Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors

Haiyan Jia
The Pennsylvania State University
University Park, PA
hjia@psu.edu

Pamela Wisniewski
The Pennsylvania State University
University Park, PA
pam@pamspam.com

Heng Xu
The Pennsylvania State University
University Park, PA
hxu@ist.psu.edu

Mary Beth Rosson
The Pennsylvania State University
University Park, PA
mrosson@ist.psu.edu

John M. Carroll
The Pennsylvania State University
University Park, PA
jcarroll@ist.psu.edu

ABSTRACT
Through a secondary data analysis of a nationally representative Pew survey [35-36], we empirically test the validity of two contrasting theoretical models of adolescent information privacy behaviors. Our results suggest that in seeking to understand the underlying processes of teens' privacy risk-taking and risk-coping behaviors within social media, a "risk-centric" framework may be more useful than a traditional "concern-centric" framework that emphasizes privacy antecedents and outcomes. Our newly proposed and validated "risk-centric" framework implies a possible risk escalation process wherein teens make online disclosures and render themselves more susceptible to experiences of risky online interactions; in turn, these risky experiences are associated with higher levels of teen privacy concern. Higher levels of teen privacy concern predict both advice-seeking and remedy/corrective risk-coping behaviors. Drawing on theories of information privacy and developmental psychology, we discuss these findings from the perspective of allowing teens to experience some level of online risk so that they can learn how to navigate the dangers and reap the benefits of online engagement.

Author Keywords
Adolescent online behavior; privacy; risk; coping

ACM Classification Keywords
K.4.1 [Public Policy Issues]: Ethics, Human safety, Privacy

General Terms
Human Factors; Theory; Design.

INTRODUCTION
Compared to adults, teenagers tend to underestimate their self-efficacy to avoid risk, but they still engage in more risk activities as they also underestimate risk [15]. In online environments, this general pattern may help to explain why teens are observed to engage in more risk-taking behaviors than adults [32, 53]. Within the context of online risk-taking, self-management of information privacy has been the target of considerable attention, controversy [16] and research [4], because the online world creates a wide variety of options for collecting, processing and distributing users' personal information. Yet, no existing law protects the online information privacy of teens who are 13 or older, making this population more vulnerable to dangerous online encounters and safety hazards [34][56]. Particularly, the rapid emergence of Social Network Sites (SNSs), such as Facebook, MySpace, and Pinterest, as well as emerging social networking applications such as Instagram, Vine, and Snapchat, are rife with opportunities for teens to reveal personal information and/or form risky online relationships [29, 31]. Therefore, we examine teens' privacy behaviors in the context of Facebook in order to empirically test two competing theoretical models of teens' online information privacy behaviors.

Specifically, we examine and contrast two theoretically different perspectives of teen online information privacy behaviors: (1) An established "***concern-centric***" model, which accentuates privacy concern in determining risk-related behavioral outcomes; and (2) a novel "***risk-centric***" model, which theorizes a direct effect of teen's risk-taking behaviors on psychological factors such as privacy concern, thus shaping teens' risk-coping behaviors. Further, we focus on two types of teen information privacy behaviors: ***risk-taking behaviors*** (such as information disclosures and choice of social connections) and ***risk-coping behaviors*** (such as seeking advice and/or help and taking protective measures to reduce risk); both types of privacy behaviors might be enacted by teens online to engage with others and/or protect themselves from online threats.

CSCW '15, March 14 - 18 2015, Vancouver, BC, Canada

http://dx.doi.org/10.1145/2675133.2675293

From a developmental standpoint, teens and adults are clearly in different cognitive stages, so the concern-centric model of information privacy antecedents and outcomes created and validated for adults [51] may not be adequate to explain teens' online privacy management. Our newly proposed risk-centric model, in contrast, embodies an experiential learning process, highlighting the role that teens' own risk-taking behaviors may take in developing their risk-coping mechanisms. Specifically, we propose that teens' online privacy risk-taking behaviors serve as learning opportunities, through which teens practice and develop risk-coping strategies to manage distinctive types of privacy risks. We focus specifically on teens' privacy risks in the context of SNSs, as privacy threats to this age group and in this context are especially abundant, and may quickly become complicated due to highly interactional situations [24, 29]. Teens' SNS privacy risks appear not only inherent to the social nature of online social networks, which motivates teenage users to maintain relationships with different levels of intimacy [45], but also multidimensional in terms of their nature and severity, with some aspects or dimensions of privacy risks being particularly unique and relevant to teens [41].

This paper reports the empirical results of testing the "concern-centric" versus the "risk-centric" theoretical models using a nationally representative dataset provided by Pew Research Center's *2012 Teens and Privacy Management Survey*. In the course of our model building and evaluation activities, we examine teens' online privacy behaviors and identified three unique dimensions of risk-taking behaviors, which vary based on increasing levels of privacy risk: 1) ***Basic Information Disclosures***; 2) ***Sensitive Information Disclosure;*** and 3) ***Risky Interactions***. We also identified two distinct dimensions of risk-coping behaviors, which include: 1) ***Advice Seeking*** and 2) ***Remedy/Corrective Behaviors***. We use these empirically constructed components of teens' online privacy risk-taking and risk-coping behaviors to explore the relationships between various demographic, individual-difference and psychological factors and these two behavioral variables. In doing so, we provide confirmatory evidence that our "risk-centric" framework of teens' online information privacy behaviors represents a better fit to the data than the previously established "concern-centric" model. Our results suggest that teens have uniquely different cognitive processes than adults that drive their information privacy decisions online.

We present our research using the following structure: First, we establish our research motivation and articulate how our work contributes to the extant literature on teens' online information privacy behaviors. Second, we present two competing theoretical models for understanding teens' online information privacy behaviors. Third, we describe our methodology for empirically testing these competing models and present our results. Finally, we discuss the theoretical and practical implications of our findings and suggest design opportunities for promoting adolescent online safety through leveraging risk-taking as a learning process that can help teens' make more prudent information privacy decisions online.

RESEARCH MOTIVATION AND CONTRIBUTIONS

Social scientists have argued that teens are still developing self-regulatory competence; their risk perceptions and risk appraisals may not yet be effective at guiding their online privacy behaviors [52]. Working from these assumptions, previous studies have focused primarily on intervention strategies that prevent teens from online risk exposure or that mitigate potential harm. For example, researchers have identified external factors that might protect teens online, such as governmental legislation, industry self-regulation, website warnings, and parental mediation strategies [60, 62-63]. However, fewer studies have focused on the internal belief structures and decision strategies of teens themselves in order to understand the processes through which teens are exposed to, and cope with, online privacy risks.

Furthermore, scholars who have investigated teen-related factors have largely focused on perceptual variables, such as privacy risk perceptions [63], information privacy self-efficacy [11], and social and self-expressive needs [31]; these factors influence teens' online privacy disclosures and management. However, underlying these perceptual variables is a view of privacy risk as a cognitive and psychological *state*, rather than as *behaviors* that teens actually engage in and experience. The cognitive approach aids in identifying psychological mechanisms but limits our understanding of the role that privacy behaviors may play in psychological processes. Our research attempts to fill the gaps in the current research by understanding the underlying cognitive mechanisms that drive teens' online information privacy behaviors. Specifically, our unique research contributions include:

- Establishing and contrasting two theoretical frameworks (i.e. "concern-centric" vs. "risk-centric") of teens' online information privacy behaviors
- Identifying multi-dimensional aspects of teens' information privacy risk-taking and risk-coping behaviors
- Empirically testing the theoretical models to conclude that the "risk-centric" framework may be a more appropriate framework for understanding the underlying psychological mechanism through which teens process, evaluate and respond to risks
- Providing theoretical and practical implications for improving teens' online safety through an autonomy-promoting and developmental framework of online information privacy

THEORETICAL FRAMEWORKS

APCO Macro Model

A cohesive model of privacy-related factors is essential for building an understanding of the social and psychological mechanisms of privacy and for predicting cognitive, affective, and especially behavioral responses. Scholars have approached information privacy from many angles, with theories and frameworks proposed from a range of backgrounds, as discussed in more detail below. However, due to the relative lack of such efforts in the privacy literature dealing with adolescents, we began with a general, empirically validated framework that provides a comprehensive view of predictors, processes, and outcomes of information privacy. This interdisciplinary, overarching model of information privacy is called the "Antecedents→ Privacy Concerns→ Outcome" or "APCO" Macro Model [51]. While this theoretical model was built based on a meta-review of 320 privacy articles and 128 books across multiple disciplines, we believe that we are the first to apply it to the unique context of teens' privacy behaviors for online information privacy management.

