Privacy Protecting Behavior in Social Network Sites

Emergent Research Forum Paper

Claus-Peter H. Ernst
Frankfurt University of Applied Sciences
cernst@fb3.fra-uas.de

Jella Pfeiffer
Karlsruher Institut für Technologie (KIT)
jella.pfeiffer@kit.edu

Franz Rothlauf
Johannes Gutenberg-Universität Mainz
rothlauf@uni-mainz.de

Abstract

Risks generally lead to Protecting Behavior. However, it is still unknown which specific Protecting Behavior results from Perceived Privacy Risk in Social Network Sites (SNSs). In this article, we draw from the Protection Motivation Theory to postulate an influence of Perceived Privacy Risk (Threat Appraisal) on six Privacy Protecting Behaviors SNS members can use, which we identified in the literature: Refusal, Misrepresentation, Removal, Selectivity in Connections, Termination of Connections, and Strictness of Privacy Settings. Moreover, we argue that because of differences between the Coping Appraisals of the six identified Privacy Protecting Behaviors, the extent of the influence of Perceived Privacy Risk on these six behaviors differs. We conclude by giving an outlook on the planned empirical evaluation of our research model as well as on potential practical implications.

Keywords

Social Network Site, Privacy Risk, Privacy Protecting Behavior.

Introduction

Social Network Sites (SNSs) provide multiple possibilities to disclose personal information (Boyd and Ellison 2007). As a result, using them presents risks to the privacy of their members: indeed, the members' information could be used for unwelcome commercial purposes or members could become the target of personal attacks (cf. Krasnova et al. 2010a).

People can address their *Perceived Privacy Risk* by performing *Privacy Protecting Behaviors* (e.g., Son and Kim 2008). *Perceived Privacy Risk* is the degree to which a person believes that using an SNS has negative consequences with regards to his/her privacy (cf. Chen 2013; Dinev and Hart 2006; Featherman and Pavlou 2003; Kim et al. 2008; Krasnova et al. 2010b; Peter and Ryan 1976; Wu et al. 2009); *Privacy Protecting Behavior* is the set of possibilities SNS members have at their disposal to safeguard themselves against the potential negative consequences associated with the risks to their privacy (cf. Krasnova et al. 2010b; Son and Kim 2008; Wu et al. 2009). But which specific *Protecting Behaviors* result from *Perceived Privacy Risk* in SNSs?

In this article, we draw from the *Protection Motivation Theory* to postulate an influence of *Perceived Privacy Risk* (*Threat Appraisal*) on six *Privacy Protecting Behaviors* SNS members can use, which we identified in the literature: *Refusal*, *Misrepresentation*, *Removal*, *Selectivity in Connections*, *Termination of Connections*, and *Strictness of Privacy Settings* (cf. Bulgurcu et al. 2010; Krasnova et al. 2010b; Son and Kim 2008). Moreover, we argue that because of differences between the *Coping Appraisals* of the six identified *Privacy Protecting Behaviors*, the extent of the influence of *Perceived Privacy Risk* on these six behaviors differs.

Theoretical Background

Protection Motivation Theory

The *Protection Motivation Theory* (Maddux and Rogers 1983; Rogers 1975; Rogers 1983) (Figure 1) generally postulates that an individual's *Threat Appraisal* and *Coping Appraisal* both influence his/her *Protection Motivation,* which is the direct antecedent of his/her *Actual Protecting Behavior* (Table 1 in the appendix defines *Protection Motivation Theory's* central constructs). More specifically, an individual has two possibilities to cope with a threat he/she is facing: (1) do nothing or (2) take counteractions. Whereas *Threat Appraisal* evaluates the threat itself, i.e., both the positive and negative consequences that might occur if an individual chooses to do nothing about it, *Coping Appraisal* evaluates the possible *Protecting Behaviors* that might safeguard against the threat. Indeed, *Coping Appraisal* is a calculus of *Response Efficacy*, *Self-efficacy*, and *Response Costs* (as defined in Table 2 in the appendix). Whereas *Response Efficacy and Self-Efficacy* increase *Coping Appraisal*, the *Response Costs* decrease it (Floyd et al. 2000).

