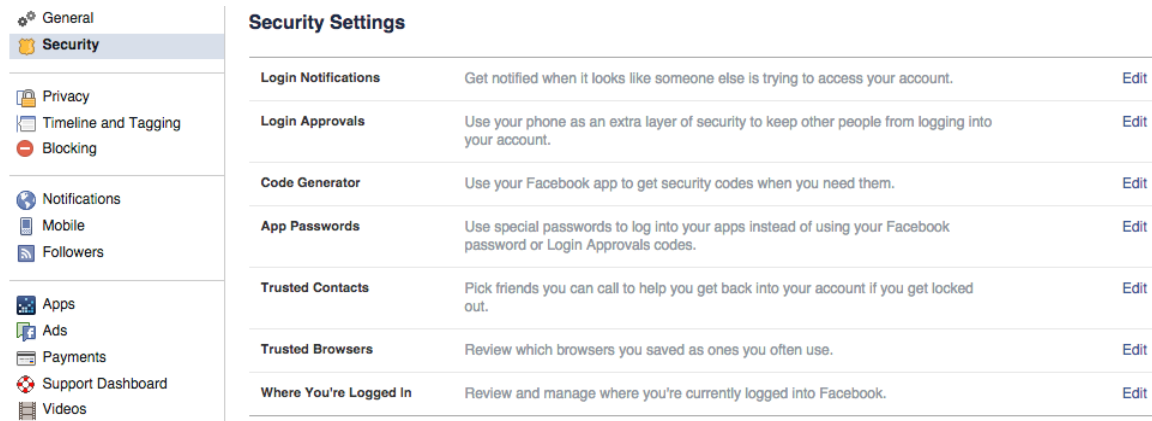


Figure 2. Screen shot of Facebook's privacy settings and tools, captured on October 30, 2014.

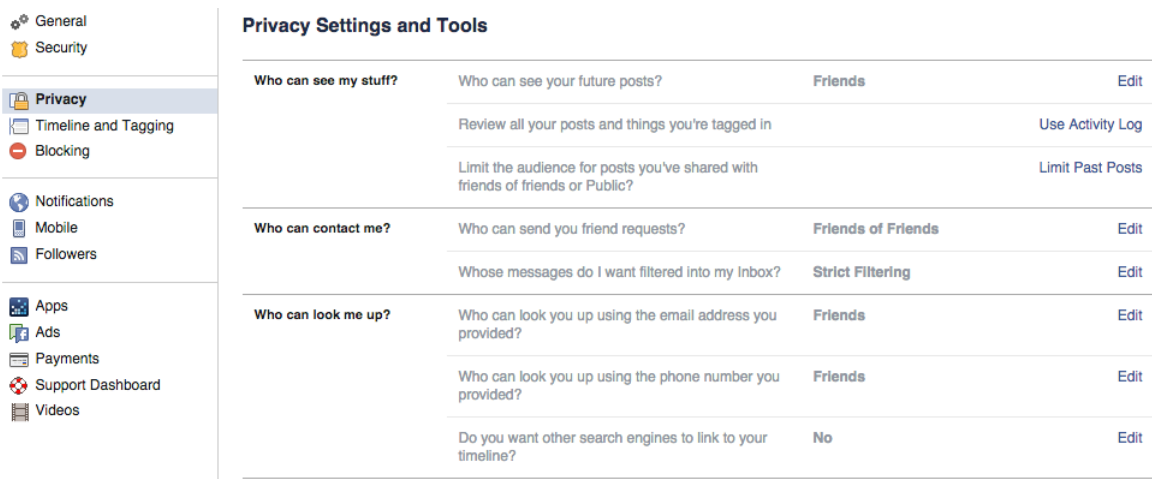















Figure 3. Screen shot of Facebook's timeline and tagging settings, captured on October 30, 2014.

HOW PEOPLE PROTECT THEIR PRIVACY

-  General
-  Security

-  Privacy
-  **Timeline and Tagging**
-  Blocking

-  Notifications
-  Mobile
-  Followers

-  Apps
-  Ads
-  Payments
-  Support Dashboard
-  Videos

Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	No One	Edit