The APCO model [51] shows versatility as it includes information privacy-related factors ranging in different levels from individual and group to organizational and societal. More importantly, it incorporates numerous empirical privacy studies and identifies commonly studied relationships among these factors. At the center of the APCO model, ***privacy concern*** functions as a "proxy" for information privacy, representing the beliefs, attitudes, and perceptions of privacy at the individual level of analysis. APCO then abstracts various antecedents and outcomes of privacy concern across various disciplines of literature. ***Antecedents*** of privacy concern have included negative privacy experiences, privacy awareness, personal differences, demographic differences, and culture/climate [51]. ***Outcomes*** that have been characterized as resulting from privacy concern include behavioral reactions, such as willingness or intent to disclose personal information at the individual level, or regulatory actions that occur at a group or societal level [51]. **Figure 1** provides a high-level, simplified overview of the APCO Macro Model.

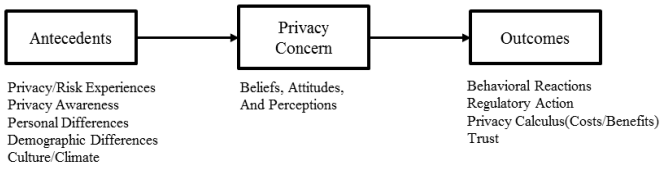

Figure 1: High-Level Overview of APCO Macro Model

The generalizability of the APCO framework provides ample flexibility for us to test relevant factors that are specific and unique to teens' online privacy risk management. Following the APCO framework, and based on an extensive literature review of other relevant privacy theories and studies, this paper will discuss the theoretical relationships between several key factors related to teen online privacy, in particular, their risk-taking versus risk-coping behaviors, privacy concern, and demographic and contextual factors, such as gender and SNS frequency, to propose a modified model of online information privacy for teens. Further, the proposed model is tested with empirical data to verify its validity and predictive power, and contrasted with an alternative model that is discussed below.

"Concern-Centric" versus "Risk-Centric" Frameworks

Two contrasting theoretical models of teens' online information privacy are proposed to theorize relationships between predictors such as demographics, other contextually relevant factors, privacy concern, teen risk-taking and risk-coping behaviors (see **Figures 2 & 3**). First, we examine the hypothesized relationships from the original APCO framework as mapped to our teen factors above; we call this baseline model our ***concern-centric*** approach to teen online privacy management (**Figure 2)**.

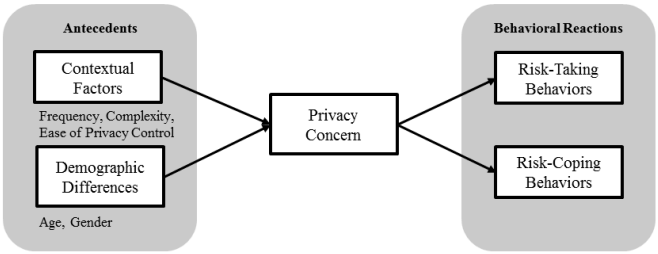

Figure 2: Concern-Centric APCO Framework

This concern-centric model hypothesizes that teens make rational privacy choices based on their concern for information privacy. Therefore, higher levels of concern would translate into more risk-adverse privacy strategies, resulting in lower levels of risk-taking and higher frequency of risk-coping behaviors. However, acknowledging that teens may operate under bounded rationality and have a limited capacity to properly assess risk, we also propose an exploratory ***risk-centric*** model (**Figure 3**) where teens' higher propensity to take risks contributes to new risk experiences, influencing privacy concern, and triggering risk-coping behaviors.

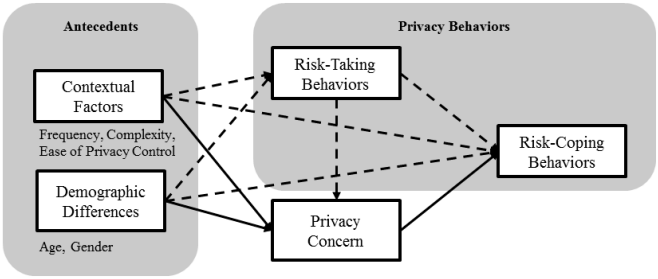

Figure 3: Risk-Centric Risk-Coping Framework

Figure 3 illustrates the new, exploratory hypotheses using dashed lines, while the original APCO hypotheses are shown with solid lines. We empirically test the concern-centric vs. risk-centric theoretical frameworks using the Pew dataset. Toward this end, we first conduct categorical principal component analyses to identify three different types of risk-taking behaviors (basic information disclosures, sensitive information disclosures, and risky interactions) and two risk-coping behaviors (advice-seeking and remedy/corrective behaviors), followed by examining their respective interrelationships between the various behaviors and other factors in our model to identify how the multidimensionality of the various behaviors uniquely effect the teen factors in our models. We further discuss the teen specific factors in the sections below.

Teen Privacy Behaviors

We specifically focus our research outcomes on teens' privacy behaviors in the context of online privacy management, not on external interventions imposed on teens by parents or regulators. Therefore, we focus on teens' risk-taking and risk-coping behaviors in the two theoretical models. From an experiential learning perspective, individuals' conception of privacy varies with life experiences [28] and is an ongoing negotiation of boundaries of disclosure, where an individual must balance the trade-offs between sharing and withholding information in a way that meets one's privacy needs [2, 44]. The decision-making process of privacy management is not fixed but often reactive to social and situational factors. This may be especially true for teens, as they may lack an effective model of self-regulation, especially when exposed to novel risk situations. Teens' experiences and negotiations through various levels of privacy threats and invasions may directly trigger their risk-coping behaviors; or it may indirectly guide the development of risk-coping strategies through increased concern. Therefore, we characterize teen privacy behaviors as an integral part of this negotiation and experiential learning process by representing teens' online privacy management behaviors as both ***risk-taking*** and ***risk-coping*** behaviors.

Risk-Taking Behaviors: A range of privacy risks have been identified with regard to teens' SNS use, such as inability to control information access, distribution, collection, or misuse by other users (social threats) or organizations (organizational threats), inability to maintain anonymity, and identity theft [26, 50]. However, the definition of privacy risk-taking behaviors varies greatly based on communicative or social norms: the social affordances of communication technologies have "forced" teens to alter conceptions of privacy [37]; as a result, contact and conduct viewed risky for an adult may serve as a self-representative or self-expressive opportunity that a teen seeks [32]. Also, relatively safe online information privacy behaviors (e.g., disclosure of age, gender and relationship status) are correlated with riskier behaviors (e.g., disclosure of personal identity information, sensitive personal information, and stigmatizing information) [40], further blurring the line between the two. In recognition of such adult-teen discrepancy in defining risk and risk escalation pattern, we define information privacy risk-taking behaviors as a spectrum of behaviors related to information disclosure and social interactions, varying from sharing basic personal information (e.g., gender and age) to disclosing highly sensitive and personal information, and further to engaging in risky social interactions.