Multiple studies have successfully used the *Protection Motivation Theory* to explain people's *Protecting Behavior* in different contexts. For example, this theory has been used to explain people's behavior when addressing health threats. For an overview, see Floyd et al. (2000).

In the following section, we describe the six *Privacy Protecting Behaviors* that can be used by SNS members to cope with their *Perceived Privacy Risk*, a specific manifestation of *Threat Appraisal*.

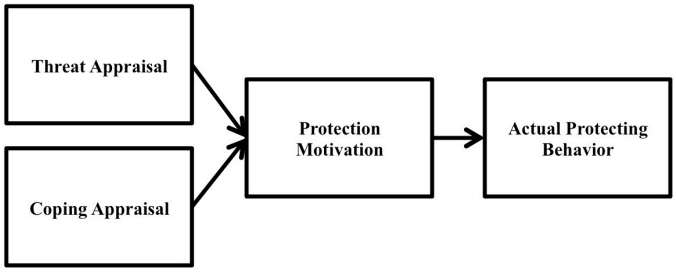

Figure 1. Protection Motivation Theory

Privacy Protecting Behavior

SNSs provide multiple possibilities to disclose personal information (Boyd and Ellison 2007). This ubiquitous provision of personal information bears risks, that is, "the extent to which there is an uncertainty in significant and disappointing outcomes that may be realized" (Chen 2013, p. 1222; Sitkin and Pablo 1992), with regards to the privacy of the members, i.e., their "claim … to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1968, p. 7).

It is known that SNS members can choose to perform *Privacy Protecting Behaviors* in order to protect themselves against their *Perceived Privacy Risk*. Based on a literature study, we identified three kinds of studies that deal with *Privacy Protecting Behaviors* (Table 3 in the appendix gives an overview of all the (implicitly) examined *Privacy Protecting Behaviors*):

One research-in-progress study crafted a catalogue of behaviors that people might use to safeguard their privacy (Bulgurcu et al. 2010). Furthermore, some studies examined the privacy-related antecedents of *Privacy Protecting Behavior* in general. These studies did not differentiate between different kinds of protecting behavior at the construct level, rather they differentiated between different kinds of protecting behavior at the item level (Chen et al. 2009; Litt 2013; Wu et al. 2009). For example, Chen et al. (2009) found a positive influence of *Privacy Concerns* on *Information Privacy Protective Responses* in SNSs. Their dependent construct was measured using a four-item scale with each item representing one specific kind of protective response such as *Complaining Directly to Online Companies*. Finally, some studies examined the privacy-related antecedents of specific *Privacy Protecting Behaviors*. These studies differentiated between different kinds of behavior at the construct level (Chakraborty et al. 2013; Chen

2013; Ernst 2014; Krasnova et al. 2009; Krasnova et al. 2010b; Lankton and Tripp 2013; Lo 2010; Son and Kim 2008; Stutzman and Kramer-Duffield 2010; Thambusamy et al. 2010). For example, Krasnova et al. (2009) found that *Privacy Concerns* negatively influence the amount of *Self-Disclosure*.

Whereas *Quitting the SNS Platform* or limiting *Actual System Use* are two possibilities SNS members can use to safeguard their privacy (cf. Table 3 in the appendix), in doing so, they simultaneously limit or prevent themselves from accessing the SNSs' beneficial services. *Complaining to SNS Service Provider or Other Parties*, *Complaining Directly to Online Companies*, *Complaining Indirectly to Third-Party Organizations*, *Negative Word-of-Mouth*, and *Searching for Additional Protection Tools* only promise SNS members indirect possibilities of safeguarding themselves against *Privacy Risks*. *Managing Personally Identifiable Information Diligently* is a rather general behavior that can include multiple different specific behaviors. Overall, we do not consider any of these behaviors in the following study. Rather, we focus on the remaining behaviors found in the literature that promise members immediate chances for success at safeguarding their privacy without simultaneously limiting or preventing their access to the SNSs' beneficial services.