Previous studies of teenage Facebook users have shown that basic information disclosure is positively related with disclosure of sensitive information, which in turn links with risky interactions with unknown others [43]. The social motivation for information sharing makes information privacy "intricately" related to interactional privacy—the type of privacy that relates to the control and management of social encounters and relationships [10]—especially in intimate and connected settings [13]. Further, different aspects and dimensions of a teens' risk-taking behavior may demonstrate different effects as well. For instance, a recent empirical study [26] showed that only social risk experiences (e.g., uncontrollable actions, bullying, stalking, etc.) is an influential predictor of users' intentional risk-coping; other privacy risk experiences, such as accessibility, organizational threats, and identity theft showed little to no effect. In our empirical models, we differentiate among three distinct types of risk-taking behaviors that emerged from the survey data: basic information disclosures, sensitive information disclosures, and risky interactions.

Risk-Coping Behaviors: Risk-coping behaviors refer to users' self-defensive measures to protect privacy rights as a response to their perceptions of privacy risks [48]. Teens do engage in risk-coping behaviors online, which help shield them from information privacy breaches, but very little attention has been focused on these more positive, yet often more reactive behaviors. Research in adolescents' risk-coping strategies [18, 48] suggests two main coping dimensions: approach and avoidance/withdrawal. For teens, the approach dimension refers to functional strategies such as problem-solving, information- or advice-seeking, and accepting social support, whereas the avoidance dimension includes dysfunctional strategies to withdraw from the situation without trying to change or improve it. Following this categorization, Youn [63] suggested two coping styles for dealing with privacy risks, one being approach strategies such as providing false or incomplete personal information, seeking alternative services that do not ask for personal information [63], and seeking help, information or social support; the other style includes avoidance strategies such as refusal to use the websites or services.

Help or information seeking as a risk-coping strategy is of great importance because it implies external influence such as parental guidance. Importantly however, proactive

seeking of advice functions very differently for adolescent development compared to imposed intervention. In Baumrind's [6] developmental framework of adolescents' risk-taking, the importance of respecting adolescents' growing need for autonomy and self-regulation, while maintaining a certain level of parental authority and control, is paramount. Pathological observations showed that lack of authoritative parenting tended to result in lower self-esteem, rebellious activities and psychological issues. In an attempt to understand why and how teens seek for help, Boldero and Fallon [7] found that help-seeking behaviors were predicted in part by gender and problem type (social problems as a significant predictor). Alternative help-seeking resources, such as the Internet, were found to be under-used by teens in a 2002 survey study [22]. Among the online help-seeking teens, only 14% found the Internet helpful, and the majority used it as a supplemental, rather than substituting, source for help.

Privacy Concern

In APCO, privacy concern has been accentuated as an important mediating factor between information privacy antecedents and outcomes, such as behavioral reactions, trust, and regulatory actions [51]. It is as a determinant of information disclosure behavior [3], protective behaviors [39], and online activity, or rather, the avoidance of it [40]. Although scholars have proposed positive consequences of privacy concern (e.g., motivating risk-coping behaviors) among adolescents [38][60], the moderating effect of privacy concern on online privacy behaviors is quite limited, especially among adolescents who lack the digital skills (e.g., [33]). SNS use, in particular, is found to weaken teens' online privacy concern [20], with only a weak impact on subsequent behaviors such as Facebook profile visibility and information disclosure [1, 55]. Many studies have reported that privacy concern has a limited to null effect, especially for information disclosure behaviors (e.g., [14]); this phenomenon is described by Barnes [5] as a "privacy paradox." What is paradoxical is that, on one hand, Internet users complain about their privacy being violated, while on the other hand, it appears that users provide personal information freely [42]. For example, information disclosure was not significantly related to online privacy concern in a survey of college students [56]. Instead, students preferred to manage their concerns by adjusting profile visibility or using fake names, not by restricting information. Deliberate restriction of personal information revelation was only influenced by direct social threats [26].

Theories of privacy, bounded rationality and trust have been used to explain the paradox of privacy concerns and behavior. For example, a factor like trust in social ties, a variable that is particularly salient within SNSs, may undermine the effects of concern [61]. Following Altman's [2] conceptualization of privacy as an optimization between disclosure and withdrawal, scholars (i.e., [8, 57, 59]) have pointed to a possible role for self-disclosure dynamics including impression management/self-presentation [21], identity expression [46], and social connections [19]. APCO suggests that measuring behavioral intent as a proxy for actual behavior may also be a contributing factor to this apparent paradox [51].

Demographic and Contextual Antecedents

Previous studies of online information privacy of teens and young adults have identified demographic differences and contextual factors seem to be antecedents of privacy-related factors. For instance, age is negatively associated with teen self-disclosure on Facebook [43]. An analysis of college students' Facebook privacy settings showed that restricting accessibility of personal profile as a risk-coping strategy was positively associated with a higher level of online activity (e.g., higher frequencies of log-ins, profile updates, browses of other profiles, etc.); presumably more active users have "more to hide" [30]. Other determinants of risk-coping strategies include frequency of Internet use, parenting, and observed peers' risk experiences [41]. In our empirical model, we examine age and gender as key demographic differences, and use SNS usage frequency, complexity, and ease of privacy control as contextual SNS factors that may influence teens' privacy concern, risk-taking, and risk-coping behaviors on Facebook.

"Concern-Centric" vs. "Risk-Centric" Perspectives

Given the contradictory and confounding relationships present in past literature, we decided to compare two contrasting models of how teens might regulate their online privacy through risk-taking and risk-coping behaviors. We argue that the concern-centric model may not be predictive of teens' privacy behaviors given that teens are not fully capable of privacy appraisals due to the difference between their cognitive developmental stage and that of an adult. Instead, a risk-centric model may better describe the privacy risk management strategies of the high risk-taking, high risk-coping teens. The bounded rationality hypothesis is especially critical for understanding teens' online privacy risk-coping behaviors, as their informational and cognitive limitations might render their abstract concern that they have in mind ineffective in fully determining their behavioral reactions. Rather, teens' risk-taking behaviors and subsequent experiences may inform privacy concern, and the two may function dynamically on forming risk-coping behaviors. Yet, researchers (e.g., [41]) tend to examine the relationship between antecedents and privacy concern, and that between privacy concern and outcomes, respectively, without attempts to examine the direct effect of risk-taking behaviors on risk-coping behaviors. Meanwhile, the mediating effect of privacy concern is unclear for younger generations according to the existing literature.

Privacy literature has found that privacy concern does not directly affect the amount of information disclosure; instead users tend to engage in remedy or corrective behaviors such

as restricting information visibility to chosen groups or providing unidentifiable information [21]. For example, one survey study [49] revealed that young adults are pragmatic, rather than highly concerned, about their online privacy. The researchers argued that the pragmatic users assumed a "contextual approach toward privacy" by constantly learning and forming behavioral strategies to deal with privacy concerns as they faced new situations to assess and respond accordingly. This supports what we have offered as the "risk-as-a-learning-process" paradigm, which may explain why younger generations may take a more risk-centric approach to online privacy than a concern-centric approach.

Furthermore, recent research has shown that exposure to a certain level of risk may be more effective in shaping privacy attitudes and behavior than general awareness. For instance, Debatin et al. [17] found through an online survey that users' personal experiences of privacy invasion, rather than claims of understanding privacy issues, are likely to lead to risk-coping behaviors (e.g., changing privacy settings). Similarly, a study of young adults' privacy beliefs and behaviors [23] showed that female users who were more likely to be exposed to negative online experiences were more concerned and more likely to engage in proactive privacy protection behaviors (regularly review privacy settings, monitoring profiles, careful about pictures posted onto profiles, un-tag pictures, careful about who to friend, set viewing access to friends only, set Facebook activities not to show on newsfeed).