These behaviors can be summarized by six *Privacy Protecting Behaviors*, which we define in Table 4 in the appendix: *Refusal*, *Misrepresentation*, *Removal*, *Selectivity in Connections*, *Termination of Connections*, and *Strictness of Privacy Settings* (cf. Bulgurcu et al. 2010; Krasnova et al. 2010b; Son and Kim 2008). Indeed, *Refusal* summarizes *Information Disclosure/Self-Disclosure* and *Willingness to provide personal information to SNSs*. *Misrepresentation*, *Giving False Information*, and *Information Falsification* are different labels for the same kind of behavior. *Deletion of Others' Comments from the Own Profile* and *Untagging Photos* can be summarized by *Removal*. *Selectivity in Connections* includes all of the following behaviors: *Allowing Only Friends One Has Interacted With A Lot in One's Friends List, Exercising Caution Before Downloading and Using SNS Applications*, *Limiting Socialization*, *Number of SNS friends*, and *Selectivity in Friends*. *Deletion of People from Network/Friend Lists* and *Quitting Third-Party Applications* are both a specific manifestation of *Termination of Connections* and, hence, can be summarized by it. Finally, *Strictness of Privacy Settings* describes *Changing Privacy Settings*, *Limiting Certain Updates to Certain People*, *Privacy Settings* and *Having a Non-Public SNS Profile*. Table 5 in the appendix gives an overview of this classification.

Research Model

In this section, we draw from the *Protection Motivation Theory* to build our research model. More specifically, we use the *Protection Motivation Theory's* upper causal chain (*Threat Appraisal→Protection Motivation→Actual Protecting Behavior*) to postulate an influence of *Perceived Privacy Risk* (*Threat Appraisal*) on each of the six *Privacy Protecting Behaviors* (*Actual Protecting Behavior*) identified earlier. Furthermore, we use *Protection Motivation Theory's* lower causal chain (*Coping Appraisal→Protection Motivation→Actual Protecting Behavior*) to build hypotheses concerning the extent of *Perceived Privacy Risk's* influences on these behaviors. Figure 2 presents our research model.[1]

Perceived Privacy Risk is a privacy-specific manifestation of *Threat Appraisal*. Indeed, it describes the SNS members' evaluation of the negative consequences to their privacy[2] that might occur if they choose maladaptive behavior, i.e., do not protect themselves within SNSs' networks (cf. Floyd et al. 2000).

---

[1] In contrast to the original *Protection Motivation Theory*, we conceptualized a direct relationship between *Threat Appraisal* and the *Actual Protecting Behaviors*. This is in line with multiple studies from different contexts that do not examine the *intentions* to perform a specific behavior, but rather the behavior itself (cf. Yousafzai et al. 2007).

[2] The *misuse of personal information* as well as the *loss of control of personal information* are regularly seen as the two most severe negative consequences with regards to an individual's privacy (e.g., Featherman and Pavlou 2003; Wu et al. 2009). *Misuse of personal information* includes any unwelcome use of an individual's personal information: this includes using the information for commercial purposes, becoming the target of personal attacks (for example, bullying), data being misinterpreted, and/or becoming an unknowing participant in illegal activities (for example, identity theft) (cf. Krasnova et al. 2010a). *Loss of control of personal information* depicts any loss of control regarding how, when, or to

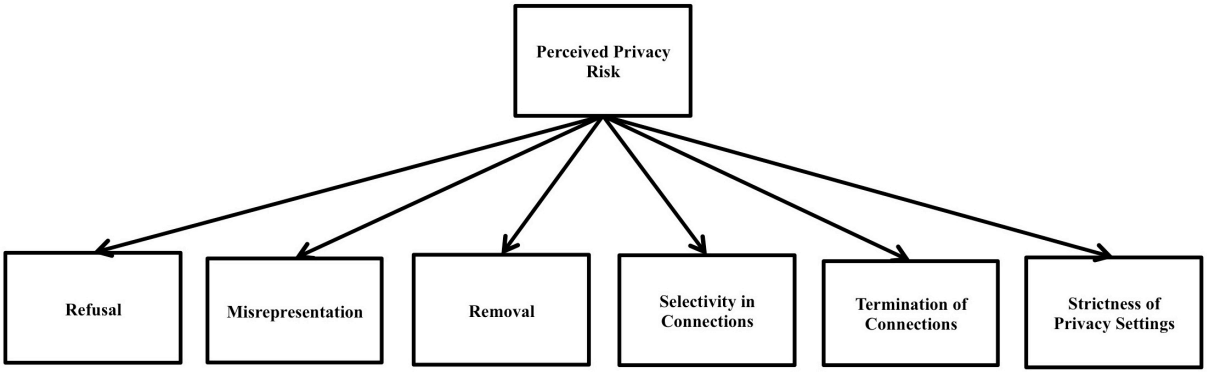

Figure 2. Research Model

Each of the six *Privacy Protecting Behaviors* identified earlier generally enables SNS members to safeguard themselves against potential negative consequences associated with the risks to their privacy: First, by *refusing* to provide specific personal information, *falsifying* personal information, and/or *removing* previously disclosed personal information (cf. Son and Kim 2008), SNS members protect their privacy by controlling the actual information that is accessible by others. Indeed, SNS members cannot lose control of missing/false personal information. Likewise, information that is protected in this manner cannot be misused by others (cf. Dinev and Hart 2006; Wu et al. 2009). Furthermore, by being *selective* when accepting or requesting connections in SNSs (cf. Bulgurcu et al. 2010), *terminating specific connections* (cf. Bulgurcu et al. 2010), and/or using *privacy settings* with strict information access control (cf. Krasnova et al. 2010b), SNS members are able to protect their privacy by controlling the entities that have access to their personal information. Indeed, allowing profile access only to connected entities and limiting these to trustworthy ones decreases the likelihood of losing control of personal information and decreases the likelihood that the personal information be misused (cf. Dinev and Hart 2006; Wu et al. 2009).

Drawing from the *Protection Motivation Theory's* upper causal chain, which postulates that *Threat Appraisal* (indirectly) influences an individual's *Actual Protecting Behavior*, we hypothesize that:

There is a positive influence of *Perceived Privacy Risk* on *Refusal* (**H1**), *Misrepresentation* (**H2**), *Removal* (**H3**), *Selectivity in Connections* (**H4**), *Termination of Connections* (**H5**), and *Strictness of Privacy Settings* (**H6**).

Furthermore, according to the *Protection Motivation Theory*, not only does the *Perceived Privacy Risk*, i.e. *Threat Appraisal*, influence an individual's actual behavior; so does the evaluation of the potential protecting behaviors themselves, i.e., *Coping Appraisal*. In other words, in order to respond to a *Perceived Privacy Risk,* SNS members prefer to use *Privacy Protecting Behaviors* that they consider as superior to the alternatives. In the following paragraphs, we discuss which of the six *Privacy Protecting Behaviors* might have better *Coping Appraisals* than their direct alternatives. We then use this information to build hypotheses regarding the extent of *Perceived Privacy Risk's* influence on them.