Theoretical frameworks from developmental psychology that are specific to adolescent population also emphasize the importance of teens' risk experiences. Baumrind argues that restricting teens' experiences and limiting their overall ability to take any risks may actually be detrimental to their developmental growth [6]. According to Stevenson & Zimmerman's [54] challenge and inoculation models of adolescent resilience, exposing teens to low levels of risk may be beneficial as they provide the teens with "a chance to practice skills or employ resources." From a developmental view, repetition of such mild challenges will demonstrate an inoculation effect and prepare teens to overcome more severe risks in the future. Such a risk-as-a-learning-process approach provides a framework that examines teens' internal management of online privacy risks out of the traditional frameworks with a significant emphasis and reliance on external factors such as parental mediation or school intervention.

These prior works have encouraged us to build an understanding of the dimensions of privacy risks centered on the teens' own conceptions, and serves as a rationale for modeling the direct and indirect effects of risk experiences on teens' concern for privacy and risk-coping strategies. With the "risk-as-a-learning-process" paradigm, our new "risk-centric" model proposes alternative and more dynamic relationships than proposed in APCO to include this new experiential learning hypothesis. Specifically, theoretical emphasis is put on teens' risk-taking behaviors as an influential factor with direct effects on both privacy concern and risk-coping strategies. Meanwhile, privacy risk-taking behaviors, as well as risk-coping strategies, are hypothesized as potentially having direct associations with the various antecedents, not mediated by privacy concern.

METHODOLOGY

We tested the concern-centric and risk-centric theoretical frameworks of teens' risk-taking and risk-coping behaviors for online privacy management using a nationally representative sample of teens provided by Pew Research. In the paragraphs below, we describe how the Pew data set was collected, followed by explaining how our measures were operationalized and our method of analysis for testing our two competing models.

Pew Data Set

We analyzed a data set from the *2012 Teens and Privacy Management Survey*, conducted from July 26 to September 30, 2012 as a telephone survey using random digit dial (RDD) to gather a nationally representative sample of 802 teens aged 12 to 17 years living in the United States. The survey was conducted by Princeton Survey Research Associates International for the Pew Research Center's Internet and American Life Project [35-36]. Many of the questions were specific to teens' use of social networking sites such as Facebook, and a vast majority (94%) of respondents reported having an active Facebook account. Given the high prevalence of teen respondents who reported having active Facebook accounts, those who did not have a Facebook account were excluded from our analysis.

The final dataset consisted of 588 valid responses. 49.7% of the responses were from males (N = 292); a majority (77.6%) were Caucasian with 15.3% being African-American; and the average age was 15 years old. Almost all respondents had access to the Internet; 80.4% reported access with mobile devices. Facebook is the most frequently used social networking site; 68.4% use this SNS at least daily. 67.9% were connected with their parent(s) through Facebook and 32.3% were connected with their teachers or coaches. 32.8% reported said that on Facebook they were connected to people they had never met. 89.2% considered it not too difficult or not difficult at all, to manage privacy controls on Facebook. Only 7% and 34.5% reported as very concerned and somewhat concerned about their online privacy, respectively.

Operationalization of Measures

The Pew telephone interviews asked teens about their general trust, device ownership, Internet use, mobile use, social media use (Facebook and Twitter in particular), privacy concern, perceived ease to manage online privacy, information disclosure behaviors, privacy management behaviors, and demographic items. Prior to our analysis, the

Pew survey items had no theoretical groupings except by these various topics of interest. Thus to process the dataset, we first identified theoretically robust constructs that exhibited both face and construct validity based on the individual survey items. We then manually reviewed the survey items and responses for items that could be meaningfully mapped to the APCO theoretical framework. Working from past literature, we identified age and gender as two important demographic differences, and grouped SNS frequency, SNS complexity, and ease of SNS privacy control as salient contextual factors. We also identified items that measured teen privacy concern, risk-taking, and risk-coping behaviors. Other demographic, contextual, and privacy-related factors were identified and analyzed but dropped from the final models because of either insufficient factor loadings or insignificant influence in our models. **Appendix A** and **B** summarize all items that remained in our final models and their psychometric properties.

Data Analysis Approach

We first used categorical principal components analyses (CATPCA) [38] to construct various dimensions of teens' privacy risk-taking and risk-coping behaviors using the 21 items identified as risk-taking behaviors and the 13 items identified as risk-coping behaviors. As in the classic PCA, CATPCA produces eigenvalues associated to each of the dimensions. Each eigenvalue is a measure of the importance of the corresponding dimension in capturing the variability of the observed variable. In this study, we follow the Kaiser criterion [25] to retain dimensions with eigenvalues higher than 1. We did this to both understand the multi-dimensionality of different risk-taking and risk-coping behaviors as well as to ensure construct validity. In this survey, the original behavior items were measured as dichotomous, categorical values (e.g. "Yes" or "No"). Thus, once we identified found items loaded on a given factor, we converted each set of dichotomous data into continuous variables by creating additive indices. Using these additive indices as our risk-taking and risk-coping constructs, we then used path analyses to assess the validity of the concern-centric and risk-centric models.

RESULTS

Principal Components Analyses

Teen Risk-Taking Behaviors

The CATPCA analysis produced three constructs related to teen risk-taking: ***Basic Information Disclosures*** (items such as posting name, birthday, school, relationship status, etc., on personal profile); ***Sensitive Information Disclosures*** (items such as posting email address, cell phone number, sensitive information that he or she later regret, etc., online); and ***Risky Interactions*** (items such as receiving unwanted communication, being contacted by or connecting with strangers, automatically sharing geo-locations, etc.). After standardization, all constructs ranged from 0 to 1, with skewness statistics between -1/+1. Specifically, for basic information disclosure, *Mean* = 0.68, *SD* = 0.22; for sensitive information disclosure, *Mean* = .25, *SD* = 0.23; and for risky interaction, *Mean* = .32, *SD* = 0.17.

Teen Risk-Coping Behaviors

Two constructs of risk-coping behaviors were revealed in the analysis. We labeled these as ***Remedy/Correction*** (consisting of items such as deleting comments, a post, a friend or an account, untagging from a photo, falsifying personal information, etc.) and ***Advice Seeking*** (consisting of items such as seeking advice of online privacy management from a friend, a parent, a sibling, a teacher, or a website). After standardization, the constructs ranged from 0 to 1, with skewness statistics between -1/+1. Specifically, remedy/correction has a *Mean* = 0.46, with *SD* = 0.22; and advice-seeking with *Mean* = .28, *SD* = 0.24.

Concern-Centric (APCO) Structural Model Results

Figure 4 summarizes the path analysis results from our test of the baseline "concern-centric" (APCO) model (Model 1). It suggests that the risk-adverse, teen privacy management perspective may not be the best fit given our data. The path analysis results (see **Table 1** and **Appendix C**) indicated poor model fit (Schermelleh-Engel et al.'s goodness-of-fit criteria were adopted, including a non-significant χ^2 value or the *p*-value associated with the χ^2 larger than 0.05; the ratio χ^2/df lower than 2; the Comparative Fit Index, or *CFI*, of 0.97 or higher; the Normed Fit Index, or *NFI*, of 0.95 or higher; and the Root Mean Square Error of Approximation, or *RMSEA*, of less than 0.06 [47]), with a number of insignificant paths, and overall low explanatory values.

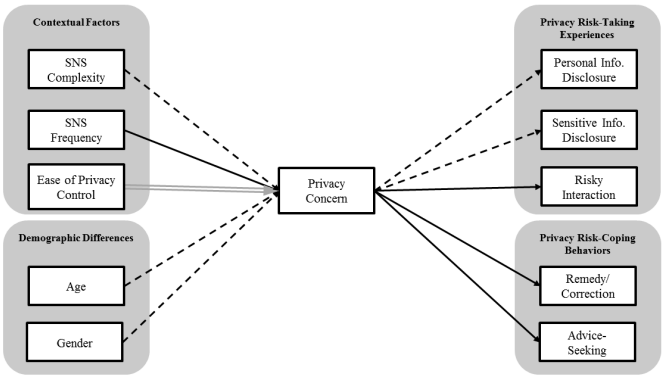

Figure 4: Concern-Centric Model (Model 1) Results.
Note*. Solid lines show paths significant at .05 level; double lines indicate negative path coefficients.*

More specifically, the Model 1 analysis indicated that SNS frequency and ease of privacy control are the only significant antecedents of teen privacy concern. Being a more frequent SNS user is associated with higher levels of concern (β = 0.13, $p < 0.001$) while higher levels of perceived ease of use for SNS privacy controls are negatively correlated with privacy concern (β = -0.19, $p < 0.001$). Privacy concern predicts risk-coping behaviors as expected, with increased levels positively associated with

both advice seeking (β = 0.19, p < 0.001) and remedy/corrective behaviors (β = 0.18, p < 0.001). However, privacy concern does not have the expected inverse relationship with respect to any of the risk-taking behaviors. The paths from privacy concern to basic information disclosure and sensitive information disclosure behaviors are both non-significant, while the *positive* relationship between privacy concern to risky interactions (β = 0.10, p < 0.05) is contrary to the hypothesized model.

Risk-Centric Structural Model Results

A nearly saturated risk-centric model (Model 2) was tested, yielding some indicators of good model fit, yet included a number of insignificant paths (**Appendix D**). Further path analyses were guided by the modification indices and yielded a more parsimonious model containing only statistically significant paths (Model 3). Model 3 (**Figure 5**) was also seen to have good model fit. **Table 1** summarizes the fit statistics across all three models. Model 3 offers the most parsimonious results with acceptable fit indicators. Therefore, the final model results reported in **Figure 5** and discussed below are based on Model 3.

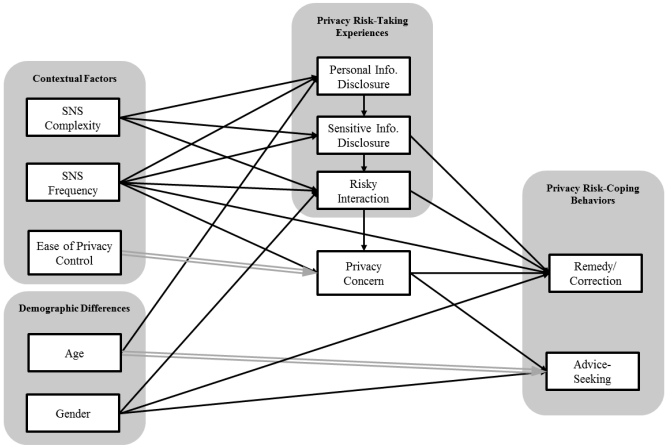

Figure 5: Risk-Centric Model (Model 3) Results.
Note: *All paths shown are significant at .05 level; double lines indicate negative path coefficients*

	χ^2 (*DF*)	NFI	CFI	RMSEA	R^2 (Remedy/ Correction)
Model 1	448.736 (31)	0.378	0.374	0.152	0.036
Model 2	1.519 (1)	0.998	0.999	0.030	0.341
Model 3	18.882 (23)	0.974	1.000	0.000	0.330

Table 1. Summary of model estimates.

The relationships in Model 3 imply an escalation trajectory for risk-taking. Specifically, basic information disclosure is positively associated with sensitive information disclosure (β = 0.22, p < 0.001), which in turn is positively associated with risky interaction (β = 0.23, p < 0.001). All three types of risk-taking behaviors are positively predicted by SNS complexity (basic information disclosure: β = 0.20, p < 0.001; sensitive information disclosure: β = 0.23, p < 0.001; and risky interaction: β = 0.36, p < 0.001) and SNS frequency (basic information disclosure: β = 0.21, p < 0.001; sensitive information disclosure: β = 0.17, p < 0.001; and risky interaction: β = 0.11, p < 0.01). Furthermore, basic information disclosure is positively associated with age (β = 0.16, p < 0.01), whereas risky interaction is significantly associated with gender (β = 0.11, p < 0.01). The level of privacy concern is positively associated with frequency of teens' SNS use (β = 0.14, p < 0.01) as well as their online risky interaction (β = 0.10, p < 0.05), and is reduced by perceived ease of privacy control (β = -0.18, p < 0.001). Finally, similar to the concern-centric model, privacy concern appears to be a significant and positive predictor of both types of risk-coping behaviors. More interestingly, risk-taking behaviors such as sensitive information disclosure (β = 0.14, p < 0.001) and risky interaction (β = 0.44, p < 0.001) also are directly associated with remedy/corrective behaviors. Some demographic factors also have demonstrated significant relationships: a gender effect is found such that girls engage more frequently in both types of risk-coping behaviors; and age is negatively associated with advice-seeking.

DISCUSSION

In this section, we summarize our results, discuss their theoretical implications, and consider opportunities for design. We conclude by pointing to some limitations of our study and areas for future research.

Summary of Results

We used categorical principal components analyses to identify distinctive dimensions or aspects of teen privacy risk-taking (resulting in three dimensions) and risk-coping behaviors (resulting in two dimensions). We then used structural equation modeling to test the validity of a concern-centric versus a risk-centric theoretical model of teens' online information privacy management. We found that the risk-centric model was a much better fit to our empirical data and that the final model revealed complex relationships between the privacy-related factors.

More specifically, SNS-related contextual factors were significant predictors for all three types of privacy risk-taking behaviors; age predicted only basic information disclosure. Both SNS frequency and risky interactions were positively associated with privacy concern, while perceived ease of privacy control appeared as a negative predictor of concern. With respect to privacy risk-coping behaviors, remedy/correction behaviors were positively associated with SNS frequency, sensitive information disclosures, risky interactions, and privacy concern. Privacy concern was also a positive predictor of advice seeking, whereas age was negatively associated with advice seeking behaviors.

Theoretical Implications

Privacy Behaviors are Multi-dimensional and Inter-related

Teen risk-taking behaviors emerged as three separate statistical factors, and teen risk-coping behaviors emerged as two additional factors. Furthermore, these different risk-taking and risk-coping behaviors functioned very differently than one another in our model. This suggests that different privacy behaviors should be tested in future models, instead of assuming that risk-taking and risk-coping behaviors are one-dimensional.

Our findings also suggest that not all risk-taking behaviors are equally as risky and that there may be a pattern of risk escalation between the three risk-taking factors. We saw accumulative effects of risk-taking behaviors, where lower levels of risk-taking are predictive of higher levels risk (basic information disclosures → sensitive information disclosures → risky interactions). At face value, we would automatically assume that risky interactions are more dangerous than disclosing sensitive information online, which in turn would be more risky than disclosing basic personal information online. Again, logically this makes sense. If a teen shares sensitive information, such as his or her phone number through social media, this would put him or her at higher risk of engaging in potentially dangerous offline interactions with strangers. However, this may not necessarily be true if a teen just shared basic information, such as his or her real name and relationship status.