Disclosing *incorrect personal information* or *refusing* to give information within SNSs' networks both equally protect members against *privacy risks*. Indeed, no one can misuse missing or incorrect information. Likewise, an SNS member cannot lose control over information that is protected with *Misrepresentation* or *Refusal*. Hence, SNS members can be expected to consider the *Response Efficacy* of *Misrepresentation* and *Refusal* to be more or less equal. However, the *Misrepresentation* of information is more challenging than *Refusal*. Indeed, in order to give misrepresented information, SNS members have to first invent this information. In contrast, in order to perform *Refusal*, members literally do nothing at all. Hence, an individual's *Self-efficacy* regarding *Misrepresentation* can be expected to be lower than an individual's *Self-efficacy* regarding *Refusal*. Moreover, there are specific negative side effects, i.e. *Response Costs*, which also differentiate *Misrepresentation* from *Refusal*. For example, SNS

---

what extent, someone [for example, employers, teachers, parents, unknown persons (Krasnova et al. 2010a)] might see/use personal information (cf. Westin 1968).

contacts might take falsified information as truth, thus, getting a false impression of the corresponding SNS member. Also, members using a fake name in an SNS network might not be found by their real-life contacts. Hence, whereas *Misrepresentation* and *Refusal* can be expected to have equal *Response Efficacies*, *Misrepresentation* has a lower *Self-efficacy* and higher *Response Costs*.

Furthermore, *Removing* personal information from SNSs and *refusing* to give this information in the first place lead to the same negative results that might arise from missing information. Likewise, both *Removal* and *Refusal* are comparably challenging to perform. However, whereas *refusing* to give personal information ensures that no one can access the corresponding information in an SNS (because it is not present, and was never present), *removing* previously disclosed information does not provide the same extent of protection. Indeed, anyone might have seen the information when it was present. Hence, SNS members using *Removal* to protect their privacy can neither be sure that they have control over the previously disclosed information, nor that someone might not misuse it sometime in the future. Hence, whereas *Removal* and *Refusal* can be expected to have equal *Self-efficacies* and *Response Costs*, *Removal* has a lower *Response Efficacy*.

Finally, *terminating* existing connections in SNSs or being *selective* when accepting them in the first place lead to the same negative results that might arise due from not having certain connections. Also, both behaviors are comparably challenging to perform. However, whereas *Selectivity in Connections* ensures that specific entities do not have access to personal information in SNSs, *terminating* existing connections does not provide the same extent of protection. Indeed, a former contact might have seen the personal information when the connection existed. Hence, like *Removal*, *Termination of Connections* can neither ensure SNS members that they have control over their personal information, nor that someone might not misuse it sometime in the future. Hence, whereas *Termination of Connections* and *Selectivity in Connections* can be expected to have equal *Self-efficacies* and *Response Costs*, *Termination of Connections* has a lower *Response Efficacy*.

In summary, there are differences between *Refusal*, *Misrepresentation*, *Removal*, *Selectivity in Connections*, and *Termination of Connections* regarding the *Self-efficacies*, *Response Efficacies* and/or *Response Costs* of these behaviors. More specifically, regarding the *Privacy Protecting Behaviors* that control the accessible information, *Misrepresentation* has a lower *Self-efficacy* and higher *Response Costs* than *Refusal*; and *Removal* has a lower *Response Efficacy* than *Refusal*. Furthermore, regarding the *Privacy Protecting Behaviors* that control entities that have access to personal information, *Termination of Connections* has a lower *Response Efficacy* than *Selectivity in Connections*.

As postulated by the *Protection Motivation Theory*, these differences lead to differing *Coping Appraisals*. More specifically, *Misrepresentation* and *Refusal* are expected to have equal *Response Efficacies* but *Misrepresentation* has lower *Self-efficacies* as well as higher *Response Costs*. Since *Self-efficacy* increases *Coping Appraisal* and *Response Costs* decrease it (Floyd et al. 2000), *Misrepresentation* can consistently be expected to have a lower *Coping Appraisal* than *Refusal*. In a similar manner, the *Coping Appraisal* of *Removal* can be expected to be lower than of *Refusal* and the *Coping Appraisal* of *Termination of Connections* can be expected to be lower than of *Selectivity in Connections*.