Our risk-centric model offers statistical evidence of risk escalation, showing that basic information disclosures are positively associated with sensitive information disclosures but not risky interactions, yet showing that sensitive information disclosures are positively associated with risky interactions. Also, only risky interactions are positively associated with heightened teen privacy concerns. It is also noteworthy that basic information disclosures are not significantly related to teen risk-coping behaviors, suggesting that disclosing basic information about oneself online may not be perceived by teens as risky at all.

Teen Privacy Management as Experiential Learning

Both empirically tested theoretical models suggest that in the case of teens, privacy concern has a direct influence on risk-coping behaviors but not on teens' propensity to take risks. The risk-centric model provides empirical evidence of teens' propensity to first seek risks, and then take corrective actions to protect their online privacy. It makes sense that teens taking more risks also take more remedy/corrective actions to protect their online privacy after-the-fact. Yet, teen privacy concerns are not significantly related to their personal or sensitive information disclosure behaviors. Teens share personal and sensitive information through social media regardless of their concern for privacy. However, when teens report engaging in risky online interactions that they view as regrettable, that behavior is positively associated with their privacy concern.

The most logical explanation for this relationship would be that risky interactions heighten teens' concerns about privacy, not that teens who already experience who already experience higher levels of concern seek more frequent risky interactions online. Furthermore, teens' privacy concern, once elevated, is positively associated with both risk-coping (advice-seeking and remedy/corrective) behaviors. Therefore, when all of these significant relationships are combined, they suggest that teens do care about their online privacy; nonetheless, they are willing to take privacy risks. And, through a process of experiential learning, where risk-taking behaviors contribute to risk-learning experiences, teens mitigate these risks later by taking protective actions when they feel their privacy boundaries may have been compromised. This reasoning, in combination with our empirical results, we propose **Figure 6** as a theoretical model for understanding the process of privacy regulation for teens' online privacy management in future research.

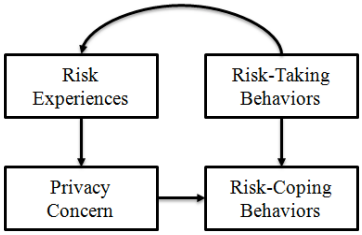

Figure 6: Theoretical Framework of Teen Online Privacy Management

Developing Privacy Awareness and Coping Strategies

Even though information disclosure does not appear to enhance teens' privacy concern, the risk-centric model reveals that disclosing sensitive information is associated with higher likelihood of remedy and corrective behaviors. This relationship indicates that teens perceive risks related to sensitive information disclosures and are more likely to take protective measures to reduce privacy breaches and threats. Risky interactions, on the other hand, appear to exceed teens' comfort level of managing the potential threats by themselves and are, thus, associated with higher levels of privacy concern. Increased privacy concern may, in turn, encourage teens to turn to external resources for guidance and help.

This dynamic relationship between the different types of privacy risks and teens' risk-coping responses lends insight into how teens negotiate their information boundaries. It suggests a developmental process through which teens' awareness and coping mechanisms of information privacy risks are shaped in response to their accumulative risk experiences. If the privacy risks experienced by teens are moderate and manageable, as the inoculation model suggests, they will develop resilience to future privacy risk events. This "risk-as-learning-process" model highlights how today's younger generations who are digital natives

form their own risk perceptions and protective strategies from personal experiences with social technologies [37].

It also suggests that teens are, to some extent, capable of identifying the manageable level of risk and adopting different coping strategies accordingly; they will cope with low-level risks by themselves, but they cope with high-level risks using external help systems. This process may be beneficial as it supports proximal development of the teens to allow them to experience and learn and at the same time to protect them from significant harms. In order to assist the identification process, effort should be put to helping teens understand potential and hidden risks, enhancing their awareness of risk invasion and threats, and thereby encouraging them to seek for information and aid when they face privacy risks.

In this sense, the so-called "privacy paradox" [5] may be misleading, at least when it is used to describe the privacy behaviors of this age group. In other words, it is not that their privacy concern fails to moderate their disclosure behaviors; rather, there is a mismatch between their conceptions of risk and the traditional conceptions tied to information disclosure. Therefore, privacy concern is not the effective motivator of risk-coping, but a potential mediating factor underlying the restrictive effect of highly risky behaviors on privacy risk-coping. For this younger generation, risk management should not be equated with *insulation* from risk; instead, we should see exposure to privacy risk and subsequent coping behaviors as an opportunity to influence today's adolescents. With their privacy perceptions and behaviors shaped by the emerging affordances of communication technologies, teens may develop novel ways of evaluating risks in general, and this new outlook and psychology of risk may have significant implications at both personal and societal levels [9].

Implications for Design

Contrasting the concern-centric and risk-centric models, we might infer that, for the generally technology-savvy younger generation, we should explore ways to *enhance risk awareness* in their frequently-used cyberspaces rather than implementing restrictive interventions, so that they can better learn from online privacy risk experiences. For example, design effort and policy-making could focus on mitigation of potential harms in social networking sites, especially those related to social threats, instead of trying to limit teens' SNS use or basic information disclosures. The risk-centric model has implications for designing more effective online security and safety mechanisms for teens. It highlights the importance of educating teenage users about possible privacy risks as they are encountered, and providing opportunities for them to seek help when risks become more dangerous than they can handle on their own. This "learning at the moment of experiencing" is in line with previous literature (e.g., [27]), which suggests embedded training as a more effective practice compared to, for instance, sending separate security emails and notices that are not specifically attached to a contextualized "learning moment," to educate users about phishing and protect them from such attacks.

The accumulative nature of information privacy risks, and especially the fact that only high-level risks such as risky interactions can lead to heightened privacy concern, indicate the importance of educating teens about the correlative relationship between low-level and high-level risks, including instruction on how disclosing basic information can potentially lead to more severe privacy invasion and harm. Education concerning privacy risk, digital literacy and cybersecurity offered through schools, workshops or online courses (e.g., MOOCs) can effectively increase teens' awareness of less apparent privacy risks and encourage them to seek help from external resources.

Beyond educating teens, SNS service providers might also be proactive in helping teens to autonomously engage with others online, while simultaneously implementing interface features that discourage them from exposing themselves to extreme, imminent risks. For example, natural language processing has been explored as a way to identify cyberbullying on Twitter [12]. Using similar and other (e.g., identifying messages sent from outside of one's network) approaches, SNSs may be able to identify common patterns leading to risky behaviors and alert teen users of these risks before they occur. Doing so may heighten teens' awareness of their own sensitive information disclosures or potentially risky interactions so that they can adjust accordingly.

Limitations and Future Research

We would like to address some of the limitations of our findings that can be leveraged as opportunities for informing future research. First, we used cross-sectional survey data to test the theoretical models of teen online privacy management, and this leads to some ambiguity between antecedents and outcomes. Therefore, future longitudinal and/or interview studies should be conducted to confirm the process-level relationships that we theorize in **Figure 6**. Second, important factors such as trust (in other users and/or in service providers), perceived security, self-efficacy, etc. were not measured in the Pew dataset; therefore, these relationships could not be examined in our models. On one hand, the Pew data set is a strength of our research because it provided a large, nationally representative sample of teens, which is a challenging population to study. On the other hand, our empirical test was constrained by the sample data because we had to construct factors from the items already measured in the survey. While we were able to leverage CATPCA to develop more theoretically and statistically robust factors, we recognize that some of the factors used in our empirical models could have been operationalized with more precision. Future studies would benefit from crafting their own survey instruments in order to pre-validate measures and test additional salient factors.