Overall, SNS members can choose between different potential *Privacy Protecting Behaviors* to respond to their *Perceived Privacy Risk*. However, there are differences with regards to the *Response Efficacies*, *Self-efficacies* and *Response Costs* of these potential behaviors. As a result, SNS members consider some potential behaviors to be better (i.e., more effective, less challenging, and/or less costly) than others. According to the *Protection Motivation Theory*, SNS members prefer to use *Privacy Protecting Behaviors* that they consider superior to the alternatives, in order to respond to their *Perceived Privacy Risk*. Hence, it can be expected that *Perceived Privacy Risk* leads rather to *Refusal* than to *Misrepresentation* or *Removal*. Likewise, it will rather lead to *Selectivity in Connections* than to *Termination of Connections*. We hypothesize that:

The influence of *Perceived Privacy Risk* on *Refusal* is higher than its influence on *Misrepresentation* (**H7**) or *Removal* (**H8**).

The influence of *Perceived Privacy Risk* on *Selectivity in Connections* is higher than its influence on *Termination of Connections* (**H9**).

Outlook

We drew from the *Protection Motivation Theory* (Maddux and Rogers 1983; Rogers 1975; Rogers 1983) in order to postulate influences of *Perceived Privacy Risk* on six *Privacy Protecting Behaviors* identified in the literature, and to build hypotheses concerning the extent of these influences.

To empirically evaluate our research model, we plan to survey users of *Facebook* using a quantitative questionnaire. In order to accomplish this, we plan to adapt existing measurements of *Perceived Privacy Risk* to our context and, due to a lack of suitable operationalization, to develop our own operationalization for the six potential *Privacy Protecting Behaviors*. To collect the data, we plan to use Facebook advertisements in multiple regions around the world that will promise a raffle of gift certificates from *Amazon.com* for every completed questionnaire. Finally, we plan to analyze the gathered data using a structural equation modeling approach.

Our findings can be expected to hold important practical implications. Foremost, if confirmed, our hypotheses would suggest that SNS service providers need to actively manage people's privacy risk perception since SNS members' resulting *Refusal*, *Misrepresentation*, *Removal*, *Selectivity in Connections*, *Termination of Connections*, and *Strictness of Privacy Settings* hinder their business model, i.e., the selling of personal advertisements.

References

Boyd, D.M., and Ellison, N.B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13:1), pp. 210-230.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook," *ICIS 2010 Proceedings*, Paper 230.

Chakraborty, R., Vishik, C., and Rao, H.R. 2013. "Privacy Preserving Actions of Older Adults on Social Media: Exploring the Behavior of Opting out of Information Sharing," *Decision Support Systems* (55:4), pp. 948-956.

Chen, J., Ping, W., Xu, Y., and Tan, B.C.Y. 2009. "Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context," *ICIS 2009 Proceedings*, Paper 174.

Chen, R. 2013. "Member Use of Social Networking Sites - an Empirical Examination," *Decision Support Systems* (54:3), pp. 1219-1227.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Ernst, C.-P.H. 2014. "Risk Hurts Fun: The Influence of Perceived Privacy Risk on Social Network Site Usage," *AMCIS 2014 Proceedings*.

Featherman, M.S., and Pavlou, P.A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451-474.

Floyd, D., Prentice-Dunn, S., and Rogers, R. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

Kim, D.J., Ferrin, D.L., and Rao, H.R. 2008. "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents," *Decision Support Systems* (44:2), pp. 544-564.

Krasnova, H., Kolesnikova, E., and Guenther, O. 2009. "'It Won't Happen to Me!': Self-Disclosure in Online Social Networks," *AMCIS 2009 Proceedings*, Paper 343.

Krasnova, H., Kolesnikova, E., and Guenther, O. 2010a. "Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study," *ECIS 2010 Proceedings*, Paper 160.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010b. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

Lankton, N., and Tripp, J. 2013. "A Quantitative and Qualitative Study of Facebook Privacy Using the Antecedent-Privacy Concern-Outcome Macro Model," *AMCIS 2013 Proceedings*.

Litt, E. 2013. "Understanding Social Network Site Users' Privacy Tool Use," *Computers in Human Behavior* (29:4), pp. 1649-1656.

Lo, J. 2010. "Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites," *AMCIS 2010 Proceedings*, Paper 110.

Maddux, J., and Rogers, R. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp. 469-479.

Peter, J.P., and Ryan, M.J. 1976. "An Investigation of Perceived Risk at the Brand Level," *Journal of Marketing Research* (13:2), pp. 184-188.

Rogers, R. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology: Interdisciplinary and Applied* (91:1), pp. 93-114.

Rogers, R. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology: A Sourcebook,* J. Cacioppo and R. Petty (eds.). New York, NY: Guilford Press, pp. 153-176.

Sitkin, S.B., and Pablo, A.L. 1992. "Reconceptualizing the Determinants of Risk Behavior," *The Academy of Management Review* (17:1), pp. 9-38.

Son, J.-Y., and Kim, S.S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.

Stutzman, F., and Kramer-Duffield, J. 2010. "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook," *CHI 2010 Proceedings*.

Thambusamy, R., Church, M., Nemati, H., and Barrick, J. 2010. "Socially Exchanging Privacy for Pleasure: Hedonic Use of Computer-Mediated Social Networks," *ICIS 2010 Proceedings*, Paper 253.

Westin, A.F. 1968. *Privacy and Freedom*. New York, NY: Atheneum.

Wu, Y.A., Ryan, S., and Windsor, J. 2009. "Influence of Social Context and Affect on Individuals' Implementation of Information Security Safeguards," *ICIS 2009 Proceedings*, Paper 70.

Yousafzai, S.Y., Foxall, G.R., and Pallister, J.G. 2007. "Technology Acceptance: A Meta-Analysis of the Tam: Part 2," *Journal of Modelling in Management* (2:3), pp. 281-304.

Appendix

Construct	Definition
Threat Appraisal	An individual's evaluation of the consequences that might occur if no actions to protect the self from a potential threat/risk are performed (Floyd et al. 2000)
Coping Appraisal	An individual's evaluation of "the ability to cope with and avert the threatened danger" (Floyd et al. 2000, p. 410)
Protection Motivation	An individual's intention to protect the self from a potential threat/risk (cf. Floyd et al. 2000)
Actual Protecting Behavior	An individual's actual "activity to protect the self from danger" (Maddux and Rogers 1983, p. 470)

Table 1. Definitions of the Protection Motivation Theory's Core Constructs

Construct	Definition
Response Efficacy	"[T]he belief that the adaptive response will work, that taking the protective action will be effective in protecting the self …" (Floyd et al. 2000, p. 411)
Self-efficacy	"[T]he perceived ability of the person to actually carry out the adaptive response (Floyd et al. 2000, p. 411)
Response Costs	"[A]ny costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response" (Floyd et al. 2000, p. 411)