Our study suggests that a moderate level of risk experience may serve as a learning opportunity in teens' developing awareness of information privacy risks and the adoption of risk-coping strategies. However, we also note that risks beyond a certain threshold can cause significant harm. Future research is needed to identify the amount and types of risk experiences that teens can be exposed to achieve an optimal amount of learning without privacy harms, or a "zone of proximal development" [58] conceptualized in cognitive development literature, in order to understand the design space and the policy space for what a teen can learn from certain types or levels of risk experiences and when a teen may need external help or guidance.

CONCLUSION

This paper theoretically constructed and empirically compared two theoretical models of teens' online information privacy risks. Using nationally representative data, the study provides a taxonomy of teens' privacy risk-taking behaviors and risk-coping behaviors. It further revealed that a concern-centric approach that emphasizes the cognitive reasoning in conceptualizing and managing information privacy risks is less applicable to teenagers than other populations studied; rather, teens develop their risk-coping strategies as direct and indirect responses to their personal experiences of privacy risks. This risk-centric approach offers a "risk-as-learning-opportunity" framework and highlights the importance of rethinking teens' conceptions of risks and strategies to reduce and prevent privacy harms for teens from a developmental perspective.

ACKNOWLEDGMENTS

First, we would like to thank Mary Madden, Senior Researcher at Pew Research Center, who enabled our access to the Pew data set. Also, this research was supported by the U.S. National Science Foundation under grant CNS-1018302. Part of the work of Heng Xu was done while working at the U.S. National Science Foundation. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

REFERENCES

1. Acquisti, A., & Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies*, (2006), 36-58.
2. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing, Monterey, CA, 1975.
3. Bansal, G., Zahedi, F. and Gefen, D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*, 2 (2010), 138-150.
4. Barkhuus, L. and Dey, A. K. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. *INTERACT 3*(2003), 702-712.
5. Barnes, S. B. *A privacy paradox: Social networking in the United States*, 2006.
6. Baumrind, D. A developmental perspective on adolescent risk taking in contemporary America. *New directions for child development*, 37 (1987), 93-125.
7. Boldero, J., & Fallon, B. Adolescent help-seeking: What do they get help for and from whom? *Journal of Adolescence*, *18*, 2 (1995), 193-209.
8. boyd, d. Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life In D. Buckingham (ed.) *YOUTH, IDENTITY, AND DIGITAL MEDIA*, *Berkman Center Research Publication No. 2007-16*, (2007).
9. Breakwell, G. M. *The psychology of risk* Cambridge University Press, Cambridge, 2007.
10. Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B. and Perry, D. Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, *6*, 2 (1989), 131-158.
11. Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions*, *52*, 2 (2009), 167-182.
12. Chen, Y., Zhang, L., Michelony, A. and Zhang, Y. 4Is of social bully filtering: identity, inference, influence, and intervention. In *Proc. Proceedings of the 21st ACM international conference on Information and knowledge management*, ACM (2012), 2677-2679.
13. Cho, H., & LaRose, R. Privacy issues in Internet surveys. *Social Science Computer Review*, *17*, 4 (1999), 421-434.
14. Christofides, E., Muise, A., & Desmarais, S. Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*, 3 (2009), 341-345.
15. Cohn, L. D., Macfarlane, S., Yanez, C., & Imai, W. K. Risk-perception: differences between adolescents and adults. *Health Psychology*, *14*, 3 (1995), 217.
16. Consumers-Union. *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*. 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.
17. Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer Mediated Communication*, *15*, 1 (2009), 83-108.

18. Dumont, M., & Provost, M. A. Resilience in adolescents: Protective role of social support, coping strategies, self-esteem, and social activities on experience of stress and depression. *Journal of youth and adolescence*, *28*, 3 (1999), 343-363.
19. Ellison, N. B., Steinfield, C. and Lampe, C. The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*, 4 (2007), 1143-1168.
20. Feng, Y. and Xie, W. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Comput. Hum. Behav.*, *33* (2014), 153-162.
21. Goffman, E. *The presentation of self in everyday life*. Anchor, New York, USA, 1959.
22. Gould, M. S., Munfakh, J. L. H., Lubell, K., Kleinman, M., & Parker, S. Seeking help from the internet during adolescence. *Journal of the American Academy of Child & Adolescent Psychiatry*, *41*, 10 (2002), 1182-1189.
23. Hoy, M. G., & Milne, G. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*, 2 (2010), 28-45.
24. ISTTF. *Enhancing Child Safety and Online Technologies*. Harvard University's Berkman Center for Internet and Society, Internet Safety Technical Task Force, 2008,
25. Kaiser, H. F. The Application of Electronic Computers to Factor Analysis. *Educational and Psychological Measurement*, *20*, 1 (April 1, 1960 1960), 141-151.
26. Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*, 1 (2009), 39-63.
27. Kumaragruru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J. and Nunge, E. Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proc. SIGCHI Conference on Human Factors in Computing Systems*, ACM (2007), 905-914.
28. Laufer, R. S. and Wolfe, M. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*, 3 (1977), 22-42.
29. Lenhart, A. and Madden, M. *Teens, Privacy & Online Social Networks, PEW Internet & American Life Project*. 2007, http://www.pewinternet.org/ppf/r/211/report_display.asp .
30. Lewis, K., Kaufman, J., & Christakis, N. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer Mediated Communication*, *14*, 1 (2008), 79-100.
31. Livingstone, S. Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy, and self-expression. *New Media & Society*, *10* (2008), 393-411.
32. Livingstone, S., i Helsper, E. Gradations in digital inclusion: children, young people and the digital divide. *New Media & Society*, *9*, 4 (2007), 671.
33. Livingstone, S., Ólafsson, K. and Staksrud, E. Risky Social Networking Practices Among "Underage" Users: Lessons for Evidence-Based Policy. *Journal of Computer-Mediated Communication*, *18*, 3 (2013), 303-320.
34. Lwin, M. O., Stanaland, A. and Miyazaki, A. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing*, *4*, 2 (2008), 205–217.
35. Madden, M., Cortesi, S., Gasser, U., Lenhart, A. and Duggan, M. *Where Teens Seek Online Privacy Advice*. Pew Research Center's Internet & American Life Project, 2013, http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/.
36. Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. and Beaton, M. *Teens, Social Media, and Privacy* 2013, http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx.
37. Marwick, A. E. and boyd, d. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* (July 21, 2014).
38. Meulman, J. J. and Heiser, W. J. *SPSS-Categories*. 2004, http://www.helsinki.fi/~komulain/Tilastokirjat/IBM-SPSS-Categories.pdf.
39. Milne, G. R. and Culnan, M. J. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*, 3 (2004), 15-29.
40. Miyazaki, A. D., & Fernandez, A. Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, *35*, 1 (2001), 27-44.
41. Moscardelli, D. M., & Divine, R. Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy Protecting Behaviors. *Family and Consumer Sciences Research Journal*, *35*, 3 (2007), 232-252.
42. Norberg, P. A., Horne, D. R., & Horne, D. A. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 1 (2007), 100-126.
43. Nosko, A., Wood, E. and Molema, S. All about me: Disclosure in online social networking profiles: The

case of FACEBOOK. *Computers in Human Behavior*, *26*, 3 (2010), 406-418.