Table 2. Definitions of Response Efficacy, Self-efficacy, and Response Costs

Study	Examined Privacy Protecting Behavior
Son and Kim (2008)	Refusal; Misrepresentation; Removal; Negative-Word-of-Mouth; Complaining Directly to Online Companies; Complaining Indirectly to Third-Party Organizations
Chen et al. (2009)	Removal; Negative Word-of-Mouth; Complaining Directly to Online Companies; Complaining Indirectly to Third-Party Organizations
Krasnova et al. (2009)	Self-Disclosure
Wu et al. (2009)	Managing Personally Identifiable Information Diligently; Changing Privacy Settings; Exercising Caution Before Downloading and Using SNS Applications
Bulgurcu et al. (2010)	Quitting the Platform; Quitting Third-Party Applications; Limiting Socialization; Terminating Connections; Giving False Information; Searching for Additional Protection Tools
Krasnova et al. (2010b)	Information Disclosure/Self-Disclosure; Information Falsification; Selectivity in Friends; Privacy Settings; Complaining to SNS Service Provider or Other Parties
Lo (2010)	Willingness to provide personal information to SNSs
Stutzman and Kramer-Duffield (2010)	Having a Non-Public SNS Profile
Thambusamy et al. (2010)	Refusal; Misrepresentation; Removal; Negative-Word-of-Mouth
Chakraborty et al. (2013)	Changing Privacy Settings
Chen (2013)	Actual System Use
Lankton and Tripp (2013)	Changing Privacy Settings; Number of SNS friends; Allowing Only Friends One Has Interacted With A Lot in One's Friends List
Litt (2013)	Changing Privacy Setting; Deletion of People from Network/Friend Lists; Untagging Photos; Limiting Certain Updates to Certain People; Deletion of Others' Comments from one's Own Profile
Ernst (2014)	Actual System Use

Table 3. Studied Privacy Protecting Behaviors in the Literature

Privacy Protecting Behavior	Definition
Refusal	The extent to which a member intentionally refuses to provide specific information on SNSs
Misrepresentation	The extent to which a member intentionally provides dishonest or inaccurate information on SNSs (cf. Krasnova et al. 2010b)
Removal	The extent to which a member intentionally removes specific information from SNSs
Selectivity in Connections	The extent of a member's selectiveness when forming connections in SNSs, e.g., SNS-friendships, connections with company/product pages, connections with applications (e.g., Facebook games), connections with third-party websites
Termination of Connections	The extent to which a member intentionally terminates specific connections on SNSs, e.g., SNS-friendships, connections with company/product pages, connections with applications (e.g., Facebook games), connections with third-party websites
Strictness of Privacy Settings	The extent to which a member has strict privacy settings in SNSs

Table 4. Definitions of Privacy Protecting Behaviors

Privacy Protecting Behavior	Assigned behavior from the literature
Refusal	- Information Disclosure/Self-Disclosure (Krasnova et al. 2009; Krasnova et al. 2010b) - Refusal (Son and Kim 2008; Thambusamy et al. 2010) - Willingness to provide personal information to SNSs (Lo 2010)
Misrepresentation	- Giving False Information (Bulgurcu et al. 2010) - Information Falsification (Krasnova et al. 2010b) - Misrepresentation (Son and Kim 2008; Thambusamy et al. 2010)
Removal	- Deletion of Others' Comments from one's Own Profile (Litt 2013) - Removal (Chen et al. 2009; Son and Kim 2008; Thambusamy et al. 2010) - Untagging Photos (Litt 2013)
Selectivity in Connections	- Allowing Only Friends One Has Interacted With A Lot in One's Friends List (Lankton and Tripp 2013) - Exercising Caution Before Downloading and Using SNS Applications (Wu et al. 2009) - Limiting Socialization (Bulgurcu et al. 2010) - Number of SNS friends (Lankton and Tripp 2013) - Selectivity in Friends (Krasnova et al. 2010b)
Termination of Connections	- Deletion of People from Network/Friend Lists (Litt 2013) - Quitting Third-Party Applications (Bulgurcu et al. 2010) - Terminating Connections (Bulgurcu et al. 2010)
Strictness of Privacy Settings	- Changing Privacy Settings (Chakraborty et al. 2013; Lankton and Tripp 2013; Litt 2013; Wu et al. 2009) - Privacy Settings (Krasnova et al. 2010b) - Limiting Certain Updates to Certain People (Litt 2013) - Having a Non-Public SNS Profile (Stutzman and Kramer-Duffield 2010)

Table 5. Classification of Literature's Privacy Protecting Behaviors