44. Palen, L. and Dourish, P. Unpacking "privacy" for a networked world. In *Proc. Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM (2003), 129-136.
45. Rachels, J. Why privacy is important. In D. G. J. J. W. Snapper (ed.) *Ethical issues in the use of computers*, (1985), 194-200.
46. Schau, H. J. and Gilly, M. C. We are what we post? Self-presentation in personal web space. *Journal of Consumer Research*, *30*, 3 (2003), 385–404.
47. Schermelleh-Engel, K., Moosbrugger, H. and Müller, H. Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of psychological research online*, *8*, 2 (2003), 23-74.
48. Seiffge-Krenke, I. *Stress, coping, and relationships in adolescence*. Lawrence Erlbaum, Mahwah, NJ, 1995.
49. Sheehan, K. B. Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*, 1 (2002), 21-32.
50. Shin, D. H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, *22*, 5 (2010), 428-438.
51. Smith, H. J., Dinev, T. and Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*, 4 (2011), 989-1015.
52. Steinberg, L. Risk taking in adolescence: what changes, and why? *Annals of the New York Academy of Sciences*, *1021*, 1 (2004), 51-58.
53. Steinberg, L. A social neuroscience perspective on adolescent risk-taking. *Developmental review*, *28*, 1 (2008), 78-106.
54. Stevenson, F. and Zimmerman, M. A. ADOLESCENT RESILIENCE: A Framework for Understanding Healthy Development in the Face of Risk. *Annual Review of Public Health*, *26* (2005), 399-419.
55. Tan, X., Qin, L., Kim, Y., & Hsu, J. Impact of privacy concern in social networking web sites. *Internet Research*, *22*, 2 (2012), 211-233.
56. Tufekci, Z. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, *28*, 1 (February 1, 2008 2008), 20-36.
57. Utz, S., & Kramer, N. The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*, 2 (2009).
58. Vygostky, L. S. *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press, Cambridge, Mass, 1978.
59. Walther, J. B. Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research*, *23* (1996), 3-44.
60. Wisniewski, P., Xu, H., Rosson, M. B. and Carroll, J. M. Adolescent Online Safety: The "Moral" of the Story. In *Proc. CSCW 2014* (2014).
61. Xu, H., Parks, R., Chu, C. H., & Zhang, X. L. Information disclosure and online social networks: From the case of Facebook news feed controversy to a theoretical understanding. In *Proc. AMCIS 2010* (2010).
62. Youn, S. Parental influence and teens' attitude toward online privacy protection. *Journal of Consumer Affairs*, *42*, 3 (2008), 362-388.
63. Youn, S. Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, *49*, 1 (2005), 86-110.

Appendix A. Categorical Principal Components Analysis Results.

Measures of Constructs	Eigenvalue
Information Privacy Risk-Taking Behaviors	
Basic Information Disclosure	**2.24**
Is your birthdate posted to your profile or account?	
Is your real name posted to your profile or account?	
Is your school name posted to your profile or account?	
Is a photo of yourself posted to your profile or account?	
Do you ever share photos of yourself online?	
Is your relationship status posted to your profile or account?	
Risky Interaction	**1.55**
Have you ever received online advertising that was clearly inappropriate for your age?	
Are you friends with or otherwise connected to other people you have never met in person?	
Have you ever been contacted online by someone you did not know in a way that made you feel scared or uncomfortable?	
Do you ever post updates, comments, photos or videos that you later regret sharing?	
Do you ever set up your profile or account so that it automatically includes your location on your posts?	
Sensitive Information Disclosure	**1.47**
Is your email address posted to your profile or account?	
Are your interests, such as movies, music, or books you like, posted to your profile or account?	
Have you ever shared sensitive information online that later caused a problem for you or others in your family?	
Is your cell phone number posted to your profile or account?	
Do you ever share videos of yourself online?	
Are videos of you posted to your profile or account?	
Have you ever said you were older than you are so you could get onto a website or sign up for an online account?	
Have you ever posted something online that got you in trouble at school?	
Information Privacy Risk-Coping Behaviors	
Remedy/Correction	**2.66**
Do you ever delete people from your network or friends' list?	
Do you ever remove your name from photos that have been tagged to identify you?	
Do you ever delete comments that others have made on your profile or account?	
Do you ever delete or edit something that you posted in the past?	
Do you ever post fake information like a fake name, age or location to help protect your privacy?	
Do you ever share inside jokes or coded messages that only some of your friends would understand?	
Do you ever block people?	
Do you ever delete or deactivate a profile or account?	
Advice-Seeking	**1.64**
Have you ever turned to a friend or peer for advice about how to manage your privacy online?	
Have you ever turned to your brother, sister or cousin for advice about how to manage your privacy online?	
Have you ever turned to your parent for advice about how to manage your privacy online?	
Have you ever turned to a teacher for advice about how to manage your privacy online?	
Have you ever turned to a website for advice about how to manage your privacy online?	

Appendix B. Measurement of Key Variables in the Models.

SNS Complexity

Are you friends with or otherwise connected to…?

1. Your parents
2. Your brothers or sisters
3. Extended family
4. Friends at school
5. Other friends that don't go to your school
6. Teachers or coaches
7. Celebrities, musicians or athletes
8. Other people you have never met in person

Frequency of SNS Use

About how often do you visit social networking sites? (Reverse-coded)

1. Several times a day
2. About once a day
3. 3 to 5 days a week
4. 1 to 2 days a week
5. Every few weeks
6. Less often

Ease of Privacy Control

Overall, how difficult is it to manage the privacy controls on your Facebook profile?

1. Very difficult
2. Somewhat difficult
3. Not too difficult
4. Not difficult at all

Privacy Concern

Thinking again about the social network site that you use most often, how concerned are you, if at all, that some of the information you share on the site might be accessed by third parties without your knowledge? (Reverse-coded)

1. Very concerned
2. Somewhat concerned
3. Not too concerned
4. Not at all concerned

Appendix C. Parameter Estimates of Model 1.

Parameter Estimate	*Standardized*	*p*
SNS Complexity → Concern	0.059	0.151
SNS Frequency → Concern	0.134	0.001
Ease of Control → Concern	-0.187	0.000
Age → Concern	-0.004	0.922
Gender → Concern	0.043	0.281
Concern → Basic Disclosure	0.022	0.594
Concern → Sensitive Disclosure	0.016	0.696
Concern → Risky Interaction	0.101	0.014
Concern → Remedy/Correction	0.189	0.000
Concern → Advice-seeking	0.180	0.000

Appendix D. Parameter Estimates of Model 2.

Parameter Estimate	*Standardized*	*p*
SNS Complexity (SC) → Basic Disclosure (BD)	0.198	0.000
SC → Sensitive Disclosure (SD)	0.225	0.000
SC → Risky Interaction (RI)	0.361	0.000
SC → Concern	0.045	0.314
SC → Remedy/Correction (RC)	-0.002	0.967
SC → Advice-seeking (AS)	0.030	0.502
SNS Frequency (SF) → BD	0.205	0.000
SF → SD	0.169	0.000
SF → RI	0.112	0.004
SF → Concern	0.135	0.001
SF → RC	0.078	0.029
SF → AS	0.044	0.304
Ease of SNS Privacy Control (EC) → BD	-0.030	0.441
EC → SD	0.028	0.490
EC → RI	-0.072	0.062
EC → Concern	-0.183	0.000
EC → RC	-0.027	0.443
EC → AS	-0.070	0.090
Age → BD	0.164	0.000
Age → SD	0.007	0.856
Age → RI	0.054	0.172
Age → Concern	-0.004	0.931
Age → RC	0.005	0.885
Age → AS	-0.111	0.009
Gender → BD	-0.007	0.850
Gender → SD	-0.120	0.002
Gender → RI	0.058	0.124
Gender → Concern	0.037	0.361
Gender → RC	0.163	0.000
Gender → AS	0.097	0.017
BD → SD	0.221	0.000
SD → RI	0.226	0.000
BD → Concern	-0.022	0.615
SD → Concern	-0.020	0.647
RI → Concern	0.096	0.016
BD → RC	0.019	0.604
BD → AS	-0.004	0.924
SD → RC	0.135	0.000
SD → AS	0.198	0.000
RI → RC	0.442	0.000
RI → AS	0.051	0.257
Concern → RC	0.225	0.000
Concern → AS	0.361	0